

International **Comparative** Legal Guides



Digital Business **2021**

A practical cross-border insight into digital business law

Second Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Armengaud Guerlain
Bagus Enrico & Partners
Charles Russell Speechlys LLP
Cozen O'Connor
E & G Economides LLC
G&W Legal
Greychapel Legal
Hammad & Al-Mehdar Law Firm

Hassan Radhi & Associates
Immigration Solutions Lawyers
Lee and Li, Attorneys-at-Law
Lewis Silkin LLP
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga
Advogados
Mic, Ilie & Asociații
Pelinari & Pelinari
Portolano Cavallo

ROBIC LLP
Shin Associates
SKW Schwarz
SLV Legal
Walder Wyss Ltd

ICLG.com



ISBN 978-1-83918-119-1
ISSN 2732-5237

Published by

glg global legal group

59 Tanner Street

London SE1 3PL

United Kingdom

+44 207 367 0720

info@glgroup.co.uk

www.iclg.com

Publisher

James Strobe

Senior Editor

Sam Friend

Head of Production

Suzie Levy

Chief Media Officer

Fraser Allan

CEO

Jason Byles

Printed by

Ashford Colour Press Ltd.

Cover image

www.istockphoto.com

Strategic partners



International **Comparative** Legal Guides

Digital Business **2021**

Second Edition

Contributing Editors:

James Gill & Victor Timon
Lewis Silkin LLP

©2021 Global Legal Group Limited.

All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.

This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Analysis Chapters

1

De-risking Digital Business Dreams

James Gill, Victor Timon & Helen Hart, Lewis Silkin LLP

5

Modern Slavery: A 'Wicked Problem' that Requires a Human Rights-Based Approach

Anne O'Donoghue, Lihini Konara, Adelaide Falzon & Tiara Dalpadado, Immigration Solutions Lawyers

Q&A Chapters

15

Bahrain

Hassan Radhi & Associates: Ahmed Abbas & Sayed Jaffer Mohamed

20

Brazil

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga
Advogados: Fabio Ferreira Kujawski, Lisa Worcman,
Paulo Marcos Rodrigues Brancher & Thiago Luís Sombra

28

Canada

ROBIC LLP: Jean-François Normand

36

Cyprus

E & G Economides LLC: Xenia Kasapi &
George Economides

43

France

Armengaud Guerlain: Catherine Mateu

54

Germany

SKW Schwarz: Dr. Christoph Krück, Franziska
Ladiges, Alexander Möller & Heiko Wunderlich

62

India

G&W Legal: Disha Mohanty & Arjun Khurana

70

Indonesia

Bagus Enrico & Partners: Enrico Iskandar,
Bratara Damanik & Jonathan Cheong

78

Ireland

Lewis Silkin LLP: Victor Timon

88

Italy

Portolano Cavallo: Irene Picciano, Fabiana Bisceglia,
Donata Cordone & Livia Petrucci

97

Japan

Anderson Mōri & Tomotsune: Ken Kawai &
Takashi Nakazaki

104

Malaysia

Shin Associates: Joel Prashant & Foo Jia Yi

116

Nigeria

Greychapel Legal: Eniola Elegushi & Maryann
Ntamere

124

Romania

Mic, Ilie & Asociații / Pelinari & Pelinari / SLV Legal:
Alexandru Stanescu, Andrei Pelinari, Stelian Mic &
Tudor Velea

135

Saudi Arabia

Hammad & Al-Mehdar Law Firm: Suhaib Hammad

141

Switzerland

Walder Wyss Ltd: Jürg Schneider, Hugh Reeves &
Maria Gentile

149

Taiwan

Lee and Li, Attorneys-at-Law: Robin Chang &
Eddie Hsiung

156

United Kingdom

Charles Russell Speechlys LLP: Jason Saiban &
Caroline Swain

164

USA

Cozen O'Connor: Victor J. Castellucci

De-risking Digital Business Dreams

Lewis Silkin LLP



James Gill



Victor Timon



Helen Hart

It is undisputed that the COVID-19 pandemic accelerated the pace of digital change. Since then, many consider that at least 10 years' development has taken place. Last year's Guide neatly highlighted five key forces of disruption that are set to transform businesses, including 5G and with it, the Internet of Things (IoT), Artificial Intelligence (AI), Autonomy, Hybridity and Blockchain. These remain highly relevant.

Businesses operating digitally must now grapple with key issues including data privacy, cybersecurity, advertising and consumer law, discrimination laws, online harms, competition laws, smart contracts and regulating emerging technologies, such as driverless cars and drones, and payment services laws. To whet your appetite for what follows in this new edition, we take a brief look at how some of the key legal issues intersect with key industry sectors and forms of technology.

AI, algorithms and employment rights

As a result of the pandemic, we have had to work online, access services online (such as healthcare and retail), and meet-up online. The House of Lords Covid Select Committee has published a report calling on the UK government to devise a hybrid strategy for healthcare, recognising that a mixed delivery model online and face-to-face healthcare is now here to stay. This is not unique to the UK. The report also called for greater protections for those working in the gig economy or via online platforms. It came against the background of a recent UK Supreme Court decision ruling that Uber drivers are workers and a similar ruling in the Netherlands regarding food delivery riders and drivers. In Spain, a new law has been proposed which would require delivery app businesses to tell riders and drivers what variables their algorithms use to rate and manage them.

For many businesses, developments over the past year have been all about people. There is recognition by businesses across the world that their people are integral to building a successful 'digital future'. They want to equip their people with the skills they need to build that future – for this reason, and many others, tech and data will remain extremely high on the boardroom agenda. Agile working is here to stay and the best businesses are investing heavily to facilitate ways of working that get the best out of their people, thus helping to retain, and attract, staff. So we expect to see a big increase in demand for agile working

technologies. 'Continuous Delivery', 'Design Thinking' and 'Growth Hacking' were crucial for agile working-tech last year and will remain so. New agile tech includes automation of HR processes (such as hiring and training staff), AI/machine learning-enabled predictive security tech, and VoIP apps. As remote workers are more likely to work longer hours, time-tracking software and employee monitoring software will be widely adopted to minimise employee burnout. Conversely, where productivity can be monitored, expect to see (more invasive) productivity-monitoring tech. Data privacy issues and employment rights law should not be underestimated.

The pandemic led to examinations in various countries being cancelled, and algorithm-based systems being used to award student grades. Following allegations in the UK of bias against students from lower income households, the system was swiftly withdrawn and grades recalculated based on human teacher assessment. A similar scenario unfolded in Ireland with mistakes in the algorithm used after the cancellation of the Leaving Certificate examinations.

The Court of Appeal told South Wales Police that it was unlawful to use facial recognition technology. It was also admitted by some businesses that their algorithms are essentially racist and cannot recognise photographs of black people. In addition, the UK Competition and Markets Authority (CMA) launched a study into the use of algorithms, particularly looking at the increasing use of pricing algorithms and the adverse impact for consumers. All of this has led to increasing scrutiny of AI and especially bias in *how* it is used. On the same day that the Covid Select Committee issued its report, the European Commission proposed a new Regulation on AI which, if implemented, will take a risk-based approach to regulating AI based on perceived risk level, as well as introducing requirements around biometrics and registration requirements for some AI products and systems.

Bias is not the only issue surrounding the use of AI – there has been litigation around the globe regarding intellectual property rights in technology created by computers. Courts and patent offices in the UK and the EU have ruled that computers cannot be inventors or own patents, and the UK government has indicated that it will consult on a range of possible policy options, including legislative change, for protecting AI-generated inventions that would otherwise not meet inventorship criteria.

Online harms

Online harms are a topic of growing concern, especially in relation to children accessing harmful content. The UK government plans to introduce an online harms Bill to Parliament later this year, following its White Paper of 2019, which could lead to fines for businesses if they fail to take sufficient steps to remove harmful and illegal content from their websites.

Regulation of platforms

The UK government has created a Digital Markets Unit as part of the CMA to regulate platforms with significant market power, and to improve competition and outcomes for consumers. At the same time the EU has proposed equivalent legislation in the form of its draft Digital Services and Digital Markets Acts. In Australia, the Australian Consumer and Competition Commission (ACCC) has published a report finding that Apple's App Store and Google's Play Store have significant market power in the distribution of mobile apps in Australia, and saying that measures are needed to address this. Separately, the CMA, ACCC and German Bundeskartellamt have issued a joint statement saying they will apply stronger scrutiny to big tech acquisitions and calling on other regulators to do the same.

Platforms are also arguing among themselves – it was reported in April 2021 that Apple had threatened to take Spotify off its App store after Spotify spoke out about what they called Apple's monopolistic behaviour and high fees. Apple and Facebook have also fallen out over Apple's recent changes to ad-tracking.

Selling and advertising online

Another topical issue is that of so-called online influencers and consumers being misled about their links with brands. The UK's Advertising Standards Authority says that it is losing patience with influencers who do not make it clear that their posts contain advertising content. Another major consequence of the pandemic was an increase in online shopping. Not being able to see an item before you buy it increases consumers' reliance on reviews, and fake reviews are a growing problem of interest for regulators, which have worked with Facebook and Instagram to reduce their prevalence.

There are concerns about the online advertising of certain sectors and restrictions are likely for sectors such as foods high in fat, sugar and salt, and gambling products.

Online shopping and logistics

Resilience and scalability are growing priorities for supply chain and logistics tech developers. Automation, blockchain, IoT and AI will be crucial for efficient connectivity across supply chains. Overall, logistics tech will focus on enhancing the agility of supply chains, reducing dependency on workers (e.g. robotic chucks and scan towers) and operating models to ensure that they respond much more quickly to disruptions and rapid fluctuations in demand. Businesses will need invest in some serious tech to solve frustrating issues relating to last-mile delivery and real-time transportation visibility, while also improving customer experience. In the UK and EU, pilots are being carried out to allow drones to deliver parcels, and there is increasing EU regulation of drones, so watch this (air)space!

Transport and autonomous vehicles

While logistics for businesses is a major issue, so is transporting people in a sustainable way, and autonomous vehicles are never far from the news. The Law Commission of England and

Wales has been carrying out a review of the legal framework for autonomous vehicles, and their use as part of public transport networks and on-demand passenger services. It has also been considering issues arising at the boundary between self-driving vehicles and widely-used driver assistance technologies such as cruise control. The use of electric cars will gradually increase as countries start to phase out cars using petrol and diesel.

Cybersecurity

With autonomous vehicles and greater use of drones, (rightly) comes a fear of hacking, and this also applies to connected devices generally, such as smartphones. The UK government plans new legislation to ensure that connected devices are better protected from hacking. Universal default passwords will be banned and manufacturers must implement a means to manage reports of vulnerabilities and to provide transparency on how long, as a minimum, their products will receive security updates.

Immersive technology

2020 was quite a year for immersive tech providers, especially those enhancing remote working experiences. This has led to extended reality technology (XR), which encompasses virtual reality (VR), augmented reality (AR), and mixed reality (MR). Major XR players are poised for significant growth as organisations implement XR technology to enable staff to socialise and work from home in 'simulated' environments. Key sectors to benefit from XR technologies are education, entertainment, healthcare, and manufacturing. Watch out for personalised AR avatars in gaming apps, AR indoor navigation apps (for example, to enhance user shopping experiences and to allow people to avoid crowded areas), XR virtual sporting events (see later), and VR human expression tracking technologies. Another driving factor will be the wider availability of 5G. XR technologies are generally Wi-Fi dependent due to large file sizes, and 5G's ultra-low latency will help to overcome this.

Gaming and e-sports

A related development has been the increase in gaming and e-sports – the Tour de France took place on the virtual cycling platform Zwift and the World Economic Forum says that e-sport will soon be a \$1 billion business with a global audience of over 300 million fans. The potential benefits are clear to see, but there will be issues around the integrity of sport, as well as other areas such as intellectual property and sponsorship rights.

Gambling

Gambling is coming under increasing scrutiny as far as advertising is concerned, but there is now convergence with cryptocurrencies and gambling is under scrutiny generally, especially in relation to loot boxes, which are considered by many to be gambling; and changes to the design of online games to reduce the potential for harm by online gambling. There is a more general overhaul of gambling laws in some countries such as the UK.

Professional services

Professional services businesses are increasingly participating in the tech revolution, including via the use of AI to automate processes and routine tasks such as data analysis. One evolution of this is the use of 'smart contracts' – essentially, computer code that can automatically monitor, execute and enforce a legal agreement. The Law Commission of England and Wales has

issued a call for evidence to conduct a scoping study on the law surrounding smart contracts. There are questions about the circumstances in which a smart contract will be legally binding, how smart contracts are to be interpreted, how vitiating factors such as ‘mistake’ can apply to smart contracts, and the remedies available where the smart contract does not perform as intended.

FinTech

We can expect to see more consolidation of the rather saturated FinTech market, as start-ups are acquired by tech giants. Indeed, FinTech is not always now the crown jewel of emerging tech and competition among start-ups is fierce. For the start-ups that survive, great customer experience will be key, including quick account set-up and quick and efficient ways of proving ID and fulfilling ‘know your customer’ (KYC) requirements. Long gone are the days of filling out paper forms. In order to create personalised and seamless user experiences, FinTechs will reduce manual processes, reduce software dependencies and automate routine tasks. Specific trends will include further leveraging open banking, paperless banking, more AI chat-bots and ‘Banking as a Service’ software. Crypto assets are increasing in significance, with several central banks considering the use of digital currencies. This includes the Bank of England, which has set up a Taskforce to consider a central bank digital currency which would allow households and businesses directly to make electronic payments using money issued by the Bank of England. As the saying goes, if you can’t beat them, join them!

NFTs

This leads us neatly onto NFTs: Non-fungible tokens are the most recent craze from the cryptocurrency world and they have exploded in the past few months. “One-of-a-kind” digital assets, NFTs are the digital answer to collectables and whilst sceptics may not be convinced, there is a reason why investors are parting with their cash and why they are suddenly worth millions, especially in the world of art, music and entertainment.

Brexit

Of course we have not yet mentioned the B word – the importance of a data adequacy decision from the EU regarding the UK is significant. At the time of writing, it looks as if that will be forthcoming, but it is certainly the case that the UK’s exit from the European Union will have and continue to have an impact in tech businesses for some years yet. Unencumbered personal data flows are essential for businesses of all kinds.

So many opportunities ahead!

COVID-19 has disrupted the world, challenging how we live and creating new opportunities. It has shown that bold thinking, swift action and the use of technology are key. That said, proper planning is key, as regulators are increasingly tackling *how* technology is used to ensure that we can all enjoy a fairer and better quality of life.



James Gill, Partner at Lewis Silkin and Co-Head of its Commercial team, provides specialist advice on commercial contracts, technology, outsourcing, logistics, digital commerce, consumer law and data privacy. James has over 25 years' experience and is widely acknowledged as a leading expert in the field of commercial contracts and technology.

James advises clients in a wide range of sectors and has a particular focus on the retail, technology, platform/gig economy, logistics, financial services, FMCG and professional services sectors.

Lewis Silkin LLP
5 Chancery Lane
Clifford's Inn
London EC4A 1BL
United Kingdom

Tel: +44 20 7074 8217
Email: james.gill@lewissilkin.com
URL: www.lewissilkin.com



Victor Timon is a Partner in the Dublin office of the international law firm Lewis Silkin, where he heads up the Commercial, Technology and Data practice of the firm.

He has over 35 years of legal experience having been an in-house counsel and then a partner in leading law firms in London and Dublin. Victor is qualified to practice in both England and Ireland.

He regularly speaks at conferences on e-commerce, technology and data privacy issues in particular.

Victor is a member of ITechLaw, the global association for technology lawyers, which spans more than 60 countries, and helped organise their European Conference in Dublin in 2019.

Lewis Silkin LLP
26 Lower Baggot Street
Dublin 2
Ireland

Tel: +353 1 566 4508
Email: victor.timon@lewissilkin.com
URL: www.lewissilkin.com



Helen Hart has a decade of experience in commercial law, especially advertising and marketing and consumer protection law, both in law firms and as part of in-house legal teams, and has spent another decade as a PSL at Practical Law and Lexis PSL.

Helen now supports the commercial lawyers by keeping them up to date with the latest legal and industry developments, and their implications, as well as writing client briefings and articles on commercial and technology law developments. Helen is qualified as a solicitor in England and Wales, and in the Republic of Ireland, and also has an LL.M. in German law.

Lewis Silkin LLP
5 Chancery Lane
Clifford's Inn
London EC4A 1BL
United Kingdom

Tel: +44 20 7074 8325
Email: helen.hart@lewissilkin.com
URL: www.lewissilkin.com

In a world full of possibilities, we help make the most of what really matters to you – your Ideas, your People, your Future. We pride ourselves on providing solutions to your most complex business challenges, with a pragmatic and human touch.

We have renowned expertise advising creative, innovative and tech-focused businesses across all sectors and our multi-disciplinary teams provide clients with commercial insight and specialist knowledge from a range of legal disciplines including: commercial, IP, data and privacy, corporate, employment, immigration, dispute resolution and real estate.

We work with an international community of clients, helping them achieve their business objectives worldwide through a combination of our own offices, international desks and strategic alliances.

Our people are at the heart of what we do, and are committed to building strong, long-lasting relationships, to providing efficient, high quality and cost-effective legal services, and to constantly challenge ourselves to provide creative solutions.

www.lewissilkin.com



LEWIS SILKIN

Modern Slavery: A 'Wicked Problem' that Requires a Human Rights-Based Approach

Immigration Solutions Lawyers



Anne O'Donoghue



Lihini Konara



Adelaide Falzon



Tiara Dalpadado

Introduction

A Tamil woman was found by paramedics in a puddle of her own urine in an extreme emaciated condition, weighing only 40 kilograms. She had been kept as a slave for eight years. This happened in 2015. This happened in Melbourne, Australia.¹

While many of us may be content to believe that all forms of slavery were extinguished in its historical abolition, or that it is too far away from home to have any relevance in our own social realities, slavery not only survived abolition, but it mutated, thrived, and spread globally and its existence taints our everyday lives – from the clothes we wear, the services we use, the food we eat, to the money we spend. This new form of slavery is known as 'Modern Slavery'.

As a result of the clandestine, lucrative, and seemingly intractable nature of the crime, this global 'wicked problem' requires an international human rights-based approach to be impactful and stamp out the conditions in which Modern Slavery is permitted to thrive.

Human rights are indivisible, inherent, interdependent, and symbiotic. This means that there is no hierarchy between them and that the fulfilment of one right ensures the fulfilment of others, and violation of one right will naturally lead to the violation of others.² A human rights-based approach to policy and law is "a way of empowering people to know and claim their rights and increases the ability and accountability of individuals and institutions who are responsible for respecting, protecting and fulfilling rights".³ The Scottish Human Rights Commission poignantly encapsulates that this involves "raising awareness of what human rights mean and giving people greater opportunities to participate in shaping the decisions that impact on their human rights...and increasing the ability of those with responsibility to respect, protect and fulfil human rights" obligations.⁴

Accordingly, this chapter will look at: the definition and nature of modern slavery as a 'wicked problem'; the difficulties in quantifying the social problem and offer ways in which organisations are innovating to solve this; the importance of human rights-based approaches to difficult public policy challenges; Australia's international and domestic framework; and the ways in which Australia can respond to ongoing and emerging policy challenges as informed by a human rights-based approach.

What is Modern Slavery and Why is it a 'Wicked Problem'?

The term 'wicked problem' describes a difficult, complex, and seemingly intractable policy issue. Rittel and Webber coined the term in their seminal work 'Dilemmas in a General Theory of Planning'

(1973) and identified that policy challenges can be conceptualised as 'wicked problems' when they are highly resistant to resolution because:

- there is a lack of definition for decent forecasting or measurement;
- there is insufficient information and a lack of knowledge;
- plurality of objectives held by multiple stakeholders and actors that may not work cohesively and make it impossible to pursue unitary aims; and
- the problem can be a symptom of another problem.⁵

Craig appropriately recognises that the identification of a challenge as a 'wicked problem' is a "lament over the serious realization that there is no quantifiable, permanent 'reality'...or unmanageable set of rules...against which to judge the success of new social policies or planning efforts" and legislative changes.⁶

'Modern Slavery' is an ill-defined buzzword which attempts to capture the complex contemporary manifestations of slavery worldwide. It can generally be defined as when "control over a person is [exercised] in such a way as to significantly deprive that person of his or her individual liberty, with the intent of exploitation through the use, management, profit, transfer or disposal of that person".⁷

This global plague and immense human rights encroachment, includes barbarous practices such as human trafficking, forced labour, debt bondage, forced marriage, and child exploitation. While there is a lack of paucity in empirical information regarding the extent of Modern Slavery (owing to its clandestine and lucrative nature), the International Labour Organization estimated in 2016 that approximately 40.3 million people are in Modern Slavery, including 24.9 million in forced labour and 15.4 million in forced marriage situations.⁸ This crime is estimated to generate US\$150 billion globally per annum in illicit profits.⁹

The policy challenge posed by article 8.7 of the Sustainable Development Goals – to end modern slavery by 2025 – is one such wicked problem highly resistant to resolution because of the fact that Modern Slavery possesses:

- lack of a clear definition;
- difficulty in measurement due to scope, targeting of hidden populations and lucrative/clandestine nature;
- the numerous stakeholders and lucrative nature of the crime; and
- the way in which Modern Slavery is symptomatic of other policy issues, such as poverty, harmful gender norms, and an absence of the rule of law.

This wicked problem requires an innovative, comprehensive, and united solution that validates the experiences of survivors, victims, and on-the-ground feedback. A human rights-based approach to Modern Slavery is one such innovative response.

Human Rights-Based Approach to Modern Slavery

A human rights-based approach can generally be defined as a “a way of empowering people to know and claim their rights and increases the ability and accountability of individuals and institutions who are responsible for respecting, protecting and fulfilling rights”.¹⁰

Conklin advises that wicked problems require innovation and a systems approach. A systems approach is a problem-solving paradigm which considers the attributes of an entire system in order to achieve the original objective of the system.¹¹ In the case of Modern Slavery, our chosen system or paradigm should predominantly be human rights-based, reflecting the human experiences of survivors and victims of modern slavery and the root causes which rendered them vulnerable to exploitation.

Daniel Vázquez and Domitille Delaplace explain in their essay ‘Public Policies from a Human Rights Perspective’, that “two of the main characteristics of a human rights-focused public policy are people’s empowerment and compliance with international human rights standards. Both aspects are guided by the central element of human rights: human dignity”.¹² Human dignity can be conceptualised as the foundation for empowerment.¹³

The United Nations Sustainable Development Group defines human rights-based approach as a:

“conceptual framework for the process of human development that is normatively based on international human rights standards and operationally directed to promoting and protecting human rights. It seeks to analyse inequalities which lie at the heart of development problems and redress discriminatory practices and unjust distributions of power that impede development progress and often result in groups of people being left behind.”¹⁴

The United Nations Human Rights Office of the High Commissioner provides that a human rights-based approach to data is central to fulfilling the 2030 Agenda for Sustainable Development and leaving no one behind.

This is primarily achieved through:

- participation of affected stakeholders to solve the wicked problem;
- data disaggregation to identify the inequalities which lie at the heart of development problems to ensure that priority is given to people in the most vulnerable situations;
- the ability for affected individuals to self-identify; and
- transparency, accessibility, and collaboration of collected data to help others educate themselves on the policy issue, implement tried and tested approaches, and develop their own approaches.¹⁵

A human rights-based response to Modern Slavery is appropriate to the transnational nature of the crime and the international aspiration. The UN Special Rapporteur on Contemporary Forms of Slavery show that between 62% and 90% of countries in the world have ratified the core international instruments on slavery. Therefore, the Sustainable Development Goals 8.7, to end all forms of slavery by 2025 represents “a [united] set of decisions [agreed upon by all] governments and other political actors to influence, change or frame a problem or issue that has been recognized as being of [global importance] by policy-makers and/or the wider public”.¹⁶

Currently, there is a lack of understanding about what Modern Slavery definitionally entails, how to identify it and how to measure it numerically. Adopting a human rights-based approach to Modern Slavery solves this issue through enabling us to measure this human-based, and therefore distinctively irrational and emotional, phenomenon qualitatively.

Qualitative measurements are well-suited to measuring Modern Slavery and managing risks in the interim because this kind of research is “concerned with understanding human behaviour

from the informant’s perspective” and “assumes a dynamic and negotiated reality”.¹⁷ In other words, a human rights-based approach gives a voice to the individuals who are or who have been affected by Modern Slavery, looking to victims’ and survivors’ points of view and their social reality as a foundation to solve this seemingly wicked problem.

Adopting a human-rights based approach, we must counter the drivers of Modern Slavery in order to effectively combat this wicked policy problem. This would specifically require nation-states, NGOs, transnational networks, epistemic communities, academics, survivors, victims, and all affected stakeholders to work collaboratively to stamp out the conditions in which Modern Slavery is permitted to thrive and empower victims/survivors.

The creation of reliable and consistent data from victims, survivors, and on-the-ground truths on a global united scale, measured and verified through a common set of metrics, will empower government and non-government actors to formulate more effective policy plans to combat modern slavery and implement evidence-based legislative changes.

While this global coordinated effort against Modern Slavery may challenge the traditional notion of Westphalian Sovereignty, “the more state actors shy away from international cooperation to shield their sovereignty, the more often they fail to meet global challenges, losing piece by piece in these failures, the very thing they seek to protect”.¹⁸ In other words, in a world with global challenges, governing responsibly now no longer means sticking to your corner.

Measuring Modern Slavery

As a result of the magnitude of the issue, its broad definition, lucrative nature, and the multitude of layers and drivers of Modern Slavery, it is easy for policymakers to become overwhelmed, particularly as they attempt to quantify a vast human experience and social phenomenon. As explained by Landman in the article ‘Measuring Modern Slavery: Law, Human Rights, and New Forms of Data’ (2020), Modern Slavery is inherently difficult to gauge as a result of the “fundamental problem of unobservability, inherent bias through the use of convenience reporting, and the specification of the concept of modern slavery itself”.¹⁹

The measurement of Modern Slavery needs to overcome these challenges innovatively in order to prevent it from occurring. Human rights-based approaches may promise greater success in policy response to Modern Slavery through aligning sustainable development goal efforts with universal norms and social realities.

Currently, our measurement of Modern Slavery is assisted through the Global Slavery Index. While “applauding their courage in waging what often feels like an impossible battle”, Dr Anne Gallagher has pointed to limitations in the current methodology of measurement used by the Global Slavery Index as ‘complex and in part opaque and incomplete’.²⁰ This is because it is unable to account for the complexities and limitations of quantifying the extent of slavery around the world. Dr Gallagher submitted:

“The fact that there is no agreed definition of “modern slavery” means that recent efforts to measure the size of the modern slavery problem are deeply compromised from the outset. More generally, the methodologies being used to estimate the number of modern ‘slaves’ worldwide, or in any given country, are deeply flawed and there is reason to treat currently available estimates with great caution.”²¹

However, the human circumstances, conditions and qualities which render individuals susceptible to Modern Slavery are “bite-sized” policy issues which nation-states, international organisations, NGOs, academics, transnational networks, businesses, victims, survivors, and all other affected stakeholders can work to improve collaboratively, and measure qualitatively.

In acknowledgment of the importance of utilising a victim- and survivor-centric and human rights-based approach to Modern Slavery, it is fundamental to understand the breeding ground that enables this grotesque phenomenon to exist. Voss identifies that Modern Slavery persists due to environmental root causes, such as:

- poverty;
- under-employment and unemployment;
- displacement, including because of natural disasters, conflict, persecution, or migrating for work opportunities;
- migration;
- discrimination and marginalisation of minority groups;
- gender inequality;
- weak rule of law;
- lack of education and lack of access to information; and
- workplace conditions.²²

The most recent environmental catalyst which enables Modern Slavery crimes to flourish has been the COVID-19 pandemic. The pandemic has exacerbated existing risks and created new risks of modern slavery as it has increased the vulnerability of individuals due to loss of jobs and income, economic instability, and displacement/isolation from family support networks.

Responding to the root causes and lived circumstances which enable Modern Slavery to flourish under the radar is integral to solving this wicked issue. Ms. Emma Germano, President of the Victorian Farmers Federation, poignantly explained this at the Mildura Hearing: “*unless you address the underlying motivation as to why someone allows themselves to be exploited [or find themselves in a vulnerable position to be exploited] no new act put in place and none of the current laws can protect these people from being exploited.*”²³

An example of innovative policy production can be seen through the creation of Delta 8.7 – a global platform for sharing developments in the measurement and analysis of Modern Slavery, led by the United Nations University Centre for Policy and Research, the Alan Turing Institute, the Computing Community Consortium, the Rights Lab at the University of Nottingham, and the Global Security Initiative at Arizona State University and AnnieCannons. This epistemic community “*research, develops and applies AI-powered anti-slavery strategies, directly informed by survivors.*”²⁴

Another example of innovative policy measures can be seen through AnnieCannons – an education provider which empowers survivors of human trafficking and gender-based violence into software engineers, based on the premise that economic opportunity is the key to breaking cycles of abuse and exploitation.²⁵

Australia's Current Response

While Australia conjures up images as a place of golden opportunity, prosperity, and multiculturalism, Modern Slavery is imbedded within our nation and affects every single citizen. Modern Slavery is entrenched in global supply chains and within the goods and services we consume in our daily lives. The Global Slavery Index 2018 estimated that on any given day in 2016, there were 15,000 people living in conditions of Modern Slavery in Australia. This aged statistic is indicative of the lack of paucity in empirical information surrounding this crime.

On 22 April 2021, it was reported by the Sydney Morning Herald that a Filipino woman who was hired by a Sydney couple to clean and care for their family was kept as a slave and forced to work in the couple's grocery store for six to seven days a week with little to no pay between November 2014 and October 2016.²⁶ The couple initially paid for the woman's tourist visa, a single plane ticket and her passport, indicating to her when her visa expired that “*she was unable to return to the Philippines until*

she repaid her initial travel costs.”²⁷ They allegedly said words to the effect of “*if you go back before you pay me back, I know people in the Philippines in the police and higher up who I can hire to harm you or your family if you go home early.*”²⁸ The couple have pleaded guilty to a series of charges relating to their treatment of the victim, including forced labour.

Utilising a human rights-based approach, the Australian Government has an incredibly important opportunity in combating Modern Slavery, both domestically and internationally. This can be achieved through the enactment of legislation that enables vulnerable individuals to empower themselves to claim their rights while dually increasing the ability and accountability of individuals and institutions who are responsible for respecting, protecting, and fulfilling rights.

Australia's definition of ‘Modern Slavery’ is best articulated by Gleeson CJ dicta in *R v Wei Tang* (2008) 237 CLR 1, Para 28:

*“Control of movement, control of physical environment, psychological control, measures taken to prevent or deter escape, force, threat of force or coercion, duration, assertion of exclusivity, subjection to cruel treatment and abuse, control of sexuality and forced labour.”*²⁹

Graeme Innes AM, Australia's former Australian Human Rights Commissioner, poignantly stated in his speech ‘A Human Rights Act for Australia’ (2009), that:

*“A Human rights Act for Australia is bold but faithful; it is faithful to the international human rights principles which we have already signed up to, and importantly it is faithful to the Australian values of respect, dignity, freedom and equality. A human rights act would boldly turn these principles into a law which everyone – including the most vulnerable people in our society – can use to better protect their human rights.”*³⁰

Currently, Australia has ratified a number of international instruments that form part of the international legal framework to combat Modern Slavery, including but not limited to the:

- Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery, ratified 1958;
- Convention against Transnational Organized Crime, ratified 2004;
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, ratified 2005;
- Worst Forms of Child Labour Convention, ratified 2006;
- International Covenant on Civil and Political Rights;
- International Covenant on Economic, Social and Cultural Rights; and
- Convention on the Elimination of All Forms of Discrimination against Women.

Domestically, Australia's National Action Plan against Modern Slavery can be applauded for its human rights-based approach and attempt to work in conjunction with international obligations and aspirations. Australia's National Action Plan attempts to evoke knowledge and empowerment from all actors involved in the crime – victims, survivors, nation-states, civil society, business, unions and academics. Under the National Action Plan 2015-2019, Australia effectively responded to Modern Slavery through:

- comprehensively criminalising codified slavery, slavery-like offences, and trafficking into Division 270 and 271 of Criminal Code Act 1995 (Cth);
- enacting the Modern Slavery Act 2018 (Cth) to harness the transnational nature of big business in the fight against modern slavery. Companies operating in Australia with a turnover of \$100 million per annum are required to submit a risk report of Modern Slavery in their global supply chains;

- creating specialist teams in the Australian Federal Police to investigate claims of Modern Slavery;
- establishing the Human Trafficking Visa Framework to enable victims and witnesses of Modern Slavery to remain in Australia while they participate in criminal investigations; and
- collaborating with stakeholders such as civil society, business and academics at the Biannual National Roundtable on Human Trafficking and Slavery.

The effectiveness and limitations of the Criminal Code, the Modern Slavery Act, and the Human Trafficking Visa Framework will be discussed in turn.

Criminalisation of Modern Slavery

Australia criminalises Modern Slavery practices through Division 270 and 271 of the Criminal Code Act 1995 (Cth). This division codifies Modern Slavery, including practices such as:

- servitude;
- forced labour;
- deceptive recruiting for labour or services;
- debt bondage;
- human trafficking;
- organ trafficking;
- concealing a victim; and
- child sex offences.

These distinctive Modern Slavery crimes possess penalties of up to 25 years' imprisonment. These crimes possess universal jurisdiction, meaning that the laws apply irrespective of whether the conduct occurred in Australia, and whether the victim or the offender are Australian citizens or permanent residents.

Despite this comprehensive codification of Modern Slavery offences, this legislation requires further institutional, human rights-based supports, which validate the distinctive social realities of victims and survivors of this heinous crime.

For example, in the recently reported case of an unlawful Filipino woman being kept as a slave by a Sydney couple, the woman said in her victim impact statement that *"I felt like a slave but I didn't say anything"*.³¹ Similarly, a Tamil woman kept as a slave for eight years by a Melbourne couple, who regularly physically and verbally abused her, desperately asked in an interview with a Federal agent, *"What can I do? Helpless. I came here for money, so I have to obey and do whatever I was told to do"*.³² This is indicative of the way that migration acts as a driver of Modern Slavery, as a result of the social realities faced by victims. For example, their cultural and language barriers, a lack of knowledge of local workplace laws and standards, and in some cases their reliance on their employer for their immigration status.

Modern Slavery is not an indiscriminate crime – it targets vulnerable minorities who may not have the capacity (owing to their own social realities) to claim or even know what their rights are to empower themselves. Victims are poverty-stricken, societally discriminated against because of gender or race, or being illiterate, displaced, and/or desperate. It is the duty of world leaders, international organisations, international businesses, academics, transnational networks, and ordinary individuals around the world to facilitate this empowerment and affordance of basic human dignity. Modern Slavery, at its roots, is about people – asking questions such as 'how' did this person find themselves in this situation, 'how' can their circumstances change to make them less vulnerable to exploitation, and 'how' can I effect this change, is central to understanding and solving this wicked problem.

Effectiveness

Australia could respond more effectively to this through ensuring that the Criminal Code and Australia's migration framework operate in unison. Echoing back to Graeme Innes AM speech on the future necessity for an overarching Human Rights Act, there currently needs to be *"clear legal [symbiotic] statement of the basic rights which the government and public bodies [are] committed to respecting and promoting"* synonymous between legislation.³³

For example, Associate Professor Segrave points to the fact that *"Australia continues to ignore the fact that migration status can impact how and whether women seek support and intervention when experiencing family violence"* and conditions of Modern Slavery.³⁴ She further states that *"our complex migration system is failing victims of gendered violence, who are on temporary visas in Australia"*.³⁵ The social reality of these victims is that they face additional barriers to reporting Modern Slavery and claiming their fundamental human rights. These barriers include harmful gender norms, lack of English-speaking skills, fear of deportation, loss of custody of children, and ineligibility for social support such as Centrelink and Medicare.

Parliament acknowledged this vulnerability in 2016, stating that *"sponsors are often in a position of power with little accountability. It is the sponsor who has knowledge of Australia, its laws and environment. The undertaking to assist the visa applicant financially and in relation to accommodation can be used by manipulative sponsors to control vulnerable visa applicants"*.³⁶

The 'Path to Nowhere' Report, authored by the National Advocacy Group on Women on Temporary Visas Experiencing Violence, explains that:

*"Perpetrators of violence against women on temporary visas use these barriers to maintain power and control and to continue to use violence against women. There is a lack of national data on women on temporary visas experiencing violence and their children."*³⁷

Coercion and control within relationships is typified by perpetrators threatening to report their partners with uncertain visa status to immigration authorities. A review by the NSW Coroner's Court found 99% of intimate partner homicides were preceded by *"coercive and controlling behaviours towards the victim"*.³⁸ While experts agree coercive control needs to be urgently addressed, they warn of stand-alone offences and over-policing through the Criminal Justice System.³⁹ This is an opportunity for migration law to be in line with human rights standards.

Currently, there are significant inequities in Australia's migration legislation which are detrimental to victims/survivors of family violence. Section 4AB of the Family Law Act 1975 defines 'family violence' as *"violent, threatening, or other behaviour by a person that coerces or controls a member of the person's family or causes the family member to be fearful"*.⁴⁰

Australia's migration programme enables people to apply to remain in Australia if a partner relationship breaks down due to violence. The family violence provisions were introduced into the Migration Regulations in response to community concerns that some partners might feel compelled to remain in abusive relationships rather than end the relationship and be required to leave Australia.⁴¹

Despite this regulation, temporary partner visa holders may be at risk of visa cancellation or refusal after the end of an abusive relationship because the applicant must prove that the relationship is genuine. Consequently, the inherent nature of forced marriage would not meet this requirement and, as such, victims of this Modern Slavery practice would become more vulnerable to exploitation and disengaged from support. The Law Council of Australia has suggested broadening the Family

Violence Provision to account for circumstances where the marriage was forced and there is no basis for proving a “genuine relationship”.⁴²

In addition, the Law Council identified that Family Law Provisions are limited to temporary partner and prospective marriage visas and have suggested extending this provision to other visa categories to ensure “consistency in the available protection to victims of forced marriage”.⁴³

Furthermore, to invoke the Family Violence Provision for partner visas, the applicant must be on a substantive visa at the time of lodging their partner visa application. Even if the relationship is genuine and the applicant suffered family violence, an applicant would be barred from invoking this protection. The effect of this being that the opinion of an independent expert about whether the alleged victim had suffered the requisite family violence would never be sought, and the applicant’s valid family violence claims will not be considered.⁴⁴ Not only does this go against the original intention of the provision to protect vulnerable individuals from unsafe situations and relationships, but it disenfranchises people from the universal right to freedom from violence and makes them vulnerable to exploitation.

Australia has shown its commitment to bolstering support for migrants experiencing family violence through the latest Budget. In the Budget that was handed down on 6 October 2020, the Australian Government announced many visa changes for partner visas. Under new legislation, sponsors will need to lodge a sponsorship application which must be approved before a partner visa application can be lodged. In addition, partner visa applicants and permanent resident sponsors will be required to have at least functional English or to have at least made reasonable efforts to learn English. These steps were taken to protect vulnerable migrants from people who commit violent crimes against women and children. The requirement to make reasonable efforts to learn English will also support vulnerable migrant women and families in accessing relevant support systems to obtain assistance. In the new sponsorship form, the sponsor will be assessed against character and will be approved before a visa application can be made. This will ensure that migrants will be aware of charges and convictions of their sponsoring partner and can make an informed decision whether to continue with the visa application. The introduction of these changes can be considered as consistent with the original intention of the Family Violence Provision to protect vulnerable individuals from unsafe situations and relationships.⁴⁵

Furthermore, on 15 April 2021, Direction 79 was revoked and replaced by Ministerial Direction 90 in relation to applying the character test. This new direction provides that primary consideration should be given to family violence and other unacceptable behaviours against vulnerable members of the community when making visa determinations. The direction specifically points to practices such as forced marriage, worker exploitation and serious nonviolent crimes against vulnerable persons. This new direction aligns with Australia’s intolerance for family violence and exploitation of vulnerable persons and behaviours which are drivers of Modern Slavery.

Modern Slavery Act 2018 (Cth)

The Modern Slavery Act 2018 (Cth) stipulates that businesses with an annual turnover of \$100 million or more, submit a Modern Slavery Statement to the Australian Government, which are publicly available through the Modern Slavery Register website (<https://modernslaveryregister.gov.au/>).

Section 1 of the Act provides that this Modern Slavery Statement must:

- (a) identify the reporting entity;

- (b) describe the structure, operations, and supply chains of the reporting entity;
- (c) describe the risks of Modern Slavery practices in the operations and supply chains of the reporting entity, and any entities that the reporting entity owns or controls;
- (d) describe the actions taken by the reporting entity and any entity that the reporting entity controls, to assess and address those risks, including due diligence and remediation processes;
- (e) describe how the reporting entity assesses the effectiveness of such actions; and
- (f) describe the process of consultation with any entities that the reporting entity owns or controls.

Effectiveness

Australia has agreed to implement the United Nations Guiding Principles on Business and Human Rights (UNGP hereafter). The UNGP is a non-binding framework which provides guidance on a human rights-based approach to business and the regulation of business activities by nation-states. The foundational principles indicate that “States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication”.⁴⁶ Governments are expected to ensure access to remedies for victims of business-related human rights harm.

The UNGP also instil a dual expectation on businesses to:

- avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; and
- seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.⁴⁷

Despite the importance in ensuring supply chain transparency and screening procurement practices in global supply chains, non-compliance with the Modern Slavery Act 2018 (Cth) is a common occurrence and met with impunity because there are currently no sanctions conferred on businesses which fail to report. This significantly undermines the potential of the Act in creating a Modern Slavery transnational community.

Australia can look to France and Germany’s proactive response to Modern Slavery in supply lines as a guide for implementation and effectiveness.

The French laws and initiatives are regarded as the strongest and most compliant with the UN Guiding Principles on Business and Human Rights. France prioritises human rights over profits through their establishment of a sanctionable ‘duty of vigilance’ on businesses. This law obliges French businesses to publish due diligence plans that account for the risks of Modern Slavery in the supply chain and empowers victims to report Modern Slavery or non-compliance with the legislation. Non-compliance can be met with fines as much as 10 million euros.

In Germany, a new Supply Chain Act is in the works (*Lieferkettengesetz*) and will enshrine due diligence and a human rights culture, stipulating that companies are held responsible for every step of their supply chains: “from the raw materials to the finished product”, and could face fines of as much as 2% of their annual profits for non-compliance.⁴⁸ The current Finance Minister importantly stated: “In future, it will be clear that ‘Made in Germany’ also means respect for human rights.”⁴⁹

While the intentions of Australia's Modern Slavery Act 2018 (Cth) are in the right place, the reporting requirements represent unique, data-rich sources which could be used in combination with other responses, such as the Human Trafficking Visa Framework and AFP Specialist Investigations Teams, to begin quantifying this wicked problem. The lack of compliance in meeting reporting requirements and the general lack of effort found in some of the turned in reports, could be rectified through:

- incentivising businesses to report through affording tax subsidies to companies who meet reporting requirements;
- sanction businesses that do not comply with reporting requirements satisfactorily;
- the mandatory creation of a Modern Slavery Risk Officer employment position in companies operating in Australia with an annual turnover of \$100 million *per annum*; and
- a detailed federal framework to help businesses identify Modern Slavery and what to do if they find Modern Slavery in their supply lines.

To help businesses identify and respond to Modern Slavery risks, the Australian Human Rights Commission and KPMG Australia are collaborating on the development of sector-specific guides to support businesses manage their Modern Slavery risks and to respond effectively to the Modern Slavery Act 2018 (Cth). Currently, they have published:

- Guide for the Property and Construction Sector.⁵⁰
- Guide for the Financial Services Sector.⁵¹

The Australian Human Rights Commission, supported by the Australian Government Department of Foreign Affairs and Trade, has also partnered with the Vietnam Chamber of Commerce and Industry (VCCI) on a two-year initiative to highlight and respond to the human rights challenges and issues that arise in the apparel and footwear industry in Vietnam, utilising a human rights-based approach. This is indicative of Australia's understanding that the fight against Modern Slavery is transnational and requires a coordinated, multi-party and multi-sector response to be effective.⁵²

Australia recently further proved their resolve against Modern Slavery in global supply chains through their response to products linked to the human rights abuses in China's Xinjiang region. The Australian Government signalled that it would be open to the implementation of tougher sanctions as part of their upcoming review of the Modern Slavery Act, based upon the concerns raised by companies about *"human rights and supply chain integrity in terms of forced labour and other issues in China and in Xinjiang"*.⁵³

Human Trafficking Visa Framework

Trafficking Visa Framework (Visa Framework) enables foreign nationals who do not already hold a valid visa and are suspected victims of human trafficking or slavery to remain lawfully in Australia, and to access the Support Programme.⁵⁴

This framework provides for two visas – a temporary Bridging Visa F (BVF) and a permanent Referred Stay Visa (RSV).

The BVF enables a person assessed by the AFP as being a trafficked person to access up to 45 days of rest and recovery; immediate family members can also be included in this application. A BVF can be granted a second time if additional rest and recovery is required, for a further 45 days. A BVF can also be granted to a trafficked person who is assisting authorities in an investigation or prosecution. Holders of this BVF have the right to work and the right to depart and re-enter Australia so long as their assistance in an investigation/prosecution is ongoing.

The RSV enables a trafficked person who has contributed to or cooperated in an investigation into Modern Slavery and would be in danger if returned to their home country.

Effectiveness

In the Joint Standing Committee on Foreign Affairs, submitters pointed to the fact that this framework is only available to victims who make an active contribution to a criminal investigation. Furthermore, the Human Trafficking Visa Framework does not encourage nor work in conjunction with the social realities faced by victims of human trafficking, such as the fact that it might not be a part of a victim's culture to complain about their circumstances, they may be fearful of authorities, or the exploitation that they are experiencing in Australia is the 'lesser of two evils' of that they would experience in their country of origin.

Anti-Slavery Australia importantly noted in this Committee that its research reveals:

*"Victims of these crimes often suffer from extreme psychological distress as a consequence of the severe exploitative conditions that they have endured. This trauma can be exacerbated by re-victimisation during the criminal investigation process, for example by providing detailed statements and evidence to the police. For this reason, many survivors of trafficking and slavery are unable to continue to assist police in lengthy investigations of offences, even if they are initially able to do so."*⁵⁵

Human Rights-Based Approach?

Singularly, the National Action Plan measures are indicative of great strides in the fight against Modern Slavery. However, it is important to note that in order to be more impactful, and in validation of the fact that Modern Slavery is a wicked problem, these tremendous, singular efforts against Modern Slavery must have an over-arching system which enables them to work in conjunction with one another on a global scale to siphon the creation of reliable and consistent data from victims, survivors, and on-the-ground truths, measured and verified through a common set of metrics. Furthermore, these measures are only effective when they operate within and validate the differing social realities in which Modern Slavery exists.

This is supported by the Law Council of Australia, who submitted to the Australian Government's Public Consultation Paper on the *National Action Plan to Combat Human Trafficking 2020-24*:

*"While Australia has a strong criminal law framework that criminalises the human rights abuses of human trafficking, slavery and slavery-like practices, an overarching strategy accounting for all stakeholders, including governments, companies, civil society and survivors is required, to eliminate modern slavery at its source and provide effective remedies for its victims. These responses should be underpinned by a human rights approach."*⁵⁶

Applying Human Rights-Based Approaches to Emerging and Ongoing Challenges

Australia has forwarded its understanding that it is important to respond to Modern Slavery through a human rights-based lens through the renewal of the *National Action Plan to Combat Human Trafficking 2020-25*. Ministers Dutton and Tudge announced in the 2020-21 Federal Budget that \$10.6 million over five years will be expended to implement the Government's next five-year *National Action Plan to Combat Modern Slavery 2020-25*.

The mission of the plan is “for the Australian Government, working in partnership with others, to actively prevent and combat all forms of modern slavery, wherever it occurs, including by supporting, protection and empower victims and survivors”.⁵⁷ To fulfil this target, the National Action Plan identified five priorities which are human rights-based, including:

1. Prevent Modern Slavery by combatting the drivers of these crimes and empower individuals and groups that are vulnerable to Modern Slavery.
2. Disrupt, investigate and prosecute Modern Slavery by identifying victims and survivors, implementing disruption strategies and holding perpetrators to account through effective investigations and prosecutions.
3. Partner across Government and with international partners, civil society, business, unions and academia to ensure a coordinated response to Modern Slavery.
4. Research by strengthening data collection, and analysis to build the evidence base that supports our response to Modern Slavery.⁵⁸

Remarks from a Global Point of View

Immigration Solutions’ Principal Lawyer, Mrs. Anne O’Donoghue, recently discussed the human rights aspect of Modern Slavery with Mr. Kevin Hyland OBE, the first Independent Anti-Slavery Commissioner in the UK, the author of Sustainable Development Goal 8.7, and a current member of the Council of Europe Group of Experts and Chair of the Institute on Business and Human Rights, who poignantly stated:

“Modern Slavery is not inevitable or something that is too complex to understand. In its most simple terms, it is a crime where someone or an organisation allows others to be exploited, mostly for financial gain. Throughout history slavery has been a concept based on free or cheap labour, sadly that remains the case today. Those who through wilful blindness, deliberately or through neglect profit from this crime need to understand, this is a crime that does not pay. So, the notion of tainted money, and its prohibition, is crucial to end this serious crime of exploitation. Simply put, if you cannot run a business without Modern Slavery in its supply chain, you cannot run a business. When we take this stance, eradication will become closer to being a reality.”

Conclusion

Australia’s efforts to combat Modern Slavery are by no means unimpressive. However, many issues continue to remain despite Australia being a leader in the attempt to prevent Modern Slavery. Adopting a human rights-based approach, we must engage key stakeholders to counter the drivers of Modern Slavery and evoke compliance with legislation in order to effectively combat this wicked policy problem. This involves taking a qualitative approach, listening to survivors’ and victims’ viewpoints and being aware of the social realities faced by potential victims.

As importantly noted by the Law Council of Australia:

*“All stakeholders, including governments, companies, civil society, survivors and their communities, should play a vital role in eliminating modern slavery. Public awareness raising about the problem of modern slavery, including human trafficking is critical to any effective Plan.”*⁵⁹

Empowering individuals and groups who are vulnerable to exploitation and holding accountable the institutions who can be impactful through the consolidation of a culture of respect for human rights, is key to innovatively solving this wicked problem. We watch with great optimism Australia’s future initiatives through the *National Action Plan 2020–2025* in attempting to meet our Sustainable Development Goal 8.7 aspirations.

Acknowledgment

Thank you to Kevin Hyland OBE for providing a quote for this chapter. Mr. Kevin Hyland OBE is the first Independent Anti-Slavery Commissioner in the UK, the author of Sustainable Development Goal 8.7, and a current member of the Council of Europe Group of Experts and Chair of the Institute on Business and Human Rights.

Endnotes

1. Cooper, A., 2021. Melbourne Couple Found Guilty of Keeping a Slave at Home. The Age, [online] Available at: <<https://www.theage.com.au/national/victoria/couple-found-guilty-of-keeping-woman-as-a-slave-in-melbourne-home-20210423-p57lva.html>> [Accessed 26 April 2021].
2. Sur - International Journal on Human Rights. 2021. *Public Policies from a Human Rights Perspective - Sur - International Journal on Human Rights*. [online] Available at: <<https://sur.conectas.org/en/public-policies-human-rights-perspective/>> [Accessed 26 April 2021].
3. Careaboutrights.scottishhumanrights.com. 2021. *What is a human rights-based approach? - SHRC - Care about Rights*. [online] Available at: <<http://careaboutrights.scottish-humanrights.com/whatisahumanrightsbasedapproach.html>> [Accessed 26 April 2021].
4. *Ibid.*
5. Rittel, H.W.J., Webber, M.M. Dilemmas in a general theory of planning. *Policy Sci* 4, 155–169 (1973). <https://doi.org/10.1007/BF01405730>.
6. Craig, Robin Kundis, Resilience Theory and Wicked Problems (December 13, 2020). 73:6 *Vanderbilt Law Review* 1733-1775 (2020), University of Utah College of Law Research Paper No. 376, Available at SSRN: <https://ssrn.com/abstract=3610420> or <http://dx.doi.org/10.2139/ssrn.3610420>.
7. Castan Centre for Human Rights Law. 2012. *Bellagio-Harvard Guidelines on the Legal Parameters of Slavery*. [online] Available at: <<https://www.monash.edu/law/research/centres/castancentre/our-areas-of-work/human-trafficking/bellagio-harvard-guidelines-on-the-legal-parameters-of-slavery>> [Accessed 26 April 2021].
8. International Labour Office, 2017. *Global Estimates of Modern Slavery*. [online] Switzerland: Alliance 8.7. Available at: <https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_575479.pdf> [Accessed 27 April 2021].
9. Oit.org. 2014. *ILO says forced labour generates annual profits of US\$13.10 billion in Africa*. [online] Available at: <http://www.oit.org/africa/whats-new/WCMS_243622/lang--en/index.htm#:~:text=Forced%20labour%20in%20the%20private,US%2413.10%20billion%20per%20year.> [Accessed 27 April 2021].
10. Above, 3.
11. Conklin, *Dialogue Mapping: Building Shared Understanding of Wicked Problems* (John Wiley & Sons, West Sussex, 2006) p. 34.
12. Sur - International Journal on Human Rights. 2021. *Public Policies from a Human Rights Perspective - Sur - International Journal on Human Rights*. [online] Available at: <<https://sur.conectas.org/en/public-policies-human-rights-perspective/>> [Accessed 26 April 2021].
13. *Ibid.*

14. Unsdg.un.org. n.d. *UNSDG | Human Rights-Based Approach*. [online] Available at: <<https://unsdg.un.org/2030-agenda/universal-values/human-rights-based-approach>> [Accessed 27 April 2021].
15. *Ibid*.
16. *UN General Assembly, Transforming our world : the 2030 Agenda for Sustainable Development*, 21 October 2015, A/RES/70/1, available at: <https://www.refworld.org/docid/57b6e3e44.html> [accessed 27 April 2021].
17. Pelletier, S., 2017. *Making the Case for Qualitative Data*. [online] MeetingsNet. Available at: <<https://www.meetingsnet.com/continuing-medical-education/making-case-qualitative-data>> [Accessed 27 April 2021].
18. Hassel, A. (2015) 'Public Policy' in Wright, J. (ed.) *International Encyclopaedia of the Social and Behavioural Sciences*, Atlanta: Elsevier, 2nd ed, pp.569-575.
19. Landman, T. (2020). *Measuring Modern Slavery: Law, Human Rights, and New Forms of Data*. *Human Rights Quarterly*, 42(2), 303-331. <https://doi.org/10.1353/hrq.2020.0019>.
20. Gallagher, A., 2016. *Unravelling the 2016 Global Slavery Index. Part one*. [online] openDemocracy. Available at: <<https://www.opendemocracy.net/en/5050/unravelling-2016-global-slavery-index/>> [Accessed 27 April 2021].
21. *Ibid*.
22. Voss, H., 2020. Implications of the COVID-19 pandemic for human rights and modern slavery vulnerabilities in global value chains. *Transnational Corporations*, 27(2), pp. 113-126.
23. Joint Standing Committee on Foreign Affairs, Defence and Trade, 2017. *Hidden in Plain Sight: An inquiry into establishing a Modern Slavery Act in Australia*. [online] Canberra: Commonwealth of Australia. Available at: <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report> [Accessed 27 April 2021]; Ms Emma Germano, President, Horticulture Group, Victorian Farmers Federation, Committee Hansard, Mildura, 30 October 2017, p. 4.
24. Bliss, N., Boyd, D., Goulding, J., Eckstein, A., Mazumder, A., Harris, B. and Hamid, N., 2021. AI For Good: Using AI to Prevent Modern Slavery, *Human Trafficking and forced child labour*.
25. <https://anniecannons.com/>
26. Chung, L., 2021. Carer forced to work in supermarket, stopped from going out by Sydney couple. *Sydney Morning Herald*, [online] Available at: <<https://www.smh.com.au/national/nsw/carers-forced-to-work-in-supermarket-stopped-from-going-out-by-sydney-couple-20210421-p57l89.html>> [Accessed 27 April 2021].
27. *Ibid*.
28. Chung, L., 2021. Carer forced to work in supermarket, stopped from going out by Sydney couple. *Sydney Morning Herald*, [online] Available at: <<https://www.smh.com.au/national/nsw/carers-forced-to-work-in-supermarket-stopped-from-going-out-by-sydney-couple-20210421-p57l89.html>> [Accessed 27 April 2021].
29. *R v Wei Tang* (2008) 237 CLR 1, Para 28.
30. *Ibid*.
31. Chung, L., 2021. Carer forced to work in supermarket, stopped from going out by Sydney couple. *Sydney Morning Herald*, [online] Available at: <<https://www.smh.com.au/national/nsw/carers-forced-to-work-in-supermarket-stopped-from-going-out-by-sydney-couple-20210421-p57l89.html>> [Accessed 27 April 2021].
32. Cooper, A., 2021. Melbourne Couple Found Guilty of Keeping a Slave at Home. *The Age*, [online] Available at: <<https://www.theage.com.au/national/victoria/couple-found-guilty-of-keeping-woman-as-a-slave-in-melbourne-home-20210423-p57lva.html>> [Accessed 26 April 2021].
33. Innes, G., 2009. *A Human Rights Act for Australia* <<https://humanrights.gov.au/about/news/speeches/human-rights-act-australia>>.
34. Segrave, M., 2019. *How the federal government is migrating responsibility*. [online] Monash Lens. Available at: <<https://lens.monash.edu/@politics-society/2019/11/11/1377635/how-australias-migration-system-is-failing-victims-of-gendered-violence>> [Accessed 27 April 2021].
35. *Ibid*.
36. Migration Amendment (Family Violence and Other Measures) Bill 2016, Bills Digest no. 21, 2016-17, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1617a/17bd02.
37. National Advocacy Group on Women on Temporary Visas Experiencing Violence, 2018. *Path to Nowhere: Women on Temporary Visas Experiencing Violence and Their Children*. [online] Available at: <<https://awava.org.au/wp-content/uploads/2018/12/National-Report-on-Women-on-Tempo...3-compressed.pdf>> [Accessed 27 April 2021].
38. Brancatisano, E. and Elvin, L., 2021. Push to criminalise coercive control in relationships sparks concern for migrant and refugee women. *SBS News*, [online] Available at: <<https://www.sbs.com.au/news/push-to-criminalise-coercive-control-in-relationships-sparks-concern-for-migrant-and-refugee-women>> [Accessed 27 April 2021].
39. *Ibid*.
40. Family Law Act 1975 (Cth) s. 4AB.
41. Department of Immigration and Citizenship, *Media Fact Sheet 38: Family Violence Provisions* (2009) <www.immi.gov.au/media/fact-sheets/38domestic.htm> at 19 January 2010.
42. Law Council of Australia, Public Consultation Paper on the National Action Plan to Combat Modern Slavery 2020-2024 <<https://www.lawcouncil.asn.au/resources/submissions/national-action-plan-to-combat-modern-slavery-2020-24-public-consultation-paper>>.
43. *Ibid*.
44. Regulation 1.23(10).
45. Australian Government, 2020. *Protecting partner visa applicants against family violence*. [online] Available at: <<https://minister.homeaffairs.gov.au/alantudge/Pages/Protecting-partner-visa-applicants-against-family-violence.aspx>> [Accessed 27 April 2021].
46. United Nations Human Rights Office of the High Commissioner, 2011, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy Framework" <https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf>.
47. *Ibid*.
48. Hammerschmid, I., Seibt, C., Aryobsei, M., Scherb, M. and Vesper-Gräse, M., 2021. *Legislative draft of German Human Rights Supply Chain Duty of Care Act: the new standard for corporate human rights duties?* [online] Freshfields Brukhaus Deringer. Available at: <<https://sustainability.freshfields.com/post/102grfi/legislative-draft-of-german-human-rights-supply-chain-duty-of-care-act-the-new-s>> [Accessed 27 April 2021].

49. Made for Minds. 2021. *Germany to implement supply chain law against exploitation* | DW | 03.03.2021. [online] Available at: <<https://www.dw.com/en/germany-to-implement-supply-chain-law-against-exploitation/a-54181340>> [Accessed 27 April 2021].
50. KPMG, Australian Human Rights Commission, 2020. *Property Construction and Modern Slavery: Practical responses for managing risk to people*. [online] Available at: <<https://humanrights.gov.au/our-work/business-and-human-rights/publications/property-construction-and-modern-slavery-2020>> [Accessed 27 April 2021].
51. KPMG, Australian Human Rights Commission, 2021. *Financial Services and Modern Slavery: Practical responses to managing risks to people*. [online] Available at: <https://humanrights.gov.au/our-work/business-and-human-rights/publications/financial-services-and-modern-slavery-practical>.
52. VCCI Uniting Entrepreneurs, Australian Aid, Australian Human Rights Commission, 2021. *Responsible business conduct and the apparel and footwear industry: Guidance for companies 2021*. [online] Vietnam Chamber of Commerce and Industry and Australian Human Rights Commission. Available at: <https://humanrights.gov.au/sites/default/files/vcci_apparel_and_footwear_guidance_2021_eng_web_7.pdf> [Accessed 27 April 2021].
53. Daniel Hurst, 27 April 2021. *Australia examined modern slavery laws amid concerns over products linked to Uyghur abuse*. The Guardian [available online] <<https://amp.theguardian.com/cdn.ampproject.org/c/s/amp.theguardian.com/law/2021/apr/27/australia-examines-modern-slavery-laws-amid-concerns-over-products-linked-to-uyghur-abuse>>.
54. Joint Standing Committee on Foreign Affairs, Defence and Trade, 2017. *Hidden in Plain Sight: An inquiry into establishing a Modern Slavery Act in Australia*. [online] Canberra: Commonwealth of Australia. Available at: <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report> [Accessed 27 April 2021].
55. Joint Standing Committee on Foreign Affairs, Defence and Trade, 2017. *Hidden in Plain Sight: An inquiry into establishing a Modern Slavery Act in Australia*. [online] Canberra: Commonwealth of Australia. Available at: <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report> [Accessed 27 April 2021].
56. Law Council of Australia, Public Consultation Paper on the *National Action Plan to Combat Modern Slavery 2020-2024* <<https://www.lawcouncil.asn.au/resources/submissions/national-action-plan-to-combat-modern-slavery-2020-24-public-consultation-paper>>.
57. Commonwealth of Australia, 2020. *National Action Plan to Combat Modern Slavery 2020-25* <<https://www.homeaffairs.gov.au/criminal-justice/files/nap-combat-modern-slavery-2020-25.pdf>>.
58. *Ibid*.
59. Law Council of Australia, 21 February 2020. *National Action Plan to Combat Modern Slavery 2020-24: Public Consultation Paper* <<https://www.lawcouncil.asn.au/publicassets/46cffbb3-1d59-ea11-9403-005056be13b5/3757%20-%20Public%20Consultation%20Paper%20on%20the%20National%20Action%20Plan%20to%20Combat%20Modern%20Slavery%202020-2024.pdf>>.



Anne O'Donoghue is an Accredited Specialist in Immigration Law with over 27 years of experience. She is the director and principal lawyer of Immigration Solutions Lawyers. Anne has been listed in WWL: Corporate Immigration for 10 consecutive years. In January 2019, she was appointed a member of the IBA's Presidential Task Force on the Refugee Crisis Initiative. On 1 January 2021, Anne was appointed as Immediate Past Co-Chair of the Immigration and Nationality Law Committee of the IBA. Anne served as Co-Chair from January 2019 to December 2020. Anne was the winner of the 2019 Lawyer's Weekly Migration Partner of the Year Award and she achieved a high commendation for the NSW Law Society's Presidents Medal (2019). Anne is also an executive member of the International Law Section of the Law Council of Australia and a member of the Advisory Board to the Professional Ethics Committee of the IBA. In October 2020, Anne was appointed as a Mentor to the University of Notre Dame Australia – Sydney Law School.

Immigration Solutions Lawyers

World Tower Commercial
1304/87-89 Liverpool Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 6432

Email: anne@immigrationsolutions.com.au

URL: www.immigrationsolutionslawyers.com.au



Lihini Konara is a Solicitor at Immigration Solutions Lawyers and team leader of the Family Stream. She has great experience as an Australian immigration lawyer on a wide range of visa categories. She specialises in partner visas and family violence claims. Lihini was admitted as a solicitor in the Supreme Court of NSW in March 2019 and in the High Court of Australia in April 2021. She currently holds a practising certificate in NSW. Lihini is well known for her detailed legal submissions to the Department of Home Affairs and Administrative Appeals Tribunal.

Immigration Solutions Lawyers

World Tower Commercial
1304/87-89 Liverpool Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 6432

Email: lihini@immigrationsolutions.com.au

URL: www.immigrationsolutionslawyers.com.au



Adelaide Falzon is a Paralegal of the Merits Review, Character, MIU & Citizenship Stream at Immigration Solutions Lawyers. Adelaide graduated from Macquarie University in 2020 with Bachelor of Laws (majoring in Public Policy, Law and Governance). She completed her Graduate Diploma in Legal Professional Practice at UNSW in 2021 and expects to be admitted as a solicitor by the NSW Supreme Court on 4 June 2021. She is passionate about human rights-based migration policies and facilitating people in vulnerable circumstances access to just outcomes.

Immigration Solutions Lawyers

World Tower Commercial
1304/87-89 Liverpool Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 6432

Email: adelaide.falzon@immigrationsolutions.com.au

URL: www.immigrationsolutionslawyers.com.au



Tiara Dalpadado is a Solicitor at Immigration Solutions Lawyers and the team leader of the RMCC Stream. She has great experience as an Australian immigration lawyer on a wide range of visa categories. She specialises in merits review applications, ministerial intervention requests and citizenship applications. She also has previous experience working in family stream visas. Tiara is a qualified lawyer in Sri Lanka and in Australia. She was admitted as a solicitor in the Supreme Court of QLD in August 2018. She currently holds a practising certificate in NSW. Being a migrant herself, Tiara developed a passion for helping others with complex migration issues and was drawn to a career in immigration law.

Immigration Solutions Lawyers

World Tower Commercial
1304/87-89 Liverpool Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 6432

Email: tiara.dalpadado@immigrationsolutions.com.au

URL: www.immigrationsolutionslawyers.com.au

Immigration Solutions Lawyers is a leading immigration law firm headed by managing director and principal lawyer, Anne O'Donoghue. The firm has been assisting clients in navigating the different avenues of migration to Australia since 1993. Immigration Solutions Lawyers take a very "hands-on" and collaborative approach with all of our clients. Anne's international presence has enabled Immigration Solutions Lawyers to participate in the development of immigration law both domestically and internationally. Immigration Solutions Lawyers consists of three streams: corporate migration; family migration; and judicial and administrative

merits review. All streams conduct a forensic review of client circumstances and submit quality submissions to immigration authorities.

www.immigrationsolutionslawyers.com.au



Bahrain

Hassan Radhi & Associates



Ahmed Abbas



Sayed Jaffer Mohamed

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

As it stands, and to the best of knowledge, there are no legal requirements that apply to B2B e-commerce in Bahrain which do not apply to non-e-commerce business. We understand that the Central Bank of Bahrain (“CBB”) on 26 June 2019 requested all licensees and listed companies to share their feedback on the draft law on Electronic Commerce by 15 July 2019. However, the law is yet to be passed by the legislator.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Please refer to our answer to question 1.1 above.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

On 19 September 2018, Legislative Decree No. (30) of the Year 2018 Issuing the Personal Data Protection Law (“PDPL”) was enacted. Prior to the enactment of the PDPL, Bahrain had certain provisions in other legislation that governed the concept of data protection. The aforementioned provisions remain enforceable and serve as supplementary provisions to the PDPL and regulate the concept of data protection in specific sectors, such as the:

- Central Bank of Bahrain and Financial Institutions Law 2006, which regulates data protection in the regulated financial activities sector;
- Telecommunications Law 2002, which regulates data protection in the telecommunications sector; and
- Labour Law 2012, which regulates data protection in employee-employer relationships.

Nonetheless, the PDPL serves as the main piece of legislation with respect to data protection issues. Since then, there has

been no domestic law development in the field of data protection, save for an order which awarded the Minister of Justice the powers of the data protection regulatory authority.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Compliance with the PDPL may be perceived as a privacy challenge to fintech, AI and digital health, particularly due to the larger amount and nature of data to be processed by the aforementioned businesses in comparison with other businesses.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

In 2017, the Central Bank of Bahrain introduced a regulatory sandbox aimed at enabling firms to test and develop their products in a virtual space. The opportunity is given to both existing licensees and newcomers, whereby they will be able to test their products in a virtual space in order to mitigate risks to customers and to the local economy.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The Kingdom of Bahrain has a well-defined national cybersecurity framework governed by the General Directorate of Anti-Corruption and Economic and Electronic Security at the Ministry of Interior (“MoI”) for cybersecurity in different sectors such as energy, finance, education, health, and other sectors. On the other hand, the Information & eGovernment Authority (“IGA”) focuses on cybersecurity in the government sector and protecting the government data network through implementing the most advanced technologies in the market, ensuring the quality of information security of all government organisations, conducting several awareness programmes and workshops, as well as providing instant support and response services for government organisations.

The IGA’s vision is to establish a secure cyber-space to safeguard national interests and protect the Kingdom of Bahrain against cyber-threats to reduce risks. The cybersecurity framework includes many initiatives such as the establishment of the National Cybersecurity Committee, which provides a governmental structure for collaboratively addressing cybersecurity

at the highest level of the government. In addition, SafeSurf Bahrain is an initiative by Bahrain's Telecommunications Regulatory Authority dedicated to empowering the citizens and residents of Bahrain and their families with knowledge and information for a safer cyber environment.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

In line with the Kingdom of Bahrain's efforts towards regulating and organising the cybersecurity framework in Bahrain, the government has issued several laws and legislation related to cybersecurity and personal data protection:

- Law No. 30 of 2018 regarding Issuing the Protecting Personal Data Law;
- Law No. 16 of 2014 regarding the Protection of Information and State Documents;
- Law No. 2 of 2017 for Ratifying the Arab Agreement on Combating IT Crimes;
- Law No. 60 of 2014 regarding IT Crimes;
- Decree-Law No. (54) of the year 2018 for Issuance of Letters and Electronic Transactions; and
- Decree of the Prime Minister No. 36 2018 regulating the technical requirements for sending, receiving and updating the electronic records and signatures of the public bodies.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Customers in Bahrain are embracing new technologies as Bahrain has one of the highest internet penetration rates in the Middle East. According to the World Economic Forum report 2018, Bahrain ranked first globally for percentage of internet users and has the highest internet penetration rate at 98%. In an article written by Abdulmonem M. Al-Shirawi and Mansoor Al-Alwan titled *An Investigation Of Factors Influencing Online Shopping: An Explanatory Study In The Kingdom Of Bahrain*, it is stated that the usefulness of online shopping influences customers to shop online, which could be explained by the fact that online shopping saves the time and effort of physical shopping and provides the desired product in a few quick easy steps. In addition, the study shows that customers are concerned about the trust aspect of online shopping. This could be attributed to the practice of selling unauthenticated products in online shops, as well as perceptions of breaching customers' privacy during online shopping.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Most customers are accustomed to both debit card and direct debit transactions. Cash on delivery is slowly fading away mainly due to the unfortunate outbreak of the COVID-19, which saw some e-commerce businesses temporarily disabling their cash on delivery option. The cash on delivery option is not anticipated to return as people are now more accustomed with electronic fund transfer systems.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

We are unaware of home state retailer websites/e-commerce platforms that have expanded into other jurisdictions, and which have publicly available information comparing their performance.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Most e-commerce platforms support Arabic and English only.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

In the study conducted by Abdulmonem M. Al-Shirawi and Mansoor Al-Alwan titled *An Investigation Of Factors Influencing Online Shopping: An Explanatory Study In The Kingdom Of Bahrain*, the study participants highlighted the features of a website through which they would shop online which would influence their decisions, including: website's interface; support; attractive presentation of products; and simplicity of transaction completion. Also, the practicality of the website plays a major role in participants' decisions; thus, websites which are user-friendly and offer guidance through the process are more favourable.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The Covid-19 pandemic saw a noticeable increase in people's reliance on e-commerce in Bahrain. Many local businesses shifted to online platforms, and such change is expected to continue in the future.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In Bahrain, it is possible to file a trademark either directly at a national level or internationally through WIPO via the Madrid Protocol. Trademark registrations are obtained through the Trademark Office at the Industrial Property Office, which forms part of the Ministry of Trade and Industry. Trademarks may be registered in Bahrain in accordance with Law No. 5 of 2014 with respect to approving the unified Gulf Cooperation Council ("GCC") Trademark Law.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

No, there are not.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The restriction on data transfer outside Bahrain, which is further detailed in our answer to question 6.2, is a vital point which should be considered by data centres and cloud providers.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Such matter is governed by Legislative Decree No. 56 of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties ("Cloud Computing Law") and the PDPL. The scope of the Cloud Computing Law applies to providers of cloud computing services to the public through data centres that are physically present in Bahrain and the customers thereof, being foreign or local. The PDPL sets a general prohibition on transferring personal data outside the Kingdom of Bahrain. However, there are exclusions to the general principle whereby the transfer of data outside Bahrain is allowed; they are as follows:

- the Authority shall issue a statement published in the Official Gazette containing a list of countries and territories to which data transfers are permissible. The Authority will issue such list after taking into consideration territories which have applicable data protection legislation and regulations that are deemed satisfactory to the extent which ensures to the Authority the adequacy of the protection provided by the laws and regulations of the said territories; and
- the Authority may authorise the transfer of data on a case-by-case basis after assessing the circumstances surrounding the data transfer. The Authority will mainly consider the size and nature of the data and purposes of the transfer thereof and the data protection laws, regulations or international conventions applicable in the territory to which data will be transferred. The authorisation will be subject to the discretion of the Authority, as the Authority may set specific conditions and time periods for such authorisation.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

One of Bahrain's most valuable geographical features is its direct link to Saudi Arabia. The Customs Affairs developed a 'Single Window' customs clearance system, operated via a streamlined software interface, simplifying the documentation processes and clearance for export-oriented companies, freight forwarders and shipping agents.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Trade agreements play a vital role in laying down the ground

to successfully adopt digital technologies for trade facilitation. Bahrain currently has free trade agreements with 22 countries, an expansion of such agreements may aid in successfully adapting digital technologies for trade facilitation.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

We are unaware of tax incentives of particular relevance to digital businesses in Bahrain. However, there are other tax incentives which apply to most businesses, such as the fact that tax is not payable on private companies' income.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

None.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

Adequate skilled and unskilled labour is available for businesses in Bahrain in view of availability of expatriate employees who make up the bulk of the work force. It is noteworthy that more than 50% of the Bahraini population is non-Bahraini. There is no minimum wage stipulated in the law which may be perceived as an advantage to some businesses. The employment of expatriate workers is subject to obtaining work permits. The Labour Market Regulatory Authority ("LMRA") is the authority which decides on whether work permits may be granted to expatriate employees.

The prescribed working hours are 48 hours per week and shall be eight hours per day. Under no circumstances shall the hours of work exceed 60 hours per week. During the month of Ramadan, hours are limited to six hours per day and 36 hours per week for Muslim workers only.

Employees are entitled to 30 days of paid leave per year after one year of service. Further, an employee is entitled 55 days of sick leave per year. This period is categorised into 15 days of sick leave on full pay, 20 days of sick leave on half pay and 20 days without pay. Sick leave can be accumulated up to 240 days.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

The legislation that covers this matter is Legislative Decree No. 36 of 2012 promulgating the Labour Law of the Private Sector ("Labour Law"). An employee has been defined by the Bahraini Labour Law as every natural person employed in consideration of a wage with an employer and under his

management or supervision. The definition of an employee does not include the factor of presence in the physical premises, therefore the same regulations apply to both employees that work from or away from the organisation's physical premises.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Due to the Covid-19 pandemic, some organisations shifted towards allowing their employees to work from home in order to ensure business continuity. While monitoring the employees' productivity is the main challenge, some organisations are expected to continue allowing employees to work from home given that there are noticeable advantages in terms of cost saving.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The absence of a specific law that governs e-commerce may be perceived as a legal barrier to digital businesses operating in Bahrain.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

The high global percentage of internet users and the high internet penetration rate serve as a notable advantage for digital businesses in Bahrain, as well as the availability of a skilled bilingual ICT workforce.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

We understand that the Central Bank of Bahrain ("CBB") on 26 June 2019 requested all licensees and listed companies to share their feedback on the draft law on Electronic Commerce by 15 July 2019. However, the law is yet to be passed by the legislator. The main areas of focus in the draft law include the requirements which must exist in any e-commerce website and the regulator's authority to block the website of any e-commerce business in case it violates any of its provisions.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Online payments are governed by the CBB Rulebook. Payment Service Provider (hereinafter referred to as "PSP") is a regulated activity which Ancillary Service Providers licensees may undertake. Paragraph AU-1.2.8 of the Rulebook defines PSP as follows:

"Payment service providers may act as an intermediary for the following services:

- (a) Services enabling cash to be placed on an escrow account and all of the operations required for operating an escrow account;*
- (b) Services enabling cash withdrawals from an escrow account and all of the operations required for operating an escrow account;*
- (c) The settlement of the direct debits of payment transactions;*
- (d) Integrating customer delivery channels to enterprises to enable transactions at delivery channels (e.g. ATMs, POS, Interactive Voice Response, mobile, internet); and*
- (e) Interfacing with external networks/institutions (e.g. national switch, VISA, MasterCard), enabling automated exchange of transactions between the enterprise and external networks."*

Furthermore, Rule AU-1.2.10 A states the following:

"When issuing any multi-purpose, electronic or otherwise, pre-paid cards, payment service providers must comply with the following requirements:

- (a) The maximum amount under each individual customer pre-paid account must not exceed BD200;*
- (b) The payment service provider must obtain a bank guarantee of BD100,000 from a retail bank licensed in the Kingdom of Bahrain; instead of the bank guarantee amount required under Paragraph AU-4.1.12;*
- (c) Comply with all the requirements outlined under Module FC (Financial Crime) and Module CL (Client Money);*
- (d) All pre-paid plastic cards must be EMV compliant (chip and PIN and online authentication);*
- (e) Any pre-paid card which is inactive for a period of six months must be placed in a dormant list;*
- (f) All transactions on pre-paid cards must be made through an escrow account with a retail bank in Bahrain."*

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Online service providers must use predefined transaction authentication methods that promote non-repudiation and establish accountability for the transactions. Licensees must establish detailed procedures to effectively identify the person originating electronic funds transfer transactions and for 'call backs' when appropriate to avoid fraud in electronic fund transfers. Failure to comply with such requirement may give rise to legal issues.



Ahmed Abbas has been an associate of the firm since 2016 and received his Bachelor of Laws from the University of Southampton, United Kingdom. He is an ambitious and very active young lawyer with high-quality legal knowledge and research skills. Ahmed proved himself within a short period of time since the commencement of his internship programme with the firm.

He has excellent analytical skills and compelling briefs, motions and arguments. He conducted many legal researches which have benefitted our firm immensely. The legal team is consistently impressed with Ahmed's performance and productivity, which shows his high degree of diligence. He is involved in different tasks including drafting and reviewing contracts, rendering legal opinions for clients, and representing clients before the courts of Bahrain.

His practice focuses on employee benefits and pensions, employment and labour law, insurance and reinsurance, litigation, telecommunications, civil aviation, arbitration and civil law. Ahmed is an Arbitrator registered at G.C.C. Commercial Centre since 2019 and successfully passed The International Federation of Consulting Engineers (FIDIC), Maritime Disputes, and Stock Market Disputes programmes at the G.C.C. Commercial Arbitration Centre. He had important participations in the annual report on doing business in Bahrain 2018–2020, a World Bank Group Flagship Report that compared business regulation for domestic firms in 190 economies, including the Kingdom of Bahrain, and has participated in many legal articles and much research.

Hassan Radhi & Associates

ERA Business Centre
Building 361, Road 1705
Block 317, Diplomatic Area
P.O. Box: 5366
Kingdom of Bahrain

Tel: +973 1753 5252

Email: ahmed.abbas@hassanradhi.com

URL: www.hassanradhi.com



Sayed Jaffer Mohamed is one of the partners at Hassan Radhi & Associates and he is also the Chief Executive Officer at the firm. He is responsible for leading the development and execution of the company's long-term strategy. He is licensed to practise before the Courts of Bahrain, including the Court of Cassation and the Constitutional Court of Bahrain. He received his Bachelor's degree in Accounting as well as a Bachelor's degree in Law from Bahrain University, Kingdom of Bahrain in 1990 and 2006, respectively. Sayed is a CPA holder from the American Institute of CPAs, USA, 2000.

Sayed has been working on a different range of transactions involving banking, capital markets, M&A, insurance and reinsurance and related corporate matters. His practice also focuses on labour law and he represented and advised clients in various employment issues.

Sayed served as Ex-Tender Board Member and Ex-Assistant Undersecretary for Financial and Technical Affairs at the Ministry of Health. Sayed is currently a member of IBA, member of Lex Mundi, member of the internal auditing committee at Bahrain Chamber of Commerce and Industry, Certified Arbitrator at GCC Commercial Arbitration Centre and Accounts Expert before the Ministry of Justice and Islamic Affairs.

Hassan Radhi & Associates

ERA Business Centre
Building 361, Road 1705
Block 317, Diplomatic Area
P.O. Box: 5366
Kingdom of Bahrain

Tel: +973 1753 5252

Email: alsayed.jaffer@hassanradhi.com

URL: www.hassanradhi.com

Hassan Radhi & Associates (HRA) is one of the largest and most reputable and leading law firms in Bahrain and in the Gulf region. The office was founded in 1974 by Dr. Hassan Ali Radhi, the senior partner of the firm who has more than 40 years of legal experience and professionalism in the legal sector, especially in banking and finance and corporate law. The firm has nine partners and eight lawyers, supported by a dedicated and professional administrative team, which provide exceptional legal services locally and internationally in Arabic and English.

As part of the Lex Mundi global network – the world's leading network of independent law firms – HRA is the exclusive member firm in Bahrain that can provide its clients with preferred access to more than 22,000 lawyers around the world with in-depth experience in 150+ countries worldwide, all from a single point of contact. Individually, each Lex Mundi member firm is a leader in its local market.

The firm has been consistently listed among the top law firms in the region by the world's largest legal referral guides, such as: *Chambers and Partners*; *IFLR1000*; *The Legal 500*; and others.

www.hassanradhi.com



Brazil

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados



Fabio Ferreira Kujawski



Lisa Worcman



Paulo Marcos Rodrigues Brancher



Thiago Luís Sombra

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

E-commerce platforms must comply with certain specific regulations that do not apply generally to non-e-commerce platforms. Specifically, the Internet Act applies to online companies and imposes certain obligations to collect user data (such as IP address, time and date of connections) when browsing ecommerce platforms. This information must be stored for six months and law enforcement authorities may request the disclosure of this data in certain circumstances, upon a valid Court order.

From a tax standpoint, B2B e-commerce transactions are subject to specific tax reporting obligations. On interstate sales carried out on B2B transactions, the purchaser is obliged to collect the difference between the interstate VAT rate and the intrastate VAT rate (“ICMS DIFAL”) to the state of destination of the purchased goods.

In addition, the following obligations must be met:

- **E-commerce – Purchase and Sale Model**
If the e-commerce carries out online sales, appearing as the seller of the goods purchased through the digital platform, the transactions will be subject to ICMS (Value-Added Tax on Sales of Goods and Services). The e-commerce will have to: (i) enrol in the various states where it operates; (ii) collect ICMS upon the sales; and (iii) comply with tax reporting obligations.
- **E-commerce – Intermediation Model**
If the e-commerce platform acts as a service provider, an intermediary between the purchaser and the seller, merely connecting these parties to enable the sales through the digital platform, its revenues shall be subject to ISS (Service Tax). In this case, the e-commerce will need to (i) enrol with the municipal taxpayer number, (ii) collect ISS, and (iii) file ISS tax reporting obligations.

Finally, the National Classification of Economic Activities (CNAE) codes adopted by e-commerce platforms must mirror the activities effectively carried out (whether intermediation or merchant), and the terms of service shall expressly and clearly define the platform’s business purpose.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In addition to the comments in the question above, B2C transactions may likely be subject to consumer laws (specifically, the Consumer Protection Code, “CDC”), except for specific circumstances.

Under the CDC, the e-commerce operator shall:

- ensure correct, clear and accurate language regarding the offer, which shall be presented in Portuguese language;
- avoid deceptive practices and misleading advertising;
- explain limitations and risks associated with the use of the product or service;
- provide adequate and clear information about the platform’s services;
- inform its business name, tax registration number and physical or virtual address; and
- disclose all transaction costs.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The Brazilian Data Protection Law (“LGPD”) came into effect in September 2020. Administrative sanctions for violation of LGPD are effective as of August 1, 2021.

Private right of action is allowed under LGPD and other Brazilian authorities (including consumer protection authorities and public prosecutors) may investigate possible violations of the law.

The Brazilian Data Protection Authority (“ANPD”) was formally constituted in November 2021 and is currently setting out its regulatory priorities. ANPD published its “2021-2022 Regulatory Agenda”, which defines the agency’s priorities for the period, which include: data subjects’ rights; criteria for administrative sanctions; international transfers; breach reporting obligations, etc.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

For organisations acting in regulated sectors, one of the challenges is how to best reconcile existing sector-specific privacy regulations with the LGPD. Some examples follow below:

- **Fintech:** The scope of the “protection of credit” legal basis to justify data processing by fintechs. Another challenge is how to reconcile the “express consent” requirement under banking secrecy law with the other lawful basis contemplated in LGPD.
- **Retail:** The scope of the legitimate interest legal basis, given the current lack of specific guidance. Legitimate interest is probably the most commonly adopted legal basis for online marketing activities.
- **AI:** The scope of transparency requirement for AI solutions and how such platforms will enable request for review of automated decisions.
- **Digital Health Sector:** As a measure to fight the COVID-19 pandemic, Brazilian health authorities have approved several rules allowing remote diagnosing and remote medical assistance, and it is uncertain as to whether such regulations will continue to exist in a post-pandemic world.

The ANPD will have to align with other Brazilian regulatory agencies and authorities to seek a coordinated and harmonised environment to foster privacy compliance and sanctioning efforts.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The Brazilian Central Bank (“BCB”) issued special regulations for fintechs in 2018, allowing regulatory sandboxes for testing innovative solutions.

The Brazilian Government has also authorised the foreign participation of up to 100% in the capital stock of online credit fintechs (direct credit companies – *sociedade de crédito direto* (“SCD”) and peer-to-peer lending companies – *sociedade de empréstimos entre pessoas* (“SEP”)). As a consequence, foreign investors are no longer required to ask for a specific presidential authorisation to join SCD and SEP. Additionally, credit fintechs are now able to fund their operations with resources from the Brazilian Development Bank (“BNDES”).

In April 2021, the Ministry of Science, Technology and Innovation published the “Brazilian Strategy for AI”, which will serve as a basis for the development of AI regulation in Brazil at a Federal level. The Strategy aims to balance ethical use of the technology while boosting research and innovation in the AI sector.

As for digital health, the Ministry of Health has published the “2020-2028 Digital Health Strategy”, which aims at modernising hospital management systems, implementing electronic medical records, among others.

Some federal laws confer tax incentives to foster R&D and innovation.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The E-commerce Decree establishes that e-commerce businesses shall adopt security mechanisms for the processing of payment transactions and the use of consumers’ data.

The LGPD determines that data processing agents shall implement technical and organisational security measures able to protect personal data from unauthorised access, and unlawful or accidental situations of destruction, loss, change, communication or any other unlawful processing activity, but does not

provide further details on how to comply with such obligation. Under certain circumstances and timeframe, data controllers may also be required to communicate the ANPD and the affected data subjects in case of data breaches that could create relevant risk or damage to the data subjects.

Further guidance from ANPD is expected on this matter.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

There are cybersecurity regulations applicable to financial institutions, payment institutions and other entities authorised to operate by the BCB that establish strict cybersecurity requirements, as well as specific requirements for engaging services of data processing and storage and cloud computing by the regulated entity. Such rules are enforced by the BCB (for instance, by requesting that cybersecurity incidents are reported to BCB), and regulated entities may be subject to administrative sanctions in case of non-compliance with such rules.

The Securities and Exchange Commission (“CVM”) has approved regulations that impose information security requirements for entities regulated by CVM (such as market intermediaries, fiduciary administrators, etc.), rules for contracting relevant third-party service providers and data incident notification requirements. Regulated entities may be subject to administrative sanctions in case of non-compliance with such rules.

The Brazilian Telecommunications Agency (“ANATEL”) has also approved regulation on cybersecurity requirements applicable to telecommunications networks, critical infrastructure and service platforms. Such regulation is enforced by ANATEL and regulated entities may be subject to administrative sanctions in case of non-compliance.

As for the public sector, in February 2020, the Brazilian President approved the “National Cybersecurity Strategy” or “E-cyber”, which is a soft law that aims to provide general guidance and policies from the federal government in the 2020-2023 timeframe.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Studies conducted in 2018 evidenced that Brazilian consumers had a cash-friendly attitude, particularly when purchasing goods/services of up to USD 100, mainly because: (a) Brazil was the ninth country in the world with the highest number of unbanked individuals, corresponding to more than 48 million people; and (b) more than 45 million individuals did not have internet access.

The number of individuals with internet access is annually growing and Brazilian consumers are embracing e-commerce purchases, particularly as a result of the Covid-19 pandemic, which made online sales grow more than 73.88%. Studies show that the number of unbanked Brazilians has been decreasing (hampering cash transactions as people are keeping social distance in the pandemic) and the emergency financial aid provided by the Brazilian government (which, as a rule, requires a bank account to be released).

Therefore, the cash culture is being continuously impacted and this should help spread other payment methods through the larger Brazilian population.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The Brazilian market currently adopts a variety of payment methods, including credit and debit cards, QR codes, near field communication (“NFC”), payment slips, cash, among others. Studies show that there is still a strong cash culture in Brazil, particularly for purchasing inexpensive products, mainly because: (a) a significant number of Brazilians is still unbanked and have limited internet access; and (b) transactions executed through credit and debit cards or other traditional payment methods may be more expensive for final users comparatively to cash payments, as payment fees apply. In turn, credit cards are more frequently used for purchases of goods/services of higher amounts.

In 2020, BCB has regulated and launched the operation of the Brazilian instant payment scheme (“Pix”), and the number of users is constantly growing. Consequently, even though Brazil still has a strong cash culture, debit and credit cards are also widely used and Pix is gaining momentum, contributing to the digitalisation of the Brazilian payments’ ecosystem.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Most Brazilian e-commerce platforms tend to perform better if located in Brazil. High shipping costs make the products sold by Brazilian online platforms not financially appealing to consumers located in other jurisdictions.

E-commerce platforms are usually characterised as intermediaries and if the platforms are not located in Brazil, their intermediation revenues will be subject to a 40% tax burden considering an international remittance. The pandemic has significantly boosted the use of e-commerce platforms, which incentivised the most successful players to establish local operations.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Brazil is the world’s largest Portuguese-speaking nation and the only one in the Americas. Most of Brazilian e-commerce platforms present content in Portuguese language only. The minority of them allows switching to another language, which means that their focus and almost exclusive targets are Brazilians.

Even large and very successful e-commerce portals do not seem to target other regions through their Brazilian website. Internationalisation efforts of Brazilian e-commerce entities typically involve establishing new operations in foreign jurisdictions.

4.5 Are there any particular web-interface design concepts that impact on consumers’ interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Considering that almost 80% of Brazilians make purchases via

smartphones, they tend to prefer online interfaces that are easy to navigate and are adapted to smartphone screens.

Brazilians typically do not like pop-up boxes and registration forms that require a lot of information before the purchase order. Generally, displaying too many pop-up boxes, requesting a user to fill in long registration forms and redirecting the user to standalone payment platforms interfere with the completion of online sales.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Studies show that the Covid-19 pandemic spurred digital and financial inclusion and made it a top priority. They revealed that: (a) 46% of consumers increased online purchases during the pandemic; (b) 7% of individuals bought online for the first time; and (c) more than 40 million people have been bankrolled in recent months.

Researchers found that about 95% of the interviewees stated that they will continue to shop online even after social distancing restrictions are lifted. Thus, it seems that the pandemic will indeed have a lasting impact on consumer behaviour, especially in terms of online shopping.

E-commerce platforms enjoyed a 41% increase in their 2020 turnover in comparison with 2019.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In Brazil, only by means of registration with the Brazilian Patent and Trademark Office (“INPI”) may a brand be formally protected against misappropriations and different sorts of third-party infringement. To proceed with the registration process, the interested party must go through the administrative proceeding established by the Industrial Property Law and further regulated by INPI’s rules. Once a brand is duly registered, its holder is entitled to the right to use it, at its own discretion, with exclusivity in Brazil, as well as to prevent others from using it without the holder’s authorisation.

Although the right to use the brand with exclusivity can only be guaranteed through brand registration with the INPI, companies that use an unregistered brand have the right to repress unfair competition, such as the use of similar brands by their competitors aiming at damaging the companies’ reputation and/or business, in addition to creating confusion among establishments or products/services offered to customers.

The process of enforcing an online brand also involves registering the domain name with the competent authority (“Registro.br”). If a registered domain name violates a holder’s brand, such holder may challenge the legitimacy of the domain name through the Internet Conflicts Administrative System (SACI-Adm).

Trademark infringement may also be repressed in courts by filing: (a) a lawsuit to declare the nullity of a trademark registration, in case the INPI has registered a trademark that infringes the plaintiff’s brand; and (b) a lawsuit for abstention of use and damages, aiming to cease the alleged unlawful practice. In both cases, the plaintiff may request preliminary injunctions (such as search and seizure of counterfeit items, immediate removal of a domain name, etc.).

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

The Industrial Property Act provides that, under certain conditions, a registered brand can be used by third parties without its holder's prior consent. However, if such use is made with the intention of causing any kind of harm to the brand or taking advantage of its reputation, it is possible to resort to the judicial measures mentioned under question 5.1 above.

Another restriction that has an impact on online brand enforcement is the fact that Brazil adopts the "first come, first served" model for domain names' registration. It means that, if a domain name is available, any interested party may register it. Registro.br does not conduct a previous analysis on potential infringement to third-party rights and, therefore, even a domain name that notoriously reproduces or, in a manner, violates an online brand might be registered.

The e-commerce operator may be held liable under the Industrial Property Act, Copyright Act or Software Act to the extent that, by its own actions or negligence, it breaches third parties' patent rights, trademarks, copyrighted materials and software.

Enforcing local laws on online service providers has always been a challenge for law enforcement authorities, notably when the service provider does not have a local presence in the jurisdiction where the services are available. However, if the platform's operator (incorporated offshore) has a Brazilian affiliate/subsidiary, there is a risk that the latter could be held liable by the Brazilian authorities and the Judiciary for the activities carried out in Brazil by the overseas platform's operator.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Despite some controversy in Brazilian courts, we believe that consumer laws should not apply to cloud/data center service agreements, which means that the parties have more freedom to determine and agree on the contractual conditions that will govern the parties' relationship.

As a general rule, the agreement should contemplate:

- description of the services;
- service level agreements ("SLAs");
- possibility of engaging outsourced services;
- description of the technical and organisational security and safety measures to be implemented by the service provider (especially if the service provider processes personal data);
- audit rights;
- termination clauses (including penalties if service levels are not achieved); and
- indemnity clauses, especially in case of IP infringement, breach of confidential obligations and third party claims.

Only in circumstances where the customer is an individual or could be considered vulnerable *vis-à-vis* the service provider may courts determine that consumer laws should apply. When this happens, provisions dealing with foreign governing law, arbitration, disclaimers or limitations of liability may not be enforced as written in the service agreements.

On a final note, there are some sector-specific requirements for engaging relevant cloud and data centre services that must be considered, such as those applicable to financial institutions regulated by the BCB.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Broadly speaking, Brazilian law imposes no general data residency requirements, except for government contracts in some circumstances. In any event, because the Internet Act and the LGPD have an extraterritorial effect, companies carrying out data processing activities in Brazil or offering services to individuals located in Brazil are subject to Brazilian laws, regardless of the location of the servers/data centres.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The Unified Foreign Trade Portal ("Single Portal") is the main initiative of the Brazilian Government to digitalise and diminish the paperwork within international trade. It was created to integrate the systems of all bodies involved in international trade, to simplify the upload of customs documents and provide detailed information regarding the stage of each trade operation.

The Brazilian IRS launched a new blockchain technology (bConnect) that is adopted by Mercosur customs to ensure the authenticity of information exchanged between them about exporting companies and cross-border operations.

As for the private sector, there are several technologies that have been adopted by Brazilian companies to reduce costs on trade, transportation and storage, as well as new technologies such as Optical Character Recognition ("OCR"), Radio Frequency Identification ("RFID"), QR codes, among others.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Digital technologies require large investments in IT and personnel to operate online systems. Most Brazilian organisations report increasing difficulties in recruiting IT professionals. Brazilian universities are still lagging behind when compared with those of developed nations and more incentives to foster public and private partnerships in R&D would certainly be welcome.

For purposes of cross-border trade, digital technologies must interoperate with other countries' platforms in a fast, efficient and secure manner. Establishing harmonised security information requirements, connectivity, interoperability of e-payment systems, intellectual property management and consumer protection (such as in relation to counterfeit goods or biosecurity standards) could also contribute to a healthier international trade environment.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Despite not being a tax incentive only destined to digital

business, the withholding income tax exemption on dividend distributed by a Brazilian company to Brazilian or foreign shareholders is a significant advantage for the local incorporation of entities to explore digital businesses in Brazil. This exemption applies to the tax on foreign exchange transactions (“IOF/FX”) when dividends are distributed abroad as well.

The main tax incentives for the tech industry are:

- Law 11,196 (“*Lei do Bem*”) and Law 8,248 (“*Lei da Informática*”) set forth tax benefits to encourage the development of the IT and telecom industry by Brazilian companies.
- The Brazilian law provides specific tax incentives granting exemption or reduction on the federal Tax on Cross-Border Transactions (Import Duty or “II”) on certain imported goods. That is the case of federal import duty exemption called “*ex-tarifário*”, under which the import duty rate can be reduced to 2% or 0% on the import of capital goods or computer and telecommunication equipment without equivalent in Brazil and their parts and components.
- Benefits on Value Added Tax (“ICMS”) may apply to digital businesses depending on the rules of each state.
- Some municipalities provide benefits on Tax on Services (“ISS”) and Real State Property Tax (“IPTU”) in view of the envisaged technology project and acquisition of land.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Brazil has a complex tax system. Historically, one of the main discussions is based on the characterisation of a digital merchandise and its effect on indirect tax that apply to those transactions. In Brazil, services are generally subject to ISS and sale of goods are subject to State VAT (“ICMS”). Given the fluid nature of most digital products, many court debates take place as to determine which of those taxes should apply. The Supreme Court recently decided that software licensing is subject to ISS and not ICMS.

This is one of the reasons which has led the Brazilian National Congress to be actively debating bills for tax reform. The three most relevant proposals of tax reform in the National Congress foresee the unification of different taxes into one, the creation of new taxable events (such as intangibles, licensing/assignment of rights, digital services).

In parallel, National Congress has also echoed a growing concern regarding the creation of digital service taxes (“DSTs”). These bills are based on the argument that the OECD does not yet have a conclusive understanding of the proper tax treatment of big techs, which has led to the creation of DSTs by several countries and Brazil should not “be left out” of this context. In this regard, most big techs have local entities and, consequently, pay taxes as all other Brazilian entities, such as IRPJ/CSLL, Social Contributions, ISS or ICMS; added by payroll taxes, import taxes, among others. Therefore, unlike other jurisdictions that impose DSTs as a way of taxing big techs that generate revenue without a physical presence in their territory, Brazilian DSTs emerge as an additional tax, teamed up with other complex and existing taxes, not only applicable to foreign companies, but also to those formally incorporated in Brazil.

In Brazil, there is a tax type for burdening a specific economic sector (as known as “CIDE”). This tax has a specific requirement: the taxpayer facing the burden must ultimately benefit from the proceeds of the collected amount by the Government. Brazilian law already provides that amounts paid, credited, delivered, employed or remitted abroad as royalties or compensation

for technical services and technical and administrative assistance services must be subject to the CIDE tax at a fixed rate of 10%. However, there are plenty of discussions – on whether CIDE is constitutional and whether it should levy on the import of technical services that do not imply the transfer of technology to Brazil – which will be ruled by the Brazilian Supreme Court soon.

Brazilian transfer pricing rules can also be an issue since it has its own standards to define the parameter price, which do not match the OECD standards.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

The basic rules governing labour relationships in Brazil are established in the Federal Constitution and in the Brazilian Labor Code (“CLT”). The Brazilian labour legislation is supplemented by other federal laws, labour and social security statutes, court precedents and collective bargaining agreements.

The CLT defines an “employee” as an individual who renders services: (a) to another individual or company on a continuous basis; (b) under the direction of such individual or company; and (c) for compensation. Outsourcing is allowed, and the outsourced worker must render service through a company, which will employ and pay the workers.

The basic employment rights are: minimum wage; limited working hours; annual paid vacation; Christmas bonus; and an Unemployment Severance Fund (“FGTS”). There are other rights that are provided in accordance with specific situations (for instance, hazardous or unhealthy conditions of work allowance).

Other benefits may be offered spontaneously by the employer, or may be negotiated in collective bargaining agreements, such as meal vouchers, lodging, education, profit sharing, etc.

Brazilian employment law applies to the work performed in Brazil, even when the employee works for a foreign company or the employee is a foreigner.

Generally, outsourcing is less burdensome if compared to a regular registered employee, but companies should be mindful to avoid treating outsourced workers as regular employees, as labour risks may kick in.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

The Brazilian employment law provides specific rules on teleworking, whether the employee is an external worker (i.e., working outside the company's premises because of the nature of the employee's activities, like vendors), or a teleworker.

Teleworking is considered when the work is performed predominantly outside the company's premises (at least, more than 50% of the working hours) by using information and communication technologies. The company and employee must sign a written agreement specifying the activities and responsibilities of the employee. The employment agreement may stipulate the parties' obligations in this work mode. As a rule, the employer is not required to pay any expenses that the employee

may incur for working remotely, unless collective bargaining agreements state otherwise. The employer is required to provide instructions to the employee about occupational safety and health matters.

In principle, employees working remotely are exempt from working hour control as they are not entitled to overtime.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Companies tend to adopt teleworking on a massive scale, despite the end of the Covid-19 pandemic. Mobility and flexibility are key elements to retain talents. Hiring, retaining and training processes must be reviewed, since they were shaped based on personal interactions. Finally, considering that employees working a teleworking shift are exempt of overtime, mental health must be one of the company's top priorities.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The key legal barrier facing digital businesses in Brazil is that, when operating a digital platform, several areas of law are potentially implicated, so digital businesses must navigate consumer, tax, data privacy, labour, intellectual property, competition and advertising issues, which may establish different requirements or compliance standards depending on where the platform's operator is incorporated or where the consumer is located. In this scenario, and considering that Brazil adopts a civil law system, digital businesses are required to keep up with a variety of complex laws and regulations, at Federal, State and local levels.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Brazil is a digitalised market with a growing interest in technology. However, a significant part of the Brazilian population is still foreign to the formal banking system, and consequently less exposed to international products that require credit card payments. Therefore, operating digital business locally, avoiding contract with foreign parties (which implies in foreign exchange transactions and a heavy tax burden), allowing for simplified payment methods and communicating with the Brazilian population at large, is an important commercial advantage. These reasons have fostered local presence of foreign digital players.

In addition, the high tax rate for remittance of service fees also encourage foreign entities to establish locally.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

- **Privacy:** In January, 2021, the ANPD published its "2021-2022 Regulatory Agenda", which provides for the regulation of a range of issues in the LGPD that are yet to be formally defined, such as providing detailed rules on: data processing carried out by start-ups; data subjects' rights;

the applicability of administrative sanctions; international data transfer, etc. ANPD has also announced a public consultation for regulating the mandatory notification of security incidents under the LGPD.

- **Fake News:** The Bill 2,630/2020 ("Fake News" bill) is currently under analysis of the Brazilian National Congress and its goal is to prevent the dissemination of disinformation on the internet. Because it establishes some controversial measures for combating disinformation and increasing transparency on the internet, the Bill has been fiercely debated in Brazil by different players.
- **Anti-Piracy:** In 2020, the National Anti-Piracy Council of the Ministry of Justice ("CNCP") published a soft law called "E-commerce Best Practice Guide" ("Guide") with the purpose of implementing repressive and preventive measures against the offering and sale of counterfeit products in e-commerce/marketplace platforms. One of the guidelines aims at preventing the sale of illegal products in the online platforms. The CNCP expects that e-commerce/marketplace platforms and IPR holders adhere to the Guide, for purpose of cooperating with the Brazilian authorities on the adoption of anti-piracy measures and developing a healthier competitive digital business environment.
- **Consumer:** Brazil has a fairly protective legal framework that affords significant consumer rights. Online entities must be mindful about all such rights, as we have very active consumer protection authorities and associations that closely monitor compliance with consumer rights. Individual claims may be filed in administrative courts at Federal, State or municipal levels, and it is easy and inexpensive to do so. Global online platforms report a considerably higher number of consumer claims in Brazil than that of other countries.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The Brazilian online payment sector is subject to specific laws and regulations, such as the Law 12,865/2013, which regulates payment scheme settlors and payment institutions, as well as establishes BCB as the authority to regulate and supervise them.

BCB's regulation currently admits and regulates four types of payment institutions in Brazil, which may be subject to specific rules and licensing requirements: (a) issuers of electronic currency; (b) issuers of post-paid payment instruments; (c) acquirers; and (d) payment initiation service providers.

After such entities are licensed to operate by BCB (as applicable), they must comply with a variety of payments regulatory requirements and implement certain policies, controls and procedures, particularly involving a risk-based approach towards anti-money laundering and combating the financing of terrorism, banking secrecy, replying to clients' complaints, cybersecurity, reporting obligations, risk management, ombudsman, internal audit, compliance, etc.

Non-compliance with the applicable legal and regulatory requirements may be deemed a crime and/or an administrative offence subject to a punitive administrative proceeding initiated by BCB. Upon conviction, certain sanctions may be applied to the regulated entity and officers.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Online payment providers that intend to operate in Brazil must consider that payment services are subject to specific legal and regulatory requirements, including the need to obtain BCB's licence to operate under certain circumstances.

After licences are granted by BCB (if applicable), regulated entities must implement policies, controls and procedures required by the applicable rules, and certain corporate events may be subject to BCB's authorisation, including changes involving corporate control, qualified equity interest, by-laws, etc.

The provision of financial services is subject to different laws and regulations, and non-compliance with the applicable rules may be deemed a crime and/or an administrative offence.

For this reason, online payment providers may not offer and provide financial products/services to their consumers directly, but may act as banking correspondents of financial institutions or develop other partnership structures in line with the regulation in force.

The Brazilian payments regulatory framework has recently been enhanced and updated in line with international trends, including to discipline and implement sandbox initiatives, instant payments and open banking. Other relevant matters are currently under public hearing with BCB, such as environmental, social and corporate governance rules (ESG), foreign exchange and prudential requirements applicable to online payment providers. Up until now, cryptocurrencies remain an unregulated matter by BCB.



Fabio Ferreira Kujawski's practice focuses on technology, data protection, telecom, intellectual property, media and entertainment, with expertise in transactional and regulatory matters affecting these industries. He advises companies on a wide-range of corporate matters, domestic and cross-border. Fabio is considered a leading professional in his areas of expertise by all legal directories, including Chambers and Partners, Legal 500, Who's Who Legal, LACCA, among others. He is the co-author and editor of the book *Legal Trends in Technology and Intellectual Property in Brazil* (2014). He is an officer of the Brazilian Association of Information Technology and Telecommunications Law.

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Alameda Joaquim Eugênio de Lima
447 - Jardim Paulista
São Paulo
Brazil

Tel: +55 11 3147 2795
Email: kujawski@mattosfilho.com.br
URL: www.mattosfilho.com.br



Lisa Worcman practises with a focus on consulting in the technology and entertainment sectors. Her tax practice is specialised in consulting, transfer pricing, applicability of international treaties, M&A transactions and the structuring of foreign company business in Brazil. She has broad knowledge in IP, copyright, the rules of the Brazilian National Telecommunications Agency and those of the Brazilian Agency of National Cinema. She is a member of the Special Commission on the Freedom of the Press of the São Paulo State Branch of the Brazilian Bar Association (OAB/SP) and of the Special Tax Law Commission, also at OAB/SP. She is vice president of IASP in the New Technologies committee.

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Alameda Joaquim Eugênio de Lima
447 - Jardim Paulista
São Paulo
Brazil

Tel: +55 11 3147 8484
Email: lisa.worcman@mattosfilho.com.br
URL: www.mattosfilho.com.br



Paulo Marcos Rodrigues Brancher specialises in technology, intellectual property and telecommunications. He holds a PhD and is a professor of Commercial Law and Technology Law at São Paulo Catholic University. Paulo was a visiting researcher at Fordham University, New York and at Universidad de Castilla - La Mancha (Spain). He is a current member of the International Technology Law Association, and was a member of the Board of Directors, chair of the Data Protection Committee and chair of the Membership Committee for Latin America. He was the chairman of the Brazilian Association of Technology and Communications Law. Author of the books: *Software Contracts, Competition and Intellectual Property Law, Industrial Property Licensing Contracts*, and co-author of the books: *The Protection of Personal Data in Brazil, Current Challenges in the Law of Competition and Current Challenges of Economic Regulation and Competition*. He is co-editor of the law journal *Business Law in the Digital Economy*.

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Alameda Joaquim Eugênio de Lima
447 - Jardim Paulista
São Paulo
Brazil

Tel: +55 11 3147 4684
Email: pbrancher@mattosfilho.com.br
URL: www.mattosfilho.com.br



Thiago Luís Sombra's practice focuses on technology, compliance and public law, and on anti-corruption investigations handled by public authorities and regulators, data protection, cybersecurity and digital platforms. He also advises clients in cases related to state-owned companies, administrative sanctioning procedures, concessions, bids and administrative contracts in general. He served as State Attorney of São Paulo before the Federal Supreme Court and Superior Court of Justice (STJ), and as a clerk at the STJ. He is currently a professor at the University of Brasília, and a member of the International Association of Privacy Professionals and the International Committee of Digital Economy of the International Chamber of Commerce. He is certified by the International Association of Privacy Professionals with CIPP/Europe and author of the book *Fundamentals of Privacy Regulation and Personal Data Protection* (2019).

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
SHS, Q 6 Conjunto A, S. 1901 - Bl. C - Asa Sul
Brasília
Brazil

Tel: +55 61 3218 6010
Email: thiago.sombra@mattosfilho.com.br
URL: www.mattosfilho.com.br

Mattos Filho is structured to provide services to clients in different legal areas in a co-ordinated and integrated manner, working in multidisciplinary teams whenever necessary. This work dynamic allows the firm to deliver tailor-made solutions to its clients, thereby enhancing the understanding of their business and making it a valuable partner. Mattos Filho is a leader in approximately 30 different legal practice areas and works continuously to ensure that all these practices become benchmarks for the market. Creation of industry groups and market niches, combined with the firm's comprehensive knowledge of the market and clients' business needs, are examples of its efforts to keep it at the forefront in providing legal services. The firm represents domestic and foreign companies, financial institutions,

investors, multilateral agencies, investment funds, pension funds, insurers and reinsurers and non-profit organisations.

www.mattosfilho.com.br

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

Canada

ROBIC LLP



Jean-François Normand

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

In Canada, e-commerce is regulated at both the federal and provincial level, with legislations varying widely on certain specific issues, while being generally consistent in their treatment of the enforceability and formation of online contracts. The general rule is that the provinces regulate internal commerce, and the federal government the interprovincial or international commerce. Thus, businesses must often deal with multiple regulatory regimes. Canadian Courts are currently using the foreseeability test to determine if Canadian, provincial or a foreign legislation applies.

It should also be noted that except for the province of Québec which independently enacted its *An Act to Establish a Legal Framework for Information Technology*, most provincial legislation governing electronic commerce and electronic transactions has been enacted and modelled on the *Uniform Electronic Commerce Act* (the UECA), which was adopted in 1999 by the Uniform Law Conference of Canada. The UECA was designed to provide provinces with consistent legislation that implemented the principles of the *United Nations Model Law on Electronic Commerce*.

E-commerce entities and non-e-commerce entities are generally treated similarly, particularly with respect to provincial and federal business registration and other registration requirements. However, e-commerce entities are subject to a wide range of laws and regulations affecting various aspects of their operations, such as taxes, export control, marketing, etc., some of which will be discussed more in depth below. Key principles governing the activities of B2B e-commerce entities in Canada include the following:

- **Electronic Document Validity:** As a general principle, information or documents, such as contracts, will not be considered invalid or unenforceable if they are solely in an electronic format. Any legal requirement to provide documents in writing, will be satisfied if such document is in an electronic form, as long as they remain accessible and can still be subsequently used. In addition, if there is a legal requirement to provide information to another person “in writing”, the recipient must be able to retain the information and not just be shown the information on a one-time basis or otherwise. Furthermore, electronic signatures

will be generally deemed as satisfying the legal requirements if, at the time an electronic signature is affixed to a document, (a) it is reliable to identify the person making it, and (b) there exists a reliable association between this electronic signature and the electronic document.

- **Consent:** Both click-wrap and web-wrap agreements are enforceable under Canadian law if the three requirements of an agreement (that is, (a) an offer, (b) an acceptance, and (c) a consideration) are met.
- **Electronic Agents:** Under provincial legislations, an electronic agent means a computer program, or any other electronic means, used to initiate an act or to respond to an electronic document or act without a review by an individual at the time of the response or act. Electronic agents are permitted to form contracts with a person. However, such transactions will be unenforceable against such person if (a) the person makes a material error in the electronic document or information used in the transaction, (b) the electronic agent does not give the person an opportunity to prevent or correct that error, (c) the person promptly notifies the other party on becoming aware of the error, and (d) where consideration is received as a result of the error, the person takes reasonable steps to return such consideration or destroy the consideration (if so instructed), and the person has not used or received any material benefit or value from the consideration.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In addition to the above, B2C e-commerce activities are also governed by federal and provincial laws regulating a wide range of commercial activities, including those related to consumer protection.

Many provincial laws incorporate obligations and requirements drawn from the *Internet Sales Contract Harmonization Template*, which was endorsed in 2001 as a common template to cover contract formation, cancellation rights, credit card chargebacks and information provisions. Some of those obligations and requirements are the following:

- **Disclosure:** Before a consumer enters into an agreement over the Internet, the supplier shall disclose certain information to the consumer. The following information must be accessible by the consumer and the consumer must be able to retain and print it:

- the name of the supplier and, if different, the name under which the supplier carries on its business;
- contact information that the consumer can use to contact the supplier (telephone number, address of the premises from which the supplier conducts business, fax number, email address, etc.);
- a fair and accurate description of the goods and services to be supplied to the consumer, including the technical requirements, if any, related to the use of the goods or services;
- an itemised list of the prices at which the goods and services are to be supplied to the consumer, including taxes and shipping charges;
- a description of each additional charge that applies or may apply, such as customs duties or brokerage fees, and the amount of the charge if the supplier can reasonably determine it;
- the total amount that the supplier knows would be payable by the consumer under the agreement, or, of the goods and services to be supplied during an indefinite period, the amount and frequency of periodic payments;
- the terms and methods of payment;
- the currency in which amounts are expressed, if it is not in Canadian currency;
- any other restrictions, limitations and conditions that would be imposed by the supplier; and
- various other information on the delivery or performance of the goods or services depending on the nature of such goods or services and on the provisions of the agreement.
- **Acceptance:** A supplier must provide the consumer with an express opportunity to accept or decline the agreement and to correct errors immediately before entering it.
- **Copy:** A supplier must deliver to the consumer who enters into an online agreement a copy of the agreement in writing within 15 days after the consumer enters into the agreement, which copy must contain certain prescribed information to meet this requirement.

It should also be noted that provincial consumer protection legislation also permits, in most provinces, for consumers to repudiate executory contracts for an established “cooling off” period.

That being said, as obligations vary from one province to another, legal counsel should be consulted prior to the operation of any e-commerce business in Canada.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Canadian privacy laws have taken a comprehensive approach to regulating public and private sectors. Like e-commerce, both federal and provincial governments regulate data protection, although the legislations’ core are generally very consistent from one jurisdiction to another, as they are all based on the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

As Canada’s adequacy status with the European Union – which allows data to flow freely between the EU and Canada – needs to be reviewed, Canadian legislative bodies are introducing new regulations in order to adapt to the new European

standard regarding the protection of personal data. In that respect, the province of Québec introduced, on June 12, 2020, a new bill that is very similar to the GDPR in Europe. The bill is still under review and is expected to be adopted by the end of 2021. The federal law (the *Personal Information Protection and Electronic Documents Act* (PIPEDA)) was also amended at the end of 2020 by the introduction of Bill C-11 to enact the Consumer Privacy Protection Act.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Fintech, retail, AI and digital health organisations deal with an immense amount of sensitive data, which are used as a resource. However, the current Canadian data protection legislations have yet to fully adapt to the reality of data being a resource. Privacy laws designed to protect individuals from exploitation are framed around what were once distinct and siloed issues. While Canadian privacy laws continue to provide important protection, notably as they are technologically neutral, there remain important questions about how to ensure these frameworks have the appropriate approach to maintain the trust of citizens in an increasingly data-fuelled world. This necessity for an appropriate balance – namely between ensuring the right flexibility and agility for innovation, while maintaining user buy-in and security – is a key theme for Canadian organisations.

Moreover, with such sensitive data, fintech and health organisations need to have strong identification and authentication procedures. Unfortunately, Canada is behind in this matter, as the main identification and authentication procedures still use the Canadian social security number.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The Government, as well as privacy, financial and other regulators, launched regulatory sandboxes to assist organisations in dealing with innovation, privacy and regulatory issues. Privacy regulators, known as privacy commissioners in Canada, are also frequently publishing and updating guidelines on the matter.

In 2019, the Government of Canada published the *Digital Charter*, and decided to move forward with an ambitious, aspirational principled approach to digital and data transformation in Canada. The principles are the foundation for a *Made in Canada* digital approach that will guide Canadian policy making and actions, while helping to build an innovative, people-centred and inclusive digital and data economy.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

In Canada, there are no regulations on digital security and encryption that apply specifically to e-commerce. Generally, the security warranties are provided by contract, although encryption may be essential for compliance with industry standards, more particularly for financial institutions or third-party payment processors. It should however be noted that, in most cases, an electronic transaction implies the exchange of personal

information, and privacy laws provide that minimum safeguards must be implemented to protect such personal information from unauthorised reproduction and disclosure. In that regard, businesses are required to implement appropriate security safeguards to protect personal information – most importantly for B2C e-commerce – from unauthorised use, disclosure, or access.

More generally, Canada's anti-spam legislation (CASL) specifically prohibits, in the course of commercial activity, the alteration of an electronic message so that the message is delivered to a different destination or as an addition to the one specified by the sender.

CASL also governs the installation of software in the course of commercial activities when the software provider or the target computer is located in Canada. It forbids the installation of viruses and spyware by prohibiting:

- the installation of software on another person's computer without the express consent of said owner or an authorised user of the computer;
- causing software to be installed without consent; and
- the installation of software that can communicate with other electronic devices without the consent of the owner or authorised user.

In November 2020, the *Digital Charter Implementation Act*, 2020 was proposed with the aim to modernise the framework for the protection of personal information in the private sector by providing clear rules for e-commerce businesses. Its impact is yet to be known as of today, but it should be considered when doing e-commerce in Canada.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Many cybercrimes such as hacking, denial-of-service attacks, phishing, infections of IT systems (ransomwares or similar tools), possession or use of hardware, software or other tool to commit cybercrime, identity theft or identity fraud, electronic theft, unsolicited penetration testing or any other activity that adversely affects or threatens the security, confidentiality integrity or availability of any IT system, infrastructure, communication network, device or data are specifically prohibited by the *Criminal Code of Canada*, RSC 1985, c C-46.

Regarding personal health information, three provinces (Ontario, New Brunswick, and Newfoundland) have specific provincial laws providing additional protection to such data.

The Financial Consumer Agency of Canada (FCAC) monitors the financial industry's compliance with several codes of conduct. Those codes can handle various topics such as banking services to seniors, debit card services, or bank relations with small and medium-sized businesses.

More specifically, the *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework* provides guiding principles to businesses in developing a consumer protection framework for electronic commerce while clarifying the responsibilities associated with the service.

Financial institutions or third-party payment processors can also decide to comply with the *Payment Card Industry Data Security* (PCI-DSS) standards.

Finally, the voluntary federal certification programme, CyberSecure Canada, can certify small and medium-sized businesses that voluntarily meet security benchmarks.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Canadian consumers have long embraced e-commerce, whose share of the overall retail market continues to grow steadily year after year. According to Canada Post's 2020 Canadian e-commerce report, "eight out of ten Canadians shopped online in 2019". With the COVID-19 pandemic, *eMarketer* observed an ecommerce growth of 20.7% in 2020, which totalled an amount of 52.04 billion dollars and represents 8.1% of all retail. As is the case in other jurisdictions, however, the most active online shoppers are concentrated in certain segments of the population and it is estimated that 60% of all online purchases in Canada are made by just 18% of online shoppers, mostly the lucrative HYPER+ segment.

According to a recent report by Absolutnet, across Canada, one dollar in 10 is traded digitally in the retail space – almost on par with the US (10.7%).

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

According to J.P. Morgan, cards (both debit and credit) are the principal way to pay online in Canada, being used for 62% of all e-commerce transactions. Moreover, Canadians are more likely to pay for products outright via debit rather than taking on debt, as evidenced by the number of debit cards in circulation, which is more than two times higher than the number of credit cards. Digital wallets are also increasingly popular among Canadians, accounting for 18% of the payments market.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Canadian retailers with an online presence have traditionally performed well with Canadian consumers but have also had to compete with foreign platforms as Canadians typically make a large number of cross-border transactions, especially through U.S.-based platforms. Politics, trade and exchange rates are important factors that influence shopping habits of Canadians and, as of recent years, Canadian retailers have benefited from a decline of cross-border shopping by Canadian consumers.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

E-commerce firms should be aware that more than 200 languages are spoken in Canada, with English and French being the two official languages. Most e-commerce platforms operating in Canada will be in both English and French. As J.P. Morgan points out, e-commerce platforms that offer multiple languages are likely to find success within this highly multilingual country.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

To our knowledge, the preferences of Canadians are not specifically different from those of other online consumers and, like them, they prefer clean, intuitive and frictionless web-interfaces. Furthermore, since apps are the dominant mobile commerce channel in Canada, used for 51.4% of all transactions completed on handheld devices, clear images and typefaces are essential when selling to Canada's online shoppers via mobile platforms.

It is worth noting that according to a recent report by Eagle Eye, Canadian consumers also respond very well to social selling and are more likely to visit social media platforms before making a purchase than US, Australian or UK consumers.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Due to the COVID-19 pandemic and the numerous lockdown periods, recent studies and reports have observed a change in consumers' shopping habits, as 48% of Canadians have reported shopping more often online during 2020, according to a recent report by Payments Canada. Moreover, as the situation is still developing, this appears to be a long lasting trend, as reported by Canada Post, since 93% of Canadians "plan to either do more online shopping or the same amount".

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

There is no general process for online brand enforcement in Canada. Brand owners can instead rely on applicable laws, specifically including trademark infringement actions, unfair competition, and/or passing-off actions to prevent the illegal use of their brands.

Regarding domain names, brand owners can rely on the complaint mechanisms made available under the *Uniform Domain Name Dispute Resolution Policy* (UDRP) or the *Uniform Rapid Suspension System* (URS) whose goal is to resolve disputes arising from abusive registration of domain names. For .ca domain name, the CIRA's Dispute Resolution Policy (CDRP) is available.

Tools provided by private platforms can help brand owners prevent the infringing use of their brands by notifying them of any use on said platforms and providing specific tools to enforce their trademarks (e.g. Amazon Brand Registry or Alibaba Intellectual Property Protection Platform).

As an alternative, Canadian rights holders of registered trademarks can submit a request for assistance with the Canada Border Services Agency to take pre-emptive steps against counterfeit products.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

For online brand enforcement, unavailable WHOIS information or lack of any contact information for infringing parties is the most recurring restriction, making it difficult to find a way to

contact or locate said infringing parties. Domain name registrars, including the Canadian Internet Registration Authority (CIRA), generally do not provide the personal information of registrants or automatically hide personal information to comply with the requirement of PIPEDA.

Regarding .ca domain names, requirements related to the eligibility of a complainant such as the Canadian Presence Requirements for Registrants (CPR) can make it difficult for foreign brand owners to use this mechanism for an abusive .ca domain name. On the other hand, the territorial nature of trademarks can also be a restriction to their enforcement when the infringing activities are occurring outside of Canada.

Private platforms may not always respond to a complaint if, for example, the infringement is ambiguous. The tools provided also have a very specific purpose and force brand owners to rely on more traditional mechanisms provided notably by trademark or competition legislation.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Since organisations that collect or process personal information have significant statutory responsibilities with respect to the collection, use and disclosure of personal information, it is essential that their relations with any third parties providing processing or hosting services are consistent with such responsibilities. Most notably:

- **Level of Protection:** Any organisation dealing with a third-party data processor must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party (e.g. the European GDPR and Schrems II). This obligation is normally met by entering into robust and detailed agreements and/or through other non-contractual oversight and auditing mechanisms. Such agreements should contain provisions relating, *inter alia*, to security, standards of performance, burden of compliance, breach detection and record keeping, incident response and notification.
- **Transparency:** The customers or individuals from whom an organisation collects personal information should be made aware of such organisation's practices when handling personal information, including the use of any third party-owned data centre or cloud provider. Such practices must also be consistent with the original purpose of collection for which a consent was obtained.

In addition to the privacy implications, there are also several other important elements to consider when entering into an agreement with a third-party provider, such as capacity, data portability, subcontracting and assignment, indemnification and liability, effects of termination, etc. Since data is often at the heart of digital businesses, these issues need to be carefully considered.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

At the federal level, PIPEDA does not require that servers or data centres be located in Canada. However, some provincial laws contain restrictions that require some data, mostly public sector data and certain types of personal information, such as health-related information, to be stored in Canada.

Even in cases where federal and provincial laws do not prevent the storage of data on servers or data centres located in other jurisdictions, it should be noted that: (a) data transferred outside of Canada becomes subject to the laws of the jurisdiction where it is stored; and (b) the organisation collecting data will ultimately remain fully accountable and responsible for that data, which means that the legal implications of such transfer should always be closely considered.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The *Advance Commercial Information Definition* (ACI) is an initiative of the Canada Border Services Agency which aims to provide officers with electronic information registered for all commercial cargo entering Canada. ACI has been in effect since 2004 for marine shipments and 2006 for air shipments. The ACI is inspired by its American equivalent, the Container Security Initiative (CSI).

The goal is to provide the necessary information to officers to help them identify any health, safety, or security issues with imported commercial goods prior to moving the freight in Canada, in order to efficiently highlight high risk goods while expediting the transfer through customs of low-risk goods.

This new process helped eliminate important delays at cargo points of entry and helped achieve faster clearance of freight.

It does require some coordination prior to shipping to ensure that an acceptance is received at the necessary date. Required documents and information (i.e. commercial invoice, bill of lading, dispatch level information, etc.) must be provided in advance so that clearances and eManifests, a special barcoded manifest, can be set up before the goods are shipped to Canada.

The final step to implement ACI is the eManifest for highway shipments and is currently under development with involvement from private and public actors.

The new *United States–Mexico–Canada Agreement* (USMCA) also includes specific provisions related to digital trade. More particularly, it prohibits customs and other charges on digital products, but parties may continue to impose internal taxes or charges. It also commits the parties to collaborate and establish necessary and appropriate safeguards regarding cybersecurity, consumer protection, or spam prevention.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Regarding trade facilitation, the increasing amount of data collected and analysed is raising concerns for customers and businesses, notably with recent issues regarding the lack of data confidentiality and potential cybersecurity threats.

To ensure proper adoption of digital technologies, it is also necessary to provide capital investments and resources to ensure that the technology is appropriately matched with the specific needs and requirements of its users. It must also be implemented properly by transferring the necessary knowledge and skills while creating documentation and resources to ensure that it is being used efficiently.

Cooperation between the stakeholders is necessary and the states must agree on standardised rules, principles or standards, otherwise it could create disparities between digital systems, making the successful adoption of digital technologies even harder in the context of trade.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Until July 1st, 2021, foreign businesses and operators of online platforms that sell intangibles or services to Canadian residents were not required to collect and remit federal and provincial sales taxes if they do not carry on business in Canada within the meaning of the *Excise Tax Act*. Since July 1st, 2021, foreign businesses and operators of online platforms will have to register and collect federal and provincial sales taxes, but only if their sales to Canadian residents exceed CAN\$30,000 over a 12-month period.

In Canada, an e-commerce business can deduct from its revenues a capital cost allowance for computer software and website development costs. Digital businesses could also, in some cases, benefit from investment tax credits, including the Scientific Research and Development Investment Program. These tax incentives come in three forms: an income tax deduction; an investment tax credit (ITC); and, in certain circumstances, a refund.

Furthermore, incentives may be provided at the provincial level, such as Québec's "Development of E-Business Tax Credit" which is available to a corporation that carries out its activities through an establishment in Québec.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

One of the most contentious issues is whether a digital business has a sufficient nexus to Canada to be subject to taxation. Such nexus would normally derive from corporate residency or the carrying on of a business through a permanent establishment. Authorities are now using elements such as servers and computer equipment as a link between Canada and a corporation's activities.

Another source of dispute is the characterisation of income, that is whether it qualifies as business or property income. This distinction is highly relevant, as the tax rates applicable differ between the two types of income and because property income can be subject to withholding taxes.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In Canada, labour and employment legislation depends primarily

on the sector of activity in which a business is active in. Even if most employers fall under provincial jurisdiction, certain industries are of federal jurisdiction, and as such, only federal labour laws may be applied, unless otherwise specified.

Even if the labour legislation in Canada provides for several different employment statuses (e.g. full-time, part-time, seasonal, fixed-term, indefinite term, etc.), Canadian legislation tends to put the emphasis on the employer-employee relationship rather than the status in itself. Thus, provincial acts normally apply solely to employees and exclude independent contractors or self-employed individuals.

However, the definition of “employee” is not standard across jurisdictions, hence, the protection and benefits included in the labour and employment laws will only benefit employees, in accordance with its corresponding meaning, and will not be available for independent contractors, among others.

Consequently, if a business wishes to resource work in Canada, the practical and legal considerations will depend on, first, whether its activities fall under provincial or federal jurisdiction and, second, the province in which said resource will work.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There is no specific regulation in place in Canada relating to telecommuting. Certain provinces, such as Ontario and Manitoba, have incorporated the concept of “homeworker” or “home work” within their employment standards legislation to provide individuals falling in that category with certain specific protections or obligations. Nevertheless, most provinces view telecommuting as a form of work where regular labour and employment legislation are still applicable. Despite some uncertainties surrounding its true application, provincial laws on occupational health and safety are also applicable when telecommuting.

Thus, the main regulation of telecommuting in Canada remains the internal policies instilled by employers and the agreements they concluded with their employees. Such policies will inherently depend on the employer's expectations and activities, but should focus on IT, confidentiality and privacy issues, work hours, among others.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

As the situation is still unfolding, the long-term effects of the COVID-19 pandemic on the employment law implications are difficult to assess. However, ADP Canada observed in a recent survey that 45% of Canadians “would prefer to work remotely at least three days a week and more than one quarter would prefer to work flex hours”. Even if, according to the same survey, 44% of Canadians do not believe there will be drastic changes in the workplace after the pandemic, 25% of Canadians do believe their employers “will offer more flexible work options”.

This could potentially indicate that, if it is not already done, more companies will benefit from having telecommuting policies to help accommodate their employees and promote a more agile workforce.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

In general, Canada is recognised as having particularly stringent consumer protection laws with which any B2C digital business should be familiar. In addition, compliance with the French language requirements necessary to operate in the province of Québec (which represents approximately 22.5% of the Canadian population) is sometimes perceived as onerous or burdensome by some digital businesses. Lastly, digital businesses must navigate a wide array of evolving federal and provincial laws and will need to invest time and resources to understand and comply with the everchanging legal landscape.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

In addition to the fact that there are no specific registrations applicable to e-commerce, digital businesses operating in Canada have access to a fast-growing, wealthy and tech-savvy market. Since the federal and provincial governments recognise the importance of digital transformation and wish to invest in the data-driven economy, there are a number of economic initiatives that promote the development of digital businesses as well.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The legislation and regulations currently in place for those operating digital businesses in Canada tend to primarily focus on consumer protection, advertisement and competition law. However, with the ever-increasing use of data (and the correlated data breaches), regulators are currently focussing on privacy and the protection of personal information. An important reform of this sector is expected in the country as new bills such as the Bill C-11 on a federal level and Bill 64 in the Province of Québec were introduced in 2020.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

In Canada, Payments Canada was established by the *Canadian Payments Act* to operate two core payment clearing and settlement systems: (a) the Large Value Transfer System (LVTS), an electronic funds transfer system that settles large-value and time-critical Canadian dollar payments; and (b) the Automated Clearing Settlement System (ACSS) for clearing of retail payments, including: direct deposits, imaged paper, point-of-service and online debit transactions, pre-authorised debits, and ABM transactions. Payments Canada establishes the rules relating to such clearing and settlement systems. Digital businesses may also be required to comply with certain rules of the payment network requirements pursuant to their agreements with network participants.

Card issuers, payment processors and other participants of the credit and debit card networks must also comply with the *Code of Conduct for the Credit and Debit Card Industry in Canada*.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The Canadian government is currently looking to implement a new retail payments oversight framework. This new framework would apply to a wide range of transactions, and a number of currently unregulated payment industry participants would be regulated as payment service providers (“PSPs”). As of the latest discussion paper published, this framework would mainly contain: (a) registration requirements for PSPs; (b) liability rules shielding end-users for losses as results of unauthorised transactions; and (c) various operational and safeguarding requirements for PSPs to protect end-users. Even if this retail payments oversight framework has yet to be adopted, it will considerably shake up the current framework applicable to payment service providers and should be closely monitored by digital businesses acting as such.

Acknowledgment

Special thanks to Vincent Caron, Vanessa Deschênes, Jules Gaudin, Élisabeth Lesage-Bigras and Julie Robert for their collaboration in the drafting of this article.



Jean-François Normand is a senior associate in the Emerging Technologies Group at ROBIC and specialises in Intellectual Property and Information Technology law. He has acquired an expertise in the high-tech industry and is involved in advising companies – from the early-stage start-ups to giant tech companies – on issues related to e-commerce and digital marketing, data protection, privacy and cybersecurity, online brand enforcement, digital health and medical devices, digital entertainment, and open source licensing.

ROBIC LLP

2875 Laurier Boulevard
Delta 3 – suite 700
Quebec (Québec) G1V 2M2
Canada

Tel: +1 418 780 0962
Email: jfnormand@robic.com
URL: www.robic.ca

Founded in Montreal in 1892, **ROBIC** is internationally renowned and has earned a reputation for excellence in intellectual property in Canada. Our firm has offices in Montreal and Quebec City, and includes a team of over 180 support staff and highly qualified professionals specialising in intellectual property and business law.

ROBIC is one of the most prolific filers of trademarks in Canada and has earned an undeniable reputation for the quality and number of patents filed annually. Our experienced litigation lawyers, some of whom are recognised by their peers as being the best intellectual property litigators in the country, represent our clients in all courts, including the Federal Court of Canada, provincial courts in Quebec, the Supreme Court of Canada, as well as specialised administrative tribunals.

In addition to offering all intellectual property services, ROBIC has an experienced team of business lawyers whose expertise is recognised internationally.

For 125 years, ROBIC has been the benchmark for the protection and commercialisation of intellectual property rights and other intangible assets in Canada.

www.robic.ca

ROBIC
1892

Cyprus



Xenia Kasapi



George Economides

E & G Economides LLC

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

The key e-commerce legislation in Cyprus that applies both to B2B and B2C transactions is the “Law on Certain Legal Aspects of Information Society Services” in Particular Electronic Commerce and Associated Matters of 2004 as amended Law No. 97 (I) 2007” (The Electronic Commerce Law). The Law implemented the Directive 2000/31/EC of the European Parliament and of the Council of the European Union based on the EU Directive (2000/31/EC) on certain legal aspects of information society services, in particular electronic commerce in the internal market.

The key e-commerce legal requirements which apply to **Business-to-Business** (“**B2B**”) are general information requirements and pre-contractual information requirements. Additionally, the commercial communications must be clearly identified and electronic contracting should indeed be allowed.

There are no requirements to register, according to Article 7 of the Electronic Commerce Law; the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation before starting any activities.

The law does not apply in the following instances:

- the field of taxation;
- questions relating to information society services covered by the provisions of the Processing of Personal Data (Protection of the Individual) Law of 2001 and the Regulation of Telecommunications and Postal Services Law of 2002 as amended or superseded on each occasion;
- questions relating to agreements on concerted practices which fragment the market or fix prices, or to other practices governed by the Protection of Competition Law of 1987 as amended or replaced on each occasion; or
- the following activities of information society services:
 1. the activities of professions directly and specifically connected with the exercise of public authority;
 2. the representation of a client and defence of his interests before the courts; and
 3. gambling activities.

From the provisions of the Electronic Commerce Law, there are legal obligations to B2B e-commerce to provide information (disclosure requirements). In order to protect consumers,

the Electronic Commerce Law states that specific information about the service provider should be disclosed to the recipient of the information when conducting business electronically. Such information includes disclosure of the name of the service provider and their contact details (including email addresses and others), the physical address at which the service provider is established, whether the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and the registration number or equivalent means of identification in that register, where the activity is subject to an authorisation scheme and the particulars of the relevant supervisory authority. Furthermore, where the service provider undertakes an activity that is subject to VAT, the identification number on value added tax must be disclosed as well.

From the provisions of Law 156(I)/2004, it arises that commercial communication must comply with the following conditions:

1. A service provider is obliged to ensure that any commercial communication provided is clearly identifiable as a commercial communication and identifies the natural or legal person on whose behalf it is made.
2. Furthermore, any promotional offers and the conditions, which must be met to qualify for the offers, must be identified and presented clearly and unambiguously. In the same way, any unsolicited commercial communications sent by email must be clearly identifiable as such as soon as they are received.
3. Specific information must be disclosed by the service provider to the contract party, if a contract is to be concluded via electronic means.
4. Where the service providers’ terms and conditions are applicable, they must be made available to the contract party in a way that will allow the contract party to store and reproduce them.
5. If an order is placed with the service provider, the order must be acknowledged without undue delay and by electronic means.

There are circumstances where the above requirements do not apply. Some of the requirements can also be omitted on a B2B basis if the participants agree.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In relation to electronic commerce, Cyprus law has come

in conformity with EU standards by passing the following legislation:

1. Electronic Commerce and Associated Matters Law 156(I)/2004, amended by Law No. 97(I)/2007 (the Electronic Commerce Law);
2. Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (No. 125(I)/2018) (Data Protection Law);
3. Law on conclusion of Distance Contracts 14(I)/2000, amended by Laws No. 237(I)/2004, No. 93(I)/2007, No. 16(I)/2008, 125(I)/2009, 133(I)/2013;
4. Legal Framework for Electronic Signatures and Associated Matters Law 188(I)/2004; and
5. Regulation of Electronic Communications and Postal Services Law 112(I)/2004, last amended by Law No. 76 (I)/2017. The Electronic Commerce Law has a broader scope, covering many aspects of e-business encompassing both B2B and B2C. Therefore, the legal requirements and obligations are those that are mentioned in question 1.1 above.

Other legal obligations specific to **Business-to-Consumers** (“**B2C**”) is that businesses shall comply with the Data Protection Law; businesses under the Data Protection Law are obliged to provide a privacy policy in which they need to explain to the consumers how they handle all consumers’ personal data. Such personal data received from the participants by electronic means should be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed. It must be accurate and, where necessary, kept up to date, and it must be kept in a form which permits identification of data subjects (participants) for no longer than is necessary for the purposes for which the data were collected or processed.

Furthermore, the businesses have obligations to provide consumers with at least the following information: the identity of the controller/their representatives; the purposes of processing of data; information about the recipients or categories of recipients of the data; the rights of the data subjects (individuals to whom the data relates); and more.

Additionally, the Law on Distance Selling Contracts obliges businesses to provide to the consumer clear information about goods and services before they buy. Confirmation should be made in writing, there is a right to withdraw from the contract and protection against credit card fraud, and unless otherwise agreed by the parties, the business must fulfil the contract within 30 days from the next day on which the consumer placed the order.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

As of 25 May 2018, the principal data protection legislation in the European Union (EU) has been Regulation (EU) 2016/679, the **General Data Protection Regulation** (“**GDPR**”). In Cyprus, a national law supplementing GDPR was enacted in July 2018, the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) (Data Protection Law).

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

The main challenge that organisations are facing is mainly to protect the Right to Privacy and to comply with GDPR, as those companies are collecting, using and storing data. Such organisations need to comply with the fundamental principles of the GDPR, such as the principle of purpose of limitation (data to be collected for specified, explicit and legitimate purposes), the purpose of data minimisation (the information that is required has to be relevant for its purpose and limited to what is necessary) and more. For example, organisations also need to provide the individuals with the rights and requirements deriving from the fairness principle, which refers, for example, to the need for organisations deploying AI applications to be aware of implications that this deployment may have on individuals and their rights and freedoms but also on communities and societal groups. Additionally, organisations must act in a way that promptly complies with the expectations of the data subjects concerning the respect of their rights, especially when the consent forms the legal ground of processing.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The government has developed and implemented data protection legislation with adequate and co-ordinated levels of enforcement, addressing the development of fintech, retail, AI and digital health in order to ensure equivalent and adequate levels of protection.

Additionally, Cyprus recognises that digital transformation, boosting investment in scientific research and innovative entrepreneurship is the prospering of every citizen and company alike in a dynamic digital economy. In Cyprus, the Institute for Research and Innovation supports innovative projects and research, by providing funding opportunities and overseeing the participation of research/innovation projects to domestic and international competitions. As of March 1 2020, the Cyprus government has been operating a Deputy Ministry of Research, Innovation and Digital Policy, as part of the Ministry of Finance, which was established in order to promote, guide and develop the digital transformation of Cyprus, while facilitating the operation of start-up businesses and supporting the Institute for Research and Innovation.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The cybersecurity framework in Cyprus, which is also applicable to e-commerce businesses, aims for the protection of all critical infrastructures of the state and the operation of information and communication technologies to implement the necessary levels of security, for the benefit of every individual and the economy. The National Cybersecurity strategy provides for a systematic approach on cybersecurity awareness, the implementation of which is co-ordinated by the Commissioner’s office of Electronic Communications and Postal Regulation. The government also supports activities in Cyprus via higher education institutions in the areas of network and information security. Further efforts have been made in order to enhance

awareness of risks and threats and to protect personal information online. Consequently, the country has adopted a strong and fundamental legal and regulatory framework addressing cybersecurity and protecting the rights of individuals and organisations in the digital environment.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Comprehensive legislation protecting consumers from online business malpractice has been adopted and is enforced through the Electronic Commerce Law (156(I)/2004), amended by Law No. 97(I)/2007. A lead agency responsible for the protection of online consumers has been designated: the Consumer Protection Service, which is a sub-division in the Ministry of Energy, Commerce and Industry. The main objective of the service is the protection of consumers' safety and economic interests. This was achieved through effective enforcement, improved monitoring of consumer markets and constant education of consumers. Overall, the country follows International and EU practices and is taking part in many EU meetings on amendments to required legislation. Additionally, Cyprus has implemented the Directive on security of **Network and Information Systems** ("NIS"). For the full implementation of the NIS Directive, the Digital Security Authority was formed, aiming for full implementation. Cyprus is obliged to boost its capabilities in the area of cybersecurity (National Competent Authority, National CSIRT, etc.) so as to co-operate with necessary stakeholders on a national and European level and at the same time manage cyberspace risks in a structured way and to impose incident notification requirements on relevant entities. Contrary to the NIS Directive, as stated in question 2.1, Cyprus has the Data Protection Law and has established in Nicosia the Commissioner's Office, which is an independent administrative authority dealing solely with the protection of personal information relating to an individual, against its unauthorised and illegal collection recording, and further use by imposing fines for those not complying.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In Cyprus, there has been an increased development and use of e-commerce in recent years. Mainly younger consumers feel confident with e-commerce transactions and embrace new technologies. Both online shopping and cashless electronic payments are booming and are among the key drivers of the digital transformation taking place in our economy and society. The ease of making electronic payments is disrupting many aspects of traditional consumer shopping behaviour, which is also increasingly driven by widespread use of mobile devices and apps.

However, sales in Cyprus still predominantly take place offline and a more cash-friendly consumer attitude still prevails in certain transactions. However, the opportunities that e-commerce and cashless transactions afford in terms of convenience, efficiency and affordability will help them gain further ground in the years to come; their popularity among younger generations and strong EU-level policy support for digital transformation are also helping boost their prospects.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

There are no particular payment methods that offer a cultural challenge; however, this can be clearly shown and will differ based on each consumer's characteristics (age, profession, etc.).

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

As stated in question 4.1, Cyprus e-commerce platforms continue to evolve along with the internet and the development of the legislation in that area.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

E-commerce in Cyprus has overcome the language barrier by developing translation and localisation services that assist to adapt a website to a foreign local market. The main target is EU markets and the language of preference for e-commerce activities is Greek, which is the native language for locals. English is also widely used and spoken by almost all consumers.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

There are no particular web-interface design concepts that influence consumers' interactivity. However, it goes without saying that the more generally solid the organisation is, the more trust the consumer will show, and hence will be more willing to enter into a transaction.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

E-commerce has indeed been affected by the Covid-19 pandemic. Temporary lockdown measures imposed to the majority of retail and trade organisations, along with social distancing measures, have changed the landscape of how businesses operate. The majority of retailers were not prepared for such a disruption to their operations. A significant number of companies in Cyprus have developed an online presence and have set up payment procedures through websites and applications so that they remain abreast with technology and up-to-date with their competition. As a result, and due to the pandemic, companies will invest more in online channels for business continuity reasons as well as to benefit from the change in consumer behaviour as Cypriot consumers are embracing e-commerce.

Consequently, the pandemic will lead to an overall accelerated adoption of e-commerce as it has changed the behaviour towards online channels, and the shifts are likely to remain after the pandemic.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

The first step to enable the brand enforcement and protection is to register its **Intellectual Property** (“IP”). Where the rights established by the registration of a trademark are infringed, the proprietor of the trademark may use alternative dispute resolution procedures or can file a court action before the District Court against the infringer.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

There are no restrictions.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

When contracting with third party-owned data centres or **Cloud Service Providers** (“CSPs”), there are indeed various privacy considerations. The Data Protection Law applies to data centres and cloud providers in the same way as any other technology where personal data is concerned and collected. The main issue when an organisation uses a CSP to store or process personal data is that the organisation needs to confirm the location of the data centres where such personal data is being kept. Many cloud providers use several firms located in different countries and are likely to qualify as international organisations; therefore, it must be ensured that appropriate safeguards are in place to protect personal data and to avoid any security risks and/or breaches.

Additionally, as cloud services may transmit data to third country controllers, they will have to meet the usual requirements of the GDPR with regard to international data transfers. This includes having a legitimate reason for the transfer, asserting data principles, applying appropriate controls or measures to protect personal data and informing the data subjects of the transfer of their personal data.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

No, there are no such requirements.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Cyprus has an advanced communications infrastructure in place to support businesses and constant efforts are being made to upgrade, expand and fully digitalise international trade.

New generation products are adopted by both private enterprises and the government; Cyprus technology is constantly being reinforced by high-end mobile networks, advanced satellite systems, fixed broadband via fibre connections, and more.

The country has dedicated fibre links to major international Points of Presence and Connectivity, ensuring all the right connections are in place.

The government is focused on creating a more efficient communications landscape and is promoting a digital economy, developing more secure and efficient global communications and launching incentives to digitalise international (cross-border) trade. Cross-border co-operation has been facilitated by the creation of infrastructure, including information and communication technology infrastructure, high-speed international connectivity, cables, platforms, devices and telecom services in order to ensure efficient connectivity among country systems to enable information flow.

Additionally, the adoption of electronic documents systems which involves the recognition of electronic signatures are also measures that enables international trade.

Consequently, with its current infrastructure and the commitment of the government to invest in the technological landscape, the country will boost its competitiveness to a digital future. Therefore, substantial growth in this sector is expected in the coming years.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

A main barrier which affects the adoption of digital technologies is the access and use of digital networks. Issues range from matters such as the quality of physical infrastructure to regulatory matters. Connectivity is a significant constrain for the adoption of digital technologies; the physical infrastructure or the cables and wires that underpin the transfer of information between countries underpin digital connectivity.

Co-ordination in and amongst countries also remains a problem, even where infrastructure exists. Therefore, the constant development of the information and communication technology infrastructure can unlock those barriers. Regional systems might also assist for smoothing out the transit process. Furthermore, regulatory differences between countries also remain. Principles of market openness enshrined in trade agreements may assist countries' approach to digital trade.

Consequently, market openness is essential for digital trade; market openness needs to be approached by taking into consideration the full range of measures that may affect any particular transaction. If logistics services costs in the receiving (or delivering) country are high due to service trade restrictions, or if goods are held up at the border by cumbersome procedures, then the benefits of digital trade may not be facilitated.

A holistic approach to market openness also means going beyond the issues that traditionally concern trade policy makers to understand how these interact with other policy domains such as infrastructure, innovation, skills and connectivity. New technologies are often made available through international trade and access to global markets for both inputs and outputs; this is indeed essential for scaling production and increase of competition. This should be possible for all businesses with the skills and capability to adapt to new data-driven solutions. Successful businesses in the digital age embrace both new technologies and access to global markets. Trade policy needs to be seen in the context of a range of other policies, which are also significant for the shared benefits for digital adoption to materialise.

Additionally, in order to successfully adopt trade facilitation and overcome such barriers, the House of Representatives has passed by majority a law establishing the Deputy Ministry of

Research, Innovation and Digital Policy. Further information can be found in question 2.3.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Cyprus introduced a flexible tax regime and managed to have one of the lowest and most favourable tax systems in the EU and globally, making it attractive to foreign and local investors to base their businesses in Cyprus.

A new amended Income Tax Law (118(I)/2002) was introduced in order to create attractive incentives through tax relief to individuals who invest in innovative businesses, including start-ups. In 2016, the Income Tax Law was amended through Article 9A and was introduced in order to enhance access to finance for new innovative businesses which face many difficulties accessing bank lending due to the high risk of operations.

In order to be eligible to benefit from the scheme, investors must be physical persons and independent investors, investing either directly or through an investment fund or through an alternative trading platform, in innovative **small and medium-sized enterprises** (“SMEs”).

Tax exemptions are subject to the following provisions:

1. The amount of deductible taxable income may not exceed 50% of the taxable income of that person during the tax year in which the investment is made.
2. The discount, insofar as it is not granted due to the above restriction, may be carried forward and granted for the next five years, subject to the above percentage limitation. Additionally, the deductible amount may not exceed the amount of €150,000 per year.

Cyprus also introduced a new Cyprus IP box regime which allows for a deductible notional expense calculated as 80% of the qualifying profits earned from qualifying intangible assets.

Qualifying intangible assets are:

1. patents;
2. computer software;
3. utility models, IP assets that provide protection to plants and genetic material, orphan drug designations, extensions of patent protection; and
4. other IP assets that are non-obvious, useful, and novel, that are certified as such by a designated authority, in Cyprus or abroad and where the taxpayer fulfils size criteria; annual IP related revenue does not exceed €7,500,000 for the taxpayer, and group total annual revenue does not exceed €50,000,000, using a five-year average for both calculations.

Qualifying intangible assets do not include business names, trademarks, brands and other marketing-related IP.

Qualifying profits include, *inter alia*:

1. royalties or other amounts resulting from the use of qualifying intangible assets;
2. licence income for the exploitation of intangible assets;
3. amounts derived from insurance or compensation in relation to the qualifying intangible assets;
4. trading income from the sale of qualifying intangible assets excluding capital gains which are not subject to taxation in Cyprus; and
5. IP income embedded in the sale of services, products, or from the use of procedures directly related to the assets.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

One of the main areas that may lead to disputes is the determination of the accountable tax jurisdiction with many sellers avoiding registration in third countries, where they trade through platforms. This most likely makes tax enforcement, collection and identification of business tax functions (individuals and systems required and the use of financial data) difficult, especially with regard to cross-border trade in services and intangible assets.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

According to Cyprus law, an employee is any person who works for another individual/company under an employment or training contract or under conditions where an employment relationship can be inferred between an employer and an employee.

Based on the above, any person who does not work full-time for another person on the basis of a contract and/or employment and/or training or under conditions where an employment relationship may be inferred between an employer and an employee, is considered as either self-employed, freelance or as an independent contractor.

Different benefits and/or advantages are provided to employees such as the fact that the employer is responsible for the actions performed by the employee, which were performed during their employment, and that the employer is responsible for providing a secure work system to the employee in order for any work to be performed.

However, outsourcing work to specialised individuals or organisations (acting as consultants) might shift the responsibility, either legal and/or professional, to them. It is understood that such terms should be clearly reflected in any agreements signed between businesses and said consultants. Furthermore, both resourcing work to employees or outsourcing work to contractors come with their own cost advantage benefits, depending on the nature of the work. Therefore, on some occasions, the employer must weigh the advantages and disadvantages based on the overall experience of the above parties and whether either party has the necessary tools/equipment/expertise to finalise any work.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There is no specific regulation in place; however, if it is either orally or contractually agreed between the employer and employee, and for whatever reason, work can be carried out away from an organisation's physical premises considering that all other measures (i.e. data protection) have been accounted for.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

As in other EU countries, employers in Cyprus had to adapt to a new working environment and conditions due to the Covid-19 pandemic. The negative impact on the Cypriot economy has been fundamental. Because of the imposed strict lockdown, the majority of employers had to move to remote working, where possible, in an effort to maintain social distancing. The majority of employees had to work from home and combine work with personal and home life. Due to the pandemic, physical meetings have been replaced by telework and video conferencing. Employers also implemented a shift rotation system and more flexible-working arrangements.

Employers, who are obliged by law to provide employees with a safe and healthy working environment, took additional measures to prevent the spread of Covid-19 as regards to employees that had to physically work at their workplace.

The Covid-19 crisis is so deep that it will not only radically affect labour markets in the short and medium terms, but it can also change substantially the way work, in general, is organised. The adjustment to new working conditions demonstrates that remote working can form a key positive part of a new working culture in Cyprus and will likely remain in place.

Furthermore, employees and employers will most likely benefit from the extensive use of technology, software, telework applications and other means that were not being used before.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

There are no legal barriers for now.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Cyprus is an EU Member State that is fully compliant with all international guidelines and regulations. Furthermore, it offers a tax system that is attractive, practical, efficient, stable and tested (whether that is for holding, financing, IP, services or trading activities). Its legal system is based on Common Law and Principles of Equity (which is easily understood and preferred) and, most importantly, Cyprus has all the necessary infrastructure to accommodate any needed level of business substance, with a comparative cost advantage when compared with other EU prime jurisdictions.

For further tax-related advantages and general incentives, see question 8.1, as well as question 7.1.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The key areas of focus by the regulators are employment matters, competition law, consumer and data protection, as well as intellectual property matters (the focus is on the portability of data over platforms, the exceptions to intellectual property such as copyright law, text and data mining, trade secrets and more).

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Cyprus conveyed the Payment Services Directive (EU) 2015/2366 and implemented such through the Payment Services Law 31(I)/2018 and the Electronic Money Law 2012, which merely provides for the development of innovative online and mobile payments, more secure payments and enhanced consumer protection. Therefore, in accordance with such laws, payments and electronic money services may only be provided within Cyprus.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

In order for **Payment Service Providers ("PSP")** such as **Credit Institutions ("CI")**, **Payment Institutions ("PI")** or **Electronic Money Institutions ("EMI")** to be fully operational, authorisation and a permit must be granted by the Central Bank of Cyprus. The key legal issues for online payment providers is that they need to be able to block any possible fraudulent activity and to secure electronic transactions by having strong security methods and measures in place so as to protect consumers' data and to prevent such activity. Additionally, payment service providers need to have in place a complaints procedure for consumers which can be used before seeking out-of-court redress or before launching any court proceedings. Such payment providers are obliged to respond, in writing, to any complaint within 15 business days.



Xenia Kasapi is an advocate and Head of the IP and Data Protection Department at E & G Economides LLC. Xenia holds a Bachelor of Laws from the University of Sheffield and a Master of Commercial Law from University of Bristol, and has successfully completed a professional course in Arbitration Law at the Chartered Institute of Arbitrators (Cyprus Branch). She is a member of the Cyprus Bar Association and a member of Arbitrators in the Chartered Institute of Arbitrators.

Xenia specialises in Information Technology (including e-commerce), data protection, intellectual property and commercial law. She has a broad commercial practice with particular focus in intellectual property law, data protection and e-commerce law. Xenia deals with all aspects of intellectual property law. She is also assisting companies with establishing and maintaining data privacy and security compliance matters and is drafting and reviewing commercial transaction documents.

Xenia is also a lecturer on Business Law and lectures to undergraduates at Cyprus College supported by the European University Cyprus.

E & G Economides LLC
17 Gr. Xenopoulou Street
3106 Limassol
Cyprus

Tel: +357 25 866 480
Email: xenia.kasapi@economideslegal.com
URL: www.economideslegal.com



George Economides is a partner at E & G Economides LLC. George obtained his Bachelor of Laws from the University of Westminster. Further to his studies, George has gained extensive experience in accounting, auditing and tax matters with a leading Cyprus accountancy firm.

His area of focus is tax, real estate, immigration and technology with IP & GDPR, and he is also involved in the firm's business development, marketing and operational activities. George is a member of the Cyprus Bar Association, a member of the Individual Tax and Private Client Committee of the International Bar Association and a member of the Society of Trust and Estate Practitioners (STEP).

He frequently works with HNWIs and international law firms and associates providing advice in restructurings, investments, acquisitions and disposals of either assets, intangible assets or real estate. He also represents and generally advises international companies and group of companies that have relocated and headquartered to Cyprus such as ship-owning, ship-management, e-commerce, investment, financial services and real estate companies.

E & G Economides LLC
17 Gr. Xenopoulou Street
3106 Limassol
Cyprus

Tel: +357 25 866 480
Email: george.economides@economideslegal.com
URL: www.economideslegal.com

E & G Economides LLC, based in Limassol, specialises in Corporate & Commercial, Mergers & Acquisitions, Banking & Finance and Capital Markets work. Litigation, Immigration, Real Estate, Financial Services, Data Protection, IP & Privacy and Private Client matters are also offered. The firm has continued to grow and expand its areas of practice with the support of an active network of global associates with longstanding ties to the corporate and financial communities.

The firm maintains a diverse client base and is regularly instructed by high-net-worth individuals, entrepreneurs, multinational corporations and tax firms, as well as global banking and credit institutions and both domestic and international transactions.

Clients' interests often have a global focus and the firm is frequently mandated to co-operate with international law firms on multijurisdictional projects and other cross-border engagements. Such assignments have been pivotal in yielding a globally minded perspective and have brought the firm in close co-operation with international law firms.

E & G Economides LLC is also ranked in prestigious professional and legal directories internationally.

www.economideslegal.com

E&G ECONOMIDES LLC

France

Armengaud Guerlain



Catherine Mateu

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

In France, a company which operates an e-commerce site is required to comply with several legal obligations (in particular the law of June 21, 2004 known as “LCEN”, the Commercial Code for B2B relations).

1. Mandatory information on the website

Each website must include mandatory information, intended to allow users (including professional users) to identify the person responsible for the site. The exhaustive list of mandatory information, listed in article 6 III of the LCEN, only concerns professionals editing websites that are relevant to their activity. These must indicate:

- If the website is operated by a natural person: name, first name, address.
- If the website is operated by an individual business: name, first name and address of the business manager, registration number in the trade and companies register or in the trades directory.
- If the site is operated by a company: company name, legal form, address of head office and amount of share capital, registration number in the commercial and companies register.
- If the activity is regulated and subject to authorisation: name and address of the authority which issued the authorisation.
- If the activity is commercial: the VAT identification number in the event of liability, the name of the person responsible for the publication, the email address and telephone number for contacting the company.
- Accommodation conditions: name or corporate name, address and telephone number and, if applicable, the CNIL declaration number.

Article 6 III-1 c) of the LCEN imposes the mention of the name of the director of publication or that of the co-director of publication.

2. Mandatory pre-contractual information in B2B

In the context of B2B relations, the rules to be observed are provided for by the Commercial Code (article L.441-6). This

text indicates that the professional is required to communicate to any professional client who requests the:

- conditions of sale;
- scale of unit prices;
- price reductions; and
- terms of payment.

Due to the crisis of Covid-19, the European Commission has postponed by six months the entry into force of the “VAT package on e-commerce”, which aims to help states fight more effectively against tax fraud. It should come into force on July 1, 2021. The Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations applicable to supplies of services and distance sales of goods, generates:

- a redefinition of the VAT regime for intra-Community distance sales of goods (B2C);
- the lowering of the turnover threshold to EUR10,000 for distance sales;
- the implementation of a one-stop VAT shop for the sale of goods and services;
- the abolition of the import VAT exemption for small shipments (up to EUR22) and the import VAT declaration via the one-stop shop;
- VAT liability of marketplaces on intra-EU imports and sales on behalf of their non-EU sellers.

France, which has already transposed this directive in its 2020 finance law, has confirmed this postponement to July 1, 2021, which will be included in the 2021 finance bill.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

E-commerce is governed by the law 2004-575 of June 21, 2004, which transposes into French law the European Directive 2000/31 regulating electronic commerce.

The provisions of this law apply whether the customer is an individual or a professional.

Moreover, the provisions of the Consumer Code also apply if the customer is a private individual, in particular articles L121-16 to L121-20.

a) On the right of withdrawal

The right of withdrawal is the right for the e-customer, within 14 calendar days from the date of online contract, to cancel the contract without justifying his decision.

In addition to the information provided for by article 19 of law n° 2004-575 of June 21, 2004 for confidence in the digital economy, e-commerce professionals must provide the consumer with the information provided for in article L.221-5 of the Consumer Code, including:

- the conditions, deadlines and procedures for exercising the right of withdrawal, as well as the standard withdrawal form;
- the fact that the consumer bears the costs of returning the goods in the event of withdrawal and, for distance contracts, the cost of returning the goods when they, due to their nature, cannot normally be returned by the post;
- information on the consumer's obligation to pay fees when he/she exercises his/her right of withdrawal from a service contract for which he/she has expressly requested the start of performance before the end of the withdrawal period;
- information according to which the consumer does not benefit from a right of withdrawal or, where applicable, the circumstances under which he/she loses it; and
- information relating to the professional's contact details.

The pre-contractual information to be provided to the consumer must include the information that the contract has a right of withdrawal or not, the conditions and procedures for exercising this right (duration of the withdrawal period, starting point of the period, etc.), as well as the standard withdrawal form (article L.221-5).

If this information is not provided before the conclusion of the contract, the withdrawal period is extended by 12 months from the expiration of the initial withdrawal period. If during this period the information provided for by law is given to the customer, a new period of 14 days runs from the date on which the consumer will have received this information.

Failure to comply with the pre-contractual information obligation linked to the right of withdrawal may be penalised with an administrative fine of EUR15,000 maximum for a natural person and EUR75,000 for a legal person (article L.242-13 of the Consumer Code).

b) On the delivery time

The professional must indicate the date or the deadline for delivery of the goods or the performance of the service. Lack of an indication of this date or of this timeframe or without an express agreement between parties, the professional must deliver the goods or perform the service without undue delay and at the latest 30 days after the conclusion of the contract (article L.216-1 of the Consumer Code).

In the event of failure to deliver on the date or within the time frame or, failing this, no later than 30 days after the conclusion of the contract, the customer may order the professional, in writing, to make the delivery or to provide the service within a reasonable additional time. If he/she has not complied within this new period, the customer may request, always in writing, the termination of the contract. This becomes effective upon receipt of the client's mail unless the professional has done so in the meantime.

c) Information relating to the conclusion of the contract

The seller must remind the consumer of the terms of his order before he places it. The consumer must also be informed that placing his order obliges him/her to pay for it.

The button dedicated to the confirmation of the order must mention, under the penalty of nullity, "order with obligation to pay" or any similar formula devoid of any ambiguity.

Moreover, concerning the security of remote payments, the company operating an e-commerce site must also respect several rules regarding remote payments.

First of all, in case of fraudulent use of a bank card, it is the company that bears the risk. The bank can automatically debit the company's account for any purchase disputed in writing by the cardholder. This right is included in the distance selling agreement between the company and the bank.

Secondly, the company must also ensure the security and confidentiality of its customers' banking data. Certain information about the customer can only be kept with the customer's consent (card number, expiration date, etc.).

Moreover, as far as the declaration to the CNIL is concerned, commercial websites that collect personal information (name or email address for example) and constitute files of customers and prospects, must make, depending on the case, a simplified declaration or a normal declaration to the CNIL.

The company must respect the following obligations concerning the information collected on the customers:

- it must obtain their prior consent;
- it must inform customers of their right to access, modify and delete this data;
- it must ensure the security and confidentiality of the data; and
- it must provide the length of time the data will be stored.

Non-performance of the contract

In the event of non-performance or improper performance of the contract by the e-commerce professional, the customer may request compensation for his/her loss and in particular for damages without having to demonstrate a breach.

Article L.221-15 of the Consumer Code provides for the distance seller "*ipso jure* liability", that is to say that the seller is liable for the proper performance of the contract throughout the command-transport-delivery chain.

Force majeure (an irresistible and unpredictable fact) or direct breach by the consumer are the only exemptions from the seller's liability.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The General Data Protection Regulation (GDPR), which entered into force on May 25, 2018 in the European Union, establishes a new legal framework for the protection of personal data.

In France, a law of June 20, 2018 relating to the protection of personal data amended the "Data Protection" law of January 6, 1978 governing the protection of personal data in France, to adapt it to the provisions of the GDPR.

In France, it is the CNIL (National Commission for Data Protection) which controls the implementation of the legislation related to data protection. It advises, has investigative powers and can impose corrective measures in the event of an offence.

The reform of the Data Protection Act has considerably increased the sanctioning powers of the CNIL.

Moreover, in a recent decision (CE of 04/17/2019, 423559: ADEF), the Council of State (CE) held that the CNIL is entitled to pronounce sanctions without prior notice when the breach found cannot be brought into compliance within the GDPR.

In April 2019, the CNIL also clarified its control strategy for 2019. The three control issues selected with regards to the entry into force of the GDPR are:

- respect for individuals' rights by companies;
- the distribution of liabilities between data controllers and processors; and
- the processing of children's data.

This year, the CNIL planned to fully verify compliance with the provisions of the GDPR by organisations with regard to complaints received, whether individual or collective, and has chosen broad issues that may concern all sectors of activity, unlike in previous years.

First, the CNIL intends to ensure that companies respect all of their obligations and the people's rights, including those of the GDPR. In fact, it has received more than 11,000 complaints/claims over a year, and almost 73% of them concern a company's non-compliance with the exercise of a right.

Next, the CNIL intends to control subcontractors with regard to their new obligations arising from the GDPR and verify compliance with the subcontracting contracts.

Finally, the CNIL will monitor the processing of underage data by publishing content on social networks, biometrics and video surveillance in schools, obtaining parental consent for persons under 15 years old (the digital majority has been fixed in France at 15 years).

In addition, to fulfil its advisory role, in 2019, the CNIL launched its "Developer Kit", to cover all stages in development:

- Choose your work tools.
- Prepare your development.
- Best practices for managing a source code.
- Libraries or third-party tools: how to integrate them into an application?
- Strengthen the quality of the source code.
- Document the source code and the architecture of the site.

The legal framework in France related to the protection of personal data is fully in force with the publication in the Official Journal on May 30, 2019 of Decree No. 2019-536 of May 29, 2019 that implements the Law No. 78-17 of January 6, 1978.

The ePrivacy Regulation and in particular its principles regarding consent to cookies should not be evaded.

Indeed, consent is an essential element of the ePrivacy 2021 regulation, and cookies and similar trackers are also the target of the new data protection bill. End-user consent will be required to process any type of electronic communication and its content.

Already, the 2002 ePrivacy Directive made it necessary to install cookie banners on websites to obtain user consent, although most of the early cookie banners from before the GDPR did not work as intended.

Under the new draft ePrivacy 2021 regulation, end-user consent is required before processing any type of data from users' computers or smartphones.

If ePrivacy 2021 is adopted, it will repeal and replace the ePrivacy Directive. The draft ePrivacy 2021 regulation emphasises that consent plays a critical role at the heart of today's internet, and that this consent requirement is here to stay.

However, the ePrivacy 2021 regulation paves the way for new ways to streamline consent across browsers, and also addresses what is known as "cookie consent fatigue" (when users are overwhelmed by the requirement to give consent on websites), emphasising that user consent is necessary for true privacy protection – now and in the future.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

For organisations managing large flows of data, crucial issues arise especially in terms of fintech, AI and digital health.

As consumers are increasingly concerned about the protection of their personal information, professionals are faced with regulations that have transformed the way they collect, control and manage their data.

Companies that operate in this area will have to manage to eliminate or minimise drifts. This may involve preprocessing and profiling data before it is used in AI systems, as the performance of AI may depend on the data that powers it. Its benefits are well established, especially in the health field. Increased privacy awareness will force the government to pass anonymity laws to encourage the collection and use of health data for the common good.

Since the appearance of fintech, financial services have become the biggest users of data, giving rise to security concerns regarding hacks and data breaches, particularly in the banking context where identity theft and asset theft can be simultaneous and potentially cause significant harm for consumers.

Several issues can arise:

- Confidentiality issues: The GDPR implemented by the European Union has had an impact on organisations around the world. Organisations that work with confidential data (fintech, digital health, notably) must ensure compliance with personal data regulations.
- Discrimination issues: Bias in the results of artificial intelligence algorithms can be harmful both to the companies that use them and to their customers, as a consumer or a citizen, because of the risks of discrimination or inadequate advice they conceal. In particular, care must be taken to ensure that the data are representative of the target population so that they do not lead to exclusionary phenomena. This is why certain financial institutions set up specific training to raise awareness of their data scientists on these aspects. Concerning fintechs, critics have voiced concerns about the fact that access to so much data could increase pricing discrimination and financial exclusion: consumers most at risk and those without digital fingerprints could be discarded. The use of algorithms, closed and exclusive, may also create a situation where consumers would be denied access to a service (for example, credit or insurance) on the basis of an inaccurate correlation, with no possibility of refuting or correcting the underlying assumptions.
- Cyber-attacks: AI increases the possible attack points (automation of repetitive tasks and increase in the volume of computer interconnections which therefore increases the number of potential vulnerabilities exploitable by cybercriminals; more and more systematic use of the cloud for AI needs multiplies the possible entry points for a cybercriminal; the use of machine learning could make it possible to "crack" passwords from previous password archives; cyber-attacks could be personalised, which would make them more effective, for example, personalised phishing, use of chatbots or voice imitation technologies to extract confidential information).

Finally, the e-privacy regulation is an effective tool but also a strategic issue to enforce privacy on the internet through the collection of enhanced consent.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Privacy protection is ensured by various regulatory provisions.

First, the implementation of the second Directive on payment services, known as DSP2, which announced major changes for the banking sector and of course for fintechs.

The DSP2, which was implemented into French law by ordinance n° 2017-1252 of August 9, 2017, includes several components and introduces new rules of direct interest to consumers including:

- The obligation of strong authentication (meaning at least two factors between a code or password that we know, a device that we have, biometric data such as the fingerprint, voice or iris) for online payments of more than EUR 30, to reduce fraud in e-commerce.
- Opening up the market to new players by providing access to account information via a secure communication channel.

Second, the entry into force of the GDPR also has a major impact for fintechs. The latter will thus have to demonstrate the integrity and the validity of the consent of the customers regarding the sharing and the marketing and commercial exploitation of personal data. Failure to comply with the principles of the regulations, in particular in connection with the recording of customer journeys and the registration process, will be severely punishable, including for a fintech under development. In short, fintechs will be keen to fully respect the confidentiality of personal data in the architecture of their solution and their services. There is no doubt that this will go in the direction of gaining users' confidence in these new innovative services.

At the European level, the European Commission has recently presented a series of measures aimed at promoting AI:

- Strengthen financial support and encourage the public and private sectors to adopt AI: the EU (public and private sectors combined) should increase investment in research and innovation in AI by at least EUR20 billion by the end of 2020.
- Prepare for the socio-economic changes brought about by AI.
- Ensure the establishment of an appropriate ethical and legal framework: the Commission has presented ethical guidelines with regard to the development of AI, which are in line with the Charter of Fundamental Rights of the EU, and take into account principles such as data protection and transparency.

Moreover, and in any case, articles 226-16 to 226-24 of the Penal Code provide for several sanctions in case of invasion of privacy on any platform, but also punish the fact of collecting personal data in an illegal way (for example: health data).

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The French legal framework for cybersecurity comes largely from European legal developments, although the law of June 20, 2018 relating to the protection of personal data amended the "Data Protection" law of January 6, 1978 governing the protection of personal data in France, was already concerned about cybersecurity.

First, the GDPR, whose application in France has modified the legal framework for the protection of personal data, applies to cybersecurity issues linked to e-commerce websites.

With the GDPR, e-commerce websites must ensure the highest possible level of data protection. To guarantee the security of their customers' personal data, merchants will have to deploy all technical means and respect strict rules: the implementation of a consent register; data retention; secure transactional emails; and a word encryption password. A data protection officer (DPO) will be appointed to ensure the implementation and monitoring of these actions.

Also, law n° 2018-133 of February 26, 2018 "laying down various provisions for adaptation to European Union law in the field of security" was adopted on February 15, 2018 and promulgated on February 26, 2018 (hereinafter the "network and information systems security law").

This law transposes Directive (EU) 2016/1148 of July 6, 2016, known by the acronym "NIS" (National Information Security) and related to measures intended to ensure a high common level of security of networks and information systems in the European Union.

This law applies to any processing of digital data, whether or not it is personal data, in particular by e-commerce sites. The latter will have to take technical measures in order to manage risks threatening network security upstream, or even prevent incidents compromising security.

Lastly, the Directive called DSP2, which was implemented into French law by ordinance n° 2017-1252 of August 9, 2017, includes several components and introduces new rules of direct interest to consumers including the obligation of strong authentication (that is to say at least two factors between a code or password that we know, a device that we have, biometric data such as the fingerprint, voice or iris) for online payments of more than EUR30, to reduce fraud in e-commerce.

In France, cybersecurity rules are applied in particular by the CNIL.

Many companies obtain insurance for security breaches. This usually involves an inspection and upgrade of the company's cybersecurity measures, as well as a training session for employees. The insurance protects against potential damage from cyberattacks and breaches and provides strategic support.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Please refer to the above answer.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

According to the French organisation FEVAD (the Federation of e-commerce and distance selling), e-commerce in France is in constant progression but is subject to variations and slowdowns due to various socioeconomic contexts.

In total, EUR92.6 billion was spent on the internet in 2018 by French consumers. The momentum was maintained for e-commerce in 2018 with an increase of 13.4% despite a weakening of growth in December due to the social context (Yellow Vests, "Gilets Jaunes") with an increase of +8% (vs +16% in October and +14% in November). The impact of this slowdown on annual

e-commerce turnover is estimated at 0.7 points of growth, or around EUR600 million. In 2019, the turnover of e-commerce reached EUR103.4 billion in France (11.6% of progression compared to 2018).

Nearly 9/10 internet users buy on the internet on any type of device. This represents almost 1 million buyers over a year, especially among those under 35 who use smartphones, but also among the over 65s for whom now more than 8/10 buy online.

It is estimated that 38.8 million French people buy online.

For 2020, there is a possibility that this trend declines after the Covid-19 crisis.

French consumers have embraced e-commerce and new technologies for a long time. Cash-friendly consumer attitude remains residual.

Indeed, Statista Research Department published in July 2019, the results of a study on the frequency of purchase on the internet of the French. The results report the frequency of online purchases of the French in January 2018. According to the report, about 30% of French people buy online, at a frequency of two to three times per month. The proportion of buyers making an online purchase less than once a month, meanwhile, is 35%. However, these figures saw a large increase in 2020, if we refer to the latest FEVAD reports. Indeed, FEVAD reveals that in the last 12 months, 16.3 million French people have made purchases on mobile. And out of these 16.3 million e-buyers, 49% have bought on the internet at least once a month.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

In France, the majority of consumers use a debit card as their payment method.

According to a survey by Statista Research Department, “Means of payment in France – Facts and figures” on September 11, 2019, in 2018, 67% of French people preferred to pay by debit card rather than pay for their online purchases by check or cash.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Home state retailer websites perform very well in France. For example, the most sold products and services on e-commerce websites in France are fashion items (growing enthusiasm for Made in France products), travel and experiences, technology products, and, increasingly, second-hand products (thanks to the increasing number of second-hand sale apps and websites and the growing concern of environmental issues). Indeed, such products and services target a huge number of potential consumers, and not only a particular sector of the French population.

Also, the influence of online advertising is another important purchase trigger. According to the Criteo Shopper Story 2020 study, consumers remain very sensitive to online advertising. In fact, 63% of 18-35 year olds say they click on an ad while online. 56% of them even claim to buy a product following an online advertising recommendation. Finally, 71% of the 18-35 year old buyers find that the products recommended to them correspond entirely with their expectations.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Many French e-commerce websites are available both in French and in English, in order to target international markets.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Several design concepts are important to facilitate consumers' interactivity and therefore show the seller's reliability:

- **The site design:** like trade dress in conventional points of sale, the website's design is important and can constitute a criterion of choice (colours, icons, design in accordance with the environment in which the site specialises, intuitive design for navigation, etc.).
- **Ease of navigation:** consumers generally look for sites where they can buy easily, a site that “makes their life easier” and allows them to find the information or product that they are looking for.
- **Information on the product:** concerning, for example, the description of the product, the brand, the possibility of checking the availability of the product.
- **The brand:** it remains an important criterion in the consumer's selection. The brand constitutes an anchor point. It is therefore important to insert a brand logo where the consumer will be able to notice it.
- **The delivery policy:** this criterion is very important online because of the immediate “non-possession” of the product. The delivery is evaluated in terms of price, deadlines and guarantees.
- **After-sales service and return policy:** after-sales service can be decisive in responding to the risk of non-compliance of the product delivered with the product ordered online.
- **Customer service:** online customer service is crucial because of the remoteness of the seller and can take the form of assistance before or during the purchase (instant chat service, for example). It constitutes a guarantee of quality and good conduct for the online seller. This can be reflected, for example, in membership of a recognised professional association, the possession of a quality label (appearance of a logo), or in consumer opinions, which are very often consulted.
- **Information on the security of payments:** in particular, on the establishment and adoption of secure means of payment such as SSL encryption (Secure Sockets Layer) or even SET security (Secure Electronic Transaction), where banking information is neither known nor stored on the site to prevent hacking of company databases.
- **Confidentiality of personal data:** information on the site provides greater reassurance to the consumer.
- **The ease of placing the order:** which often depends on the design of the site, the ease of use of the interface. It is preferable that the platform be of “intuitive” use, with icons, images, etc.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

French consumers' attitudes were already settled regarding internet shopping.

Nevertheless, the pandemic caused multiple lockdowns and curfews. During the lockdowns (three in France to date), only "essential" businesses were open. As a result, consumers have integrated into their behaviour the fact (almost systematically) to buy online.

This modification – or reinforcement – has been accentuated in particular in the food sector (online orders), second-hand purchases (Vinted), but also cultural purchases.

Today, this represents almost one in six purchases.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

The main process for online brand enforcement in France is the trademark infringement action on the basis of articles L.713-2 and s. and L.716-4 and s. of the French Intellectual Property Code before Civil or Criminal Courts.

Often this action is initiated after a cease-and-desist letter sent by the right holder or a demand letter.

Notably, if a registered trademark is used without the authorisation of its right holder online, the latter can obtain:

- damages;
- withdrawal of the sign from the litigious website;
- if applicable, retrieving of the litigious domain name; and
- publication of the ruling.

In addition, unfair competition and/or parasitism actions can be brought.

Also, rights on trade names, signboards, domain names, copyrights, databases or corporate names can be opposed to unauthorised parties. Finally, actions based on violations of consumer or competition law (particularly unfair practices) can be brought.

Brand enforcement is also ensured by actions performed by custom authorities and arbitrations regarding domain names initiated by rightholders.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

There are no specific restrictions that have an impact on online brand enforcement in France. However, there are some limits to brand enforcement that also apply on online brand enforcement, including:

- **Theory of exhaustion of rights:** according to this principle, the owner of an intellectual property right cannot prohibit subsequent sales of products which have already been put on the market in the community or the European Economic Area under this mark with the right owner's consent. This theory was set by case law (CJCE *Deutsche Grammophon* – June 8, 1971) on the basis of articles 28 (ex 30) and 30 (ex 36) of the Treaty of Rome relating to the free movement of goods. It was then integrated into the legislation by Directive n° 89/104/EEC of December 21, 1988, then by the regulation of December 20, 1993. Today this theory is codified in article L.713-4 of the French Intellectual Property Code. This theory is also applicable to other intellectual property rights (design rights:

article L.513-8 of the French Intellectual Property Code; author's rights: L.211-6 of the French Intellectual Property Code; and patent rights: L.613-6 of the French Intellectual Property Code).

- **Abusive proceedings:** this tort sanctions the abuse of taking legal action based on general civil liability and may lead to remedies such as damages, injunction under penalties per day of delay or per tort, or publication measures. It is codified in article 32-1 of the French Civil Procedure Code: anyone who acts in a dilatory or abusive manner may be sentenced to a civil fine of a maximum of EUR10,000. The right holder must therefore be careful not to fall into the abuse of process when he or she seeks protection (abusive seizure, abusive internet bailiff report, etc.).

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

French laws relating to the protection of personal data within the meaning of Directive No. 95/46/EC of October 24, 1995 consider the third-party provider (host of the cloud computing system) as a sub-processor of data acting in accordance with the instructions of a data controller.

The implementation of cloud computing services involves risks with regard to data security. In fact, access to data and applications is made between the client and the multiplicity of remote servers. This risk is therefore amplified by the pooling of servers and by their relocation.

Access to services will therefore induce secure connections and user authentication. The problem of managing identifiers and that of responsibilities will then arise (unauthorised access, loss or theft of identifiers, level of authorisation, resignation or dismissal, etc.).

For the same reasons, there is also a risk of data loss that should be taken into consideration, evaluated and anticipated in the context of suitable backup procedures (storage in private spaces, locally, in a public environment, etc.). Similarly, there are also risks with regard to the confidentiality of data (leaks), given the number of servers and the relocation of these.

In addition, since cloud computing services are provided by an external service provider, this involves risks with regard to the quality of service obtained, and the ownership and integrity of the data and/or applications entrusted; risks which should therefore be provided for contractually.

In addition, setting up this type of service can sometimes be expensive. It will thus be necessary to contractually define a unit of measurement for storage, and IT resources used, or even the number of active users, so that this remains advantageous for the company concerned.

Finally, the implementation of cloud computing services gives rise to a number of risks for the company with regard to personal data and formalities imposed by the CNIL. These risks are aggravated in the event of data transfer outside the European Union (EU). The drafting of cloud computing contracts will therefore also have to take these issues into consideration.

The contract must therefore take these constraints into account, especially as the fact of entrusting his data to a subcontractor does not exonerate the data controller from his obligations. This question takes on a particular magnitude because the servers are relocated and the client does not have to know the location of the servers.

To mitigate the risks mentioned above, it will generally be necessary to set up, as in any outsourcing project, a service level agreement, also called an “SLA”, allowing the customer to obtain from the service provider a quality of service contractually agreed.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Since the entry into force in France of the GDPR in the law of June 20, 2018, modifying the law of January 6, 1978, the rules for data centres have been modified and supplemented: the entities handling personal data must implement new measures and be able to demonstrate that they comply with the rules laid down by the GDPR.

Data centres will have to:

- follow up on consent requests and approvals for many different measures;
- link this consent to specific personal data collected or updated for this purpose;
- keep records of processing activities, transfer activities and access or disclosure activities;
- implement organisational and technical protection measures for all production IT systems that contain personal data; and
- create a technical solution to identify, catalogue and classify all data sources in order to allow appropriate action on all the personal data thus identified.

For any organisation preparing to comply with the GDPR, article 5 describes the key principles of data confidentiality to be implemented in the data centre.

The data which must be protected is the information which makes it possible, directly or indirectly, to identify a natural person (name, IP address used, photograph, landline or mobile phone number, postal or email address, fingerprint, registration, etc.).

In particular, the GDPR compels those who wish to collect personal data from minors under the age of 16 to obtain the authorisation of their parents (France has chosen to set the minimum age to consent to the processing of its data at 15 years).

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

French private enterprises and government border agencies use digital tools in the course of international trade.

Indeed, today, information and communication technology is simply omnipresent in the Customs environment. From the use of ICT in office automation and the internet for publishing and disseminating information, to the use of automated clearance systems for customs declarations, risk management, validation and processing of information to final approval procedures, ICT has transformed the way Customs and governments operate.

At recent WCO Council sessions, President Zouhair Chorfi has focused on the rapid changes brought about by ICT, emphasising the need to provide WCO Members with a comprehensive picture of all the possibilities offered by information technology (IT), which enable them to ensure continuous control of cross-border trade and to incorporate best practices and international advances in the field of IT.

Import export work more and more digitally. Private enterprises use more and more e-commerce platforms to sell their goods or services internationally.

Some AI applications can benefit the trade of goods, for example by optimising route planning and enabling autonomous driving, reducing logistics costs by tracking cargo and shipments, using intelligent robots to optimise the storage and inventory, integrating 3D printing to reduce the need for transportation and logistics services, etc.

Thanks to digital customs platforms, the countries in which customs procedures are digitised offer more efficiency and transparency in terms of formalities required for trade. In France, it is called the “GUN”, a national one-stop service for customs clearance.

On this online platform, users can carry out all of the compulsory procedures for importing and exporting goods, and obtain permits, licences, certificates and authorisations.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

The use of digital technologies raises a number of concerns, which can be an obstacle to their effectiveness in facilitating trade.

- **Privacy and personal data:** the collection and analysis of personal data has commercial and social advantages. However, there are growing concerns that companies do not respect data confidentiality enough. The purpose of the laws in France is therefore to clarify the nature of the information about individuals that businesses can collect and store and the use that can be made of it.
- **The adaptation time necessary for technological changes to penetrate the whole economy and the digital divide:**
 - The digital divide is one of the main challenges of the digital economy. It remains significant between developed and developing areas in terms of access to e-commerce platforms in particular.
 - Digitalisation varies considerably across skill categories, leading to an increase in demand for highly skilled workers with skills complementary to digitalisation, and a decrease in demand for low-skilled workers who can easily be replaced by labour-saving technologies and automation. In addition, digital intensity differs across sectors and companies. There are significant differences between sectors in terms of dependence on digital technologies: service companies use more digital technologies than manufacturing companies, while high-tech companies use more industrial robots than service or low-tech companies.

In addition, businesses aiming to build a digital culture must first define a digital mindset, build a digital innovation team and protect it from the rest of the organisation to let the new culture develop. The digital capacity of companies must be on the organisational and IT level.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

In France, there are several tax incentives for financing digital businesses.

1. Tax reductions applicable to capital subscriptions for young innovative companies

New companies, created before December 31, 2022, which invest in research and development, having the status of a young innovative company or young university company, can benefit from tax and social exemptions.

New companies that have the status of a young innovative company can benefit from exemptions in:

- income or corporate tax: 100% exemption for the first financial year or the first beneficiary tax period (which cannot exceed 12 months), then 50% exemption for the following beneficiary financial year; and
- territorial economic contribution and property tax for seven years after deliberation by local authorities.

2. Tax reductions applicable to capital subscriptions for new businesses

The creation of a business in certain areas allows you to benefit from exemption or profit reduction schemes for the first years of activity.

These exemptions exist in favour of new businesses in order to promote employment.

3. Tax rate (income tax or corporate tax) reduced to patent and trademark licence fees

This is an innovation from the reform of the tax regime for patent products (Finance Law for 2019, article 37 – now codified in article 238 of the French General Tax Code).

The system for taxing products from patents and similar industrial property rights (royalties and capital gains on disposal) has been adjusted to comply with the recommendations of the OECD. The tax rate on profits from industrial property income has been reduced to the rate of 10% for companies subject to corporation tax, as well as for companies whose profits are subject to income tax.

Up to now, products from a patent or similar industrial property rights have benefitted from a reduced tax rate (15% for companies with corporate income tax and 12.8% for companies subject to income tax), without any condition linked to the methods of carrying out R&D activities of the company owning the assets being applied.

It applies, for fiscal years beginning on or after January 1, 2019, to net income from items having the nature of the following intangible fixed assets:

- patents, utility certificates and additional protection certificates attached to a patent;
- plant variety certificates;
- industrial manufacturing processes when they are the result of research operations, are the essential accessory for the exploitation of an invention and are the subject of a single exploitation licence with the invention;
- software protected by copyright; and
- inventions whose patentability has been certified by the INPI.

4. Research tax credit applicable to R&D expenses

Businesses that incur research costs can obtain a tax credit that is chargeable against the corporate tax they have to pay.

The research tax credit is a device which can benefit all industrial, commercial or agricultural companies, taxed according to their actual profit (normal or simplified), whatever their legal form.

For the purposes of the scheme, basic research activities, applied research activities and experimental development activities are considered to be scientific or technical research operations.

Research expenses giving entitlement to the tax credit include:

- depreciation and amortization of fixed assets, created or acquired in new condition and used directly for carrying out scientific and technical research operations;
- staff costs relating to researchers and research technicians directly and exclusively assigned to these operations;
- other operating expenses exposed in the same operations: these expenses are fixed at a flat rate of 75% of depreciation charges and 43% of personnel expenses (200% in the case of newly recruited doctorate holders);
- research expenses entrusted in particular to public research organisations and to research organisations approved by the Research Ministry; and
- legal and expert expenses related to patent infringement actions.

5. The digital over-amortization device

Over-amortization system for investments by industrial SMEs in the field of robotics and digital transformation.

The State has reintroduced a system of tax amortization allowing industrial SMEs to deduct from its taxable profit up to 40% of the cost price of the goods and software contributing to its transformation towards the industry of the future, for any acquisition carried out in the period 2019-2020.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

There are several points of tax law that can lead to disputes between digital businesses and tax authorities in France:

- **Tax evasion:** this kind of fraud consists of voluntarily circumventing tax legislation through illegitimate schemes, unlike optimisation or planning where tax legislation is used in order to reduce tax by various legal means (derogatory regimes, use of tax exemptions, etc.).
- **Tax optimisation** (which may be abusive): unlike fraud, optimisation is legal even if its legitimacy or effectiveness can be challenged. Indeed, this strategy can be legally considered illegal insofar as it constitutes an abuse of rights (using legal mechanisms to escape tax); but demonstrating it in practice remains difficult for the tax administration. This is particularly the case when individuals or companies subject their income or profits in a country different from that where they have their economic interests, to very low or even zero tax rates, as in “tax heavens”. In relation to intellectual property, tax optimisation can be abusive for businesses (digital or physical) using tax schemes to avoid IP rights taxation.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

The main considerations to take before resourcing work concern qualification, duration and cost of the work.

French law provides for several types of contracts with different advantages and disadvantages for each. For example:

- **Interim work:** this type of temporary recruitment can be chosen in the case of special circumstances due to an increase in the activity of the company. The advantage of

this contract is that it can be ended easily, at the end of the mission. The disadvantages are that this work is more costly for the employer and may be a deterrent for talent retention.

- Fixed-term contract: if the need for labour is cyclical (increases in orders, new markets, etc.). This contract is only possible for the execution of a specific and temporary task. The advantage is that this contract can be ended easily at the contract term, or before in case of anticipated break. This contract is easy to set up and is less expensive for the employer than interim work. However, labour law is very strict on the type of employment contract chosen, in favour of the protection of the employee. For example, a succession of fixed-term contracts (type of contract more precarious because temporary and less restrictive for the employer) on the same workstation for the same person can be reclassified as a permanent contract.
- Permanent contract: if the need is permanent and structural. The inconvenience with this kind of contract is that its termination is subject to compliance with labour law rules. As there is not a fixed term, the only way to end this contract is either resignation, mutual agreement, or dismissal, which can be expensive for the employer because dismissal implies payment of an indemnity (except in cases of gross negligence). Furthermore, improper dismissal can be challenged at Court.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

The legal provisions relating to teleworking are provided for in articles L.1222-9 *et seq.* of the Labor Code since Law No. 2012-387 of March 22, 2012.

The provisions governing teleworking are found in articles 1222-9 to 1222-11 of the Labor Code.

Teleworking is defined as “any form of work organisation in which a work which could also have been carried out on the employer’s premises is carried out by an employee outside these premises on a voluntary basis using information and communication technologies” (article L.1222-9 of the Labor Code).

Teleworking within a company can be regular or occasional. The employer can offer all of its employees the benefit of teleworking or only a selection of them.

The Labor Code provides that teleworking is set up by collective agreement or as part of a charter drawn up by the employer after consulting the social and economic committee (article L.1222-9 of the Labor Code). The agreement or charter must regulate the conditions for using telework as well as the procedures for exercising it (article L.1222-9 of the Labor Code).

In the absence of a collective agreement or charter, an employee and his employer can jointly decide to use teleworking. The Labor Code provides that they can formalise their agreement freely, by any oral or written means. An amendment to the employment contract is not necessary.

Employees teleworking on an occasional or permanent basis benefit from the same individual and collective rights as other employees of the company (article L.1222-9 of the Labor Code).

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

With the Covid-19 crisis, the use of teleworking has almost become the rule in France.

Indeed, according to the words of the Prime Minister Jean Castex: the use of teleworking must be the rule; while the work “on site” must remain the exception.

It has been really democratised since 2020 and employees love to use it. For many, the end of the crisis will be marked by this important step in their lives, but also a willingness to share working time on the company’s premises but also outside the company’s premises.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Digital businesses can face several legal barriers. For example:

- Offering for sale products or services prohibited or limited to sale or contrary to public order.
- Use of protected intellectual property rights (author’s rights, trademark, domain name), which can lead to a dispute with the right holder, or to a refusal for use (domain name already reserved for example).
- Compliance with the legal obligations for e-commerce websites (see section 1).
- Compliance with legal requirements for digital contents (GDPR and privacy/confidentiality provisions notably).
- Legal liability, in particular for content host, seller or publisher.
- Compliance with competition law provisions (denigrating a competitor, using and abusing comparative advertising for competitive purposes, etc.).

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Digital businesses operating in France benefit from several advantages, notably:

- Tax incentives (please see the answer to question 8.1: tax reductions applicable to capital subscriptions for young innovative companies; tax reductions applicable to capital subscriptions for new businesses; tax rate (income tax or corporate tax) reduced to patent and trademark licence fees; research tax credit applicable to R&D expenses; and the digital over-amortization device).
- The development of e-buyers: according to the FEVAD, e-commerce is an increasingly dynamic market.

The advantages inherent to e-commerce: opening an online store is an easily funded project that requires a low start-up budget and very little time; the possibility of working anywhere in the world, which increases sales power; development of website design and marketing strategies; and greater ease of adaptation.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The Digital Services Act (DSA) and the Digital Markets Act (DMA) aim to regulate “digital platforms”, such as social networks, video content sharing platforms, online marketplaces and search engines (e.g. Google, Bing, etc.). The objective is to make these large online platforms more accountable, in particular with regard to their necessary role in the fight against

the online distribution of illegal or damaging content and their market behaviour, in order to prevent market blocking practices and obstacles to innovation and the development of alternative offers.

These draft reforms introduce new rules to prevent these major platforms from controlling the market and imposing unfair commercial or technical conditions. They also aim to oblige platforms to equip themselves with the necessary means to fight against the online distribution of illicit or dangerous content for their users. Social networks, online marketplaces (large online sales platforms) and content sharing platforms, in particular, are affected by the proposed changes.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Lastly, the DSP2 (Payment Services Directive), which was transposed into French law by an ordinance n° 2017-1252 of August 9, 2017, includes several components and introduces new rules of direct interest to consumers including the obligation of strong authentication (that is to say at least two factors between a code or password that we know, a device that we have, biometric data such as the fingerprint, voice or iris) for online payments of more than EUR30, to reduce fraud in e-commerce.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The DSP2 – effective January 1, 2021 – is a new European regulation which requires all online payment providers (banks and e-merchants) to carry out strong authentication of online transactions over EUR30.

This new directive will therefore upset the daily life of e-commerce sites and banks.

Indeed, it is the responsibility of banks to provide such authentication guarantees, and no longer of online merchants.

In addition, this directive defines the legal status of account aggregation services and payment initiators. From now on, these two activities must be carried out by approved service providers. The directive establishes their conditions of exercise and the manner in which they must operate with the banks of their customers.

The main parties to the changes incurred by this directive are banks, technical payment operators and merchants. All must now connect to a new version of the secure payment protocol on the internet (3-D Secure), which will allow banks, merchants and customers to connect to each other to trigger enhanced authentication and validate the transaction.

For online merchants in France, the challenge is not to slow down online shopping and therefore the development of e-commerce.



Catherine Mateu, partner at Armengaud & Guerlain, has more than 20 years of experience in French and European intellectual property law, serving clients that range from inventors, designers, nonprofit groups and local start-ups to multinational corporations. Her practice focuses on finding timely and cost-effective solutions to a wide array of patent, copyright, trademark, design infringement, licensing matters and strategic advisory.

She is bilingual in French and Spanish, and fluent in English and Basque.

Catherine Mateu is a regular speaker at Intellectual Property conferences, and has been ranked in industry publications such as IP Stars, The Legal 500, Les Décideurs, Women in Business Law, Chambers and Who's Who.

AIPPI – Chair of the TRIPS Committee and INTA – Vice-chair of the Emerging Issues Committee and the French contributor to Trade Dress International Practice and Procedures.

Armengaud Guerlain
12, Avenue Victor Hugo
75116 Paris
France

Tel: +33 1 47 54 01 48
Email: c.mateu@armengaud-guerlain.com
URL: www.armengaud-guerlain.com

Armengaud Guerlain, founded in 1993, is a law firm fully specialised in intellectual property (patents, trademarks, designs and models, and copyright) and the related issues of unfair competition, consumer law, advertising rights (particularly comparative advertising), and the Internet. Reflecting its well-recognised expertise, the firm has worked with a wide variety of French and international clients, from artists and inventors to blue-chip companies, governments, and state-owned enterprises. In addition to French, the firm's daily working languages include English and Spanish.

Armengaud Guerlain works with a network of foreign colleagues selected for their high level of technical expertise and their use of complementary work methods, thereby enabling the firm to manage files simultaneously in several countries. Each file is treated in a collaborative manner and the firm places particular emphasis on maintaining lasting, high-quality relationships with its clients, combining competence and reactivity.

Since its founding, the firm regularly appears in the rankings of top law firms established by specialised publications including WTR, IAM, Who's Who Legal, The Legal 500, Chambers, Les Décideurs, Managing Intellectual Property and IP Stars.

www.armengaud-guerlain.com



Germany

SKW Schwarz



Dr. Christoph Krück



Franziska Ladiges



Alexander Möller



Heiko Wunderlich

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

Numerous information obligations exist in e-commerce in Germany. Due to the complexity of the topic and the large number of contradictory case law, the following information can only cover part of the problem.

Regardless of whether sales are made to entrepreneurs or consumers, the German Civil Code lays down a number of obligations. The trader must *inter alia*:

- provide technical means by which the customer can identify and correct input errors before placing his order;
- confirm receipt of the customer's order;
- provide the possibility to retrieve and save the terms and conditions of the contract; and
- provide the following information before placing an order:
 - individual technical steps leading to the contract;
 - whether the text of the contract is saved by the trader after the conclusion of the contract and whether it is accessible to the customer;
 - how the entrepreneur can recognise and correct input errors with the technical means provided before submitting the contractual declaration;
 - the languages available for the conclusion of the contract; and
 - any relevant codes of conduct to which the entrepreneur subscribes, as well as the possibility of electronic access to these codes.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Due to the complexity of the topic and the large number of partially contradictory rulings in Germany, the following information can only cover part of the problem.

Furthermore, there are specific rules on an EU law level in particular regarding terms and conditions of providers of online

platforms, where an entrepreneur contracts with consumers: Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services ("Platform-2-Business-Regulation").

Regardless of being such online platform provider, the following rules apply to e-commerce:

Information obligations before concluding a contract with a consumer

The consumer must be provided with the following information *before* the conclusion of the contract:

- essential characteristics of the products;
- identity, address, telephone number and, where applicable, fax number and e-mail address of the trader;
- total price of the product (including all taxes and duties, as well as any additional shipping costs and any other costs);
- cost of using the means of distance communication used for the conclusion of the contract, if the consumer is charged with costs that exceed the cost of merely using the means of distance communication;
- terms of payment, delivery and performance, the deadline by which the entrepreneur must deliver the goods or provide the service, and, if applicable, the entrepreneur's procedure for dealing with complaints;
- existence of a statutory right of liability for defects;
- where applicable, the existence and terms of after-sales services and guarantees;
- relevant codes of practice, if any, and how copies may be obtained;
- where applicable, the duration of the contract or the terms of termination of contracts of indefinite duration or automatically renewing contracts;
- where applicable, the minimum duration of the consumer's obligations under the contract;
- where applicable, the fact that the entrepreneur may require the consumer to provide a deposit or other financial security, and their conditions;
- where applicable, the functioning of digital content, including applicable technical protection measures for such content;
- where applicable, to the extent material, limitations on the interoperability and compatibility of digital content with hardware and software, to the extent that such limitations are known and need to be known by the trader; and
- where applicable, that the consumer may use an out-of-court complaint and redress procedure to which the trader is subject and its access requirements.

Confirmation of the contract

In addition, there is an obligation to provide the consumer with a copy or confirmation of the contract on a data carrier and within a reasonable period of time.

Exceptions from applicability

An exception exists if the conclusion of the contract does not take place within the framework of a distribution or service system organised for distance selling; for example, if a supplier sells goods via a store and only accepts telephone orders as an exception. Also, the following contracts are also excluded from distance selling law:

- on notarized contracts;
- on the establishment, acquisition or transfer of ownership or other rights to real property;
- concerning the construction of new buildings or substantial alterations to existing buildings;
- for travel services;
- on the transportation of persons;
- on part-time residential rights, long-term vacation products, mediation and exchange systems;
- treatment contracts;
- on the supply of food, beverages or other household goods for daily use;
- concluded with the use of vending machines and automated business premises;
- concluded with operators of telecommunication means with the use of public coin and card telephones for their use;
- for the use of a single telephone, Internet or fax connection established by a consumer;
- contracts concluded away from business premises, where the service is provided and paid for immediately upon conclusion of the negotiations and the consideration payable by the consumer does not exceed EUR 40; and
- on the sale of movable property on the basis of execution or other judicial measures.

Right of withdrawal

If a consumer concludes a legal transaction online, he or she may be entitled to a right of withdrawal. Certain services are excluded from the scope of distance selling law, e.g., contracts for travel services concluded at a distance, or contracts for the delivery of food, beverages or other household goods for daily use that are delivered at a consumer's domicile, place of residence or place of work by an entrepreneur in the course of frequent and regular trips. In addition to the exceptions to distance selling law, there are also exceptions to the right of withdrawal. A right of withdrawal does not apply, for example, to contracts:

- for the delivery of "customer specification";
- for the delivery of perishable goods;
- for the delivery of sealed goods, which are not suitable for return due to health protection or hygiene reasons;
- for the delivery of audio or video recordings or computer software in a sealed package, if the seal has been removed after delivery; or
- for the delivery of newspapers, periodicals or magazines with the exception of subscription contracts.

In those cases in which a right of withdrawal does not exist or may expire, the entrepreneur must inform the consumer of this fact.

Expiration of the right of withdrawal for services and downloads

The right of withdrawal expires in the case of a contract for the provision of services if the entrepreneur has provided the

service in full and has only begun to perform the service after the consumer has given his express consent.

Furthermore, the consumer also has a right of withdrawal for digital content. This includes downloads and streaming, for example. However, this right of withdrawal expires before the end of the withdrawal period if the entrepreneur has started to perform the contract after the consumer (1) has expressly agreed that the entrepreneur begins with the execution of the contract before the expiry of the withdrawal period, and (2) has confirmed his knowledge that by giving his consent he loses his right of withdrawal upon commencement of the performance of the contract.

Withdrawal period start and duration

The revocation period is 14 days. The period can already begin with the conclusion of the contract (e.g. in the case of downloads); in the case of delivery of goods, the period begins with receipt of the goods. If the entrepreneur has not (properly) informed the consumer about his right of withdrawal, the withdrawal period expires after 12 months and 14 days.

Withdrawal policy

The entrepreneur must inform the consumer about the right of withdrawal. The legislator provides templates for this purpose. The entrepreneur can use this, but does not have to. Choosing the right text module from the design instructions can be extremely complicated.

Further obligations in e-commerce

Information on delivery restrictions and means of payment

In online stores, consumers must be informed whether delivery restrictions exist and which means of payment are accepted. The entrepreneur must also provide the consumer with at least one common and reasonable free method of payment. These are, for example, direct debit, credit card or payment in advance. If additional, chargeable means of payment are also made available, the agreed fee may not exceed the costs incurred by the entrepreneur through the use of the means of payment.

"Button solution"

The entrepreneur must design the ordering process in such a way that the consumer expressly confirms with his order that he undertakes to pay. In doing so, the order button must be clearly legible, contain only the words "zahlungspflichtig bestellen" or other unambiguous wording. Wording such as "order" or "place order" or "continue" should not be used. The consequence of mislabeling the order button is that no contract is concluded with the consumer.

Obligations in technical terms

When concluding a contract, e.g. in an online store, the entrepreneur must:

- provide adequate, effective and accessible technical means by which the customer can identify and correct input errors before placing his order; and
- communicate the following information in a clear and comprehensible manner in good time before the consumer places his order:
 - the individual technical steps leading to the conclusion of the contract;
 - whether the text of the contract is stored by the entrepreneur after the conclusion of the contract and whether it is accessible to the customer;
 - the languages available for the conclusion of the contract;

- all relevant codes of conduct to which the entrepreneur subscribes, as well as about the possibility of electronic access to these codes;
- confirm the receipt of his order electronically without delay; and
- provide the opportunity to retrieve the contractual provisions, including the General Terms and Conditions, upon conclusion of the contract and store them in reproducible form.

Online dispute resolution

Due to the EU Regulation on the Online Settlement of Consumer Disputes (ODR Regulation), companies offering online sales contracts or online service contracts, as well as companies offering their goods or services through online marketplaces established in the Union, must post an easily accessible link to the ODR platform on their website. The ODR platform can be accessed via the following link: <http://ec.europa.eu/consumers/odr/>.

To ensure that the link is easily accessible for consumers, it is advisable to include it in the imprint.

Imprint obligation

Anyone offering goods or services on a businesslike basis on the Internet must, as a matter of principle, provide certain information in a clearly visible place on their website. It should be clearly marked as “*Impressum*” and placed in such a way that a user can find it without problems (no long scrolling, not too many links).

Information must be provided about:

- the name (if applicable, the complete company) and the postal address of the provider (P.O. Box and e-mail address are not sufficient);
- in the case of legal entities (such as the GmbH and the AG), additionally the legal form, the name of the person authorised to represent the company and, if information is provided about the capital of the company, the share or nominal capital and, if not all contributions to be made in money have been paid in, the total amount of the outstanding contributions;
- the e-mail address and fax number, which is information that enables rapid electronic contact and direct communication. The ECJ has provided clarity regarding the classification of telephone numbers in this area through its ruling in October 2008. It ruled that there are communication channels other than the telephone that satisfy the criteria of direct and efficient communication, such as the fax. Accordingly, the provision of a telephone number is not required;
- the commercial register, partnership register, register of cooperatives or register of associations responsible for the provider, including its register number (if it is registered in one of these registers);
- details of the competent supervisory authority (name, postal address, telephone number), if the activity performed requires state approval (for example, in the brokerage and property development trades, insurance brokerage) and professional details in the case of regulated professions;
- the sales tax identification number (VAT ID number) if available (the normal tax number does not have to be indicated on the Internet) or the business identification number; and
- in the case of stock corporations, partnerships limited by shares and limited liability companies that are in liquidation or being wound up, the details thereof.

According to the State Media Treaty, providers of journalistic and editorial content must state the name and address of the person responsible for the content of journalistic and editorial content (applies only to so-called media services).

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

There have been no relevant changes in German law regarding data protection in the last year (2020).

However, online sellers should keep in mind that the European Court of Justice declared the EU-US-Privacy-Shield void. In the case that the online shop uses US-American service providers, the data transfer to those service providers should be reviewed and if necessary new guarantees for transferring data should be concluded.

Moreover, the development of the E-Privacy-Regulation should be kept in mind.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

One of the biggest hurdles in this area is likely to be the legally compliant aggregation of data, some of which is also particularly sensitive. In addition, data is often exchanged with third countries.

All of these topics are closely monitored by the data protection supervisory authorities, and some of the requirements are changing rapidly, e.g., third-country transfers. In this respect, it is important that special attention is paid to technical data security. In addition, the principle of data minimisation should be strictly observed.

Another hurdle in this area is likely to be the guarantee of data subject rights. In particular, the obligation to provide information must be observed. The data subjects should be informed as precisely as possible about the processing.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Both the German government and data protection regulators are open to developments in fintech, digital health and AI. The development of new ideas and projects is closely monitored and the data protection supervisory authorities in particular are always available to answer questions.

In addition, various working papers have already been published on these topics, e.g. on AI or the digital health sector. With regard to AI, the Data Protection Conference has already defined the following seven requirements in 2019:

- AI must not turn people into objects;
- AI may only be used for constitutionally legitimised purposes and may not override the requirement of purpose limitation;
- AI must be transparent, comprehensible and explainable;
- AI must avoid discrimination;
- the principle of data minimisation applies to AI;
- AI needs accountability;
- AI needs technical and organisational standards.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

Legal requirements for greater cyber security create the conditions for citizens and businesses to move freely and securely in the digital space and to trust the use of information and communications technology. As a significant milestone in German digitisation policy, the IT Security Act entered into force back in 2015.

Legal amendments were made to telecommunications and tele media law to increase security on the internet in general. This created a legal framework in which government and industry work together for greater cyber security.

Furthermore, e-commerce businesses have to comply with the security regulations in the GDPR, especially implementing technical and organisational security measures.

A directive on measures to ensure a high common level of security of network and information systems in the Union has been created at the European level (Directive (EU) 2016/1148). Only a few additions were necessary in 2017 to implement the requirements of the NIS Directive in Germany. In addition, the options for detecting and blocking cyber-attacks were expanded in telecommunications law.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The IT Security Act introduced binding minimum requirements and reporting obligations for operators of critical infrastructures in the Federal Office for Information Security Act (BSI Act). The role and powers of the Federal Office for Information Security (BSI) were significantly strengthened. The seven CRITIS sectors are covered:

- Energy.
- Water.
- Food.
- Information and Communication Technology.
- Transport and traffic.
- Health.
- Finance and insurance.

Competent authorities under the BSI Act have a range of enforcement instruments ranging from investigation and information measures to binding orders and administrative fines.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

German consumers – in particular age 40+ – are still rather cash-friendly and conservative when it comes to adopting new technologies.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The opposite: there is no debit card culture. It seems that

“purchase on account” is something which is still attracting many (older) German consumers.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

No.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

It seems that Austria, UK, France, Spain, Italy and/or Netherlands are typical further markets that are targeted; typical further supported languages are therefore English, French Spain, Italian and/or Dutch.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

No.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Most likely Germany became more e-commerce friendly during the pandemic, which will possibly last.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In cases where an online platform does not provide a specific intellectual property protection scheme, sending warning letters is the common way to stop infringers out of court. Such warning letters usually require that the infringer provides a cease-and-desist declaration, including an obligation to pay a contractual fine for any case of future violation and are sufficient to stop an allegedly illegal activity. If the infringer does not provide such declaration, the rights holder may apply for an (immediate) court action. In court, the rights holder can enforce its right by a preliminary injunction or a principal proceeding. Contrarily to preliminary injunctions, proceedings on the merits provide conclusive and final resolution of the matter but will not be issued as rapid.

In many online infringement cases, the rights holder can choose the court where to bring the proceeding.

Besides civil proceedings, a rights holder can also seek criminal proceedings and border measures to enforce its rights.

The court may not only issue injunctions against infringers but also against intermediaries, like online platforms and/or marketplaces, whose activities are used by a third party to infringe IP rights, when the intermediary has contributed to the infringement in a way, e.g. by failing to observe certain duties, including insufficient measures to prevent such infringements. The duty to examine, e.g., arises for a provider of the platform as soon as he has been informed of an infringement of IP rights.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Requesting a preliminary injunction (see above) requires the matter to be considered urgent. Therefore, there is a certain timeframe in Germany within which rights holders need to apply for a preliminary injunction. This time limit is at the court's discretion; some courts are rather strict (one month), but most courts accept time limits of four to six weeks, starting from the time when the rights holder first obtained knowledge of the infringement.

Under certain circumstances, luxury product manufacturers can set up a selective distribution system to protect the image of their luxury goods by preventing their products being sold on third-party platforms (e.g. eBay, Amazon). Such schemes are only compatible with competition law when the properties of the product necessitate a selective distribution system, when resellers are chosen on the basis of objective criteria of a qualitative nature which is determined uniformly for all potential resellers and applied in a non-discriminatory manner; and the restrictions do not go beyond what is necessary. Where the criteria are not met, manufacturers of luxury products cannot prohibit their resellers from using third-party online platforms.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

There are no specific legal requirements for cloud providers and data centres in Germany.

In both cases, data privacy and data security play a major role in assessing whether to contract with a provider or not, but this is governed by the general principles of GDPR.

Regarding cloud services, questions of international data transfer also regularly play a further major role.

In practice, cloud or SaaS providers mostly offer standard software for a large number of customers. This leads to the scalability and lower costs. This, however, is often accompanied by a lack of customisability for the customer and, in some cases, the customer's individual maintenance and support needs cannot be met. On the other hand, the provider can regularly offer flexible performance, remuneration and termination models.

In the context of cloud computing, the rules on the transfer of personal data to third countries in accordance with Art. 44 *et seq.* GDPR have to be complied with. Also, in particular, if the SaaS solution involves the storage of data on the provider's servers, this should regularly constitute a controller-processor situation within the meaning of Art. 28 of the GDPR and a processing agreement becomes necessary.

Despite the trend towards the cloud, however, a data centre can also play an important role within the IT-strategy of a company. It can be used, for example, if individual (high) security or (high) availability levels are to be realised for individual IT systems, which cannot be offered as part of a cloud solution. It can therefore be part of a company's IT security strategy and is therefore also used to implement redundant systems and as part of disaster recovery plans, e.g. by mirroring the primary systems at the housing provider. Also, issues such as fire protection, (emergency) power supply or air-conditioning technology can be outsourced to the data centre provider.

The range of services offered by data centres is broad and extends from additional services such as "remote hands", to individual security precautions at the server rack, to individual data backup models. If, for example, the "remote hands" service is used, it may be necessary to conclude a data processing agreement in accordance with Art. 28 GDPR with the provider.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

There are no specific strict requirements to locate servers/data centres in Germany. However, the general requirements of GDPR must be complied with. Data protection requirements with regard to cloud computing can be challenging, since the virtualisation and grid computing technology behind the business model is based on a flexible pooling of resources that are typically not located in only one jurisdiction; the distribution of data across different time zones, in fact, often brings further efficiencies. This gives rise to the typical challenges of transferring personal data to third countries pursuant to Art. 44 *et seq.* GDPR.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The IT procedure ATLAS (Automated Tariff and Local Customs Clearance System) ensures largely automated clearance and monitoring of cross-border goods traffic. With ATLAS, written documents of customs clearance (e.g. customs declarations, import duty notices) are replaced by electronic messages. In this way, the customs administration provides the conditions required in Article 4a (1) of Regulation (EEC) No. 2454/93 (Customs Code Implementing Regulation, CCIP) for the largely automated clearance and monitoring of cross-border goods traffic.

The declaration data is stored centrally and can be read or processed by the responsible offices of the customs administration (e.g. customs offices, main customs offices, customs investigation offices). ATLAS transmits the data required for customs clearance to other EU member states, so that communication with other customs administrations within the EU is largely handled electronically.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

One of the biggest hurdles to digitisation is likely to be the scepticism of the companies, authorities and private individuals involved, especially when personal data is involved. As soon as German citizens are asked to provide data to a company or public authority digitally, they question whether the data is secure and, above all, what will happen to the data. Companies can counter this scepticism primarily with proper data protection management.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

There are no special tax incentives for digital businesses. However, entrepreneurs being active in digital business can get the same incentives as any other businesses. With regard to start-ups, one of the most important tax regulations might be § 8d *Körperschaftsteuergesetz* (Corporate Income Tax Law) – so-called “*Fortführungsgebundener Verlustvortrag*” (going concern loss carry forward), which states that a loss carry forward will not cease due to a change in ownership (e.g. during a finance round) if the business will be continued in the same way, as in the past.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Some other very important changes will be made in the area of VAT. Beginning July 1, 2021, new rules apply for VAT entrepreneurs running platforms, especially § 25e *Umsatzsteuergesetz* (Value Added Tax Code). According to those rules, the enterprise running the platform is – under certain circumstances – liable for the VAT on the turnover of the entrepreneurs using the platform for their business. Thus, it is likely that in the first time these new rules will lead to some uncertainty in the practical appliance and thus, we expect some disputes between the tax authorities and the taxpayers. Taxpayers running such a platform should inform and take all necessary measures to make sure that they are not liable for any VAT issues of the users of the platform. In some cases, it might be necessary to establish a control process, etc. to be able to perform all legally required controls.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In general, a company can hire staff on an employment or a freelancer basis. A hire through a regular employment relationship triggers several financial and legal disadvantages for a company, such as the obligation to carry off contributions to social security and income taxes or a restriction in flexibility in connection with a reduction of the workforce – both do not apply in relation to persons hired on a freelancer basis. Insofar, using employees for your business is much more cost intensive in comparison to using freelancers. However, there is a significant practical advantage in using employees, namely the right to give instructions. In contrast to freelancers, employees can be instructed – among others – (i) to work in a certain manner, (ii) to work in a specific location, (iii) to work at a certain hour, and (iv) to combine (i)-(iii) at the same time. For that matter, the

company has to decide which model fits best, i.e. is a strong integration into the operation necessary or not. Typically, companies prefer the comfort of being able to have a certain task done at its discretion, which is why they choose regular employment relationships. If this model is chosen, companies have to decide whether the staff shall be hired on a fixed-term contract basis or for an indefinite term. Taking the challenging market for new hires into account, companies nowadays decide against fixed-term contracts as suitable candidates ask for indefinite contracts and even mark that a possible “dealbreaker”.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no general mandatory requirements that explicitly relate to work away from the premises. However, companies have to make sure that mandatory regulations are complied with at all times. Most notably, this applies to compliance with mandatory working hours requirements and with mandatory obligations on confidentiality as well as data privacy. In case employees are granted remote working, such as from home, then companies also need to take safe and healthy regulations into account.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

First, a continued abandonment of office work. Both, companies and employees have experienced the advantages of remote working, and since the pandemic, which has lasted now for over a year, have embraced as well as solve many practical challenges in organising work streams. At the same time, companies have seen the financial advantages of remote working. It is no longer necessary to rent large expensive downtown office premises to keep your organisation on track; moreover, savings in office rents are of permanent nature which mitigates the financial need to reduce the workforce. Second, a new set of management skills will further develop. Company leadership was forced to adapt to a new world in which employees could no longer be monitored in a classic fashion. New methods to motivate the team but also to monitor the team were necessary – and both are still a work in progress. Managers need to develop new practical means to lead a team and get the best of team members, considering that only some team members, if at all, will be present in office at the same time.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

According to our understanding there are no real legal barriers for a digital business operating in Germany. However, depending on the field of business, there might exist some hurdles, such as data protection rules for data driven businesses.

Moreover, the German government did not push the development of digital infrastructure enough in the past years. Although some progress has been made in recent years, there is still a lot of work to be done in Germany.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Since the German government wants to make up for the failures of recent years in the development of digital infrastructure, there are currently good opportunities for correspondingly innovative companies. Germany is also seeing the emergence of an increasingly large start-up market, which is even being supported by the government in the area of digital business.

With more than 83 million inhabitants, Germany is therefore a major market for digital businesses. Added to this is the availability of well-trained specialists.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

To enable SMEs to exploit the economic potential of digitisation, the German Federal Ministry for Economic Affairs and Energy (BMWi) supports small and medium-sized enterprises (SMEs) with the “Digital Now – Investment Support for SMEs” programme. The programme offers financial grants and is designed to encourage companies to invest more in digital technologies and in the qualification of their employees.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The online payment sector in Germany is governed by EU law – Payment Service Directive (EU) 2015/2366 and Commission Delegated Regulation (EU) 2018/389. The Directive is implemented by the German Civil Code (civil law) and the German Payment Services Supervision Act – ZAG (regulatory aspects).

Pursuant to the ZAG, every institution wishing to provide payment services in Germany needs an authorisation from the Federal Financial Supervisory Authority (BaFin). The authorisation is even needed when a non-German company offers payment services to companies or individuals having their registered office or regular residence in Germany.

Having received the authorisation, the companies offering payment services are being supervised by the BaFin on a regular basis depending on the scope of risks.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

In order to increase security of online payments and reduce fraud, service providers have to comply with strict technical requirements when verifying customer's identity (PSD2). Stronger security requirements will help to increase the number of customers using online payment providers in Germany.



Dr. Christoph Krück specialises in digital business and data protection law. In this context, one focus is on advising online platforms and other online services on platform and media regulation, youth protection law, platform liability (safe harbor provisions; notice-and-take-down), as well as on any other requirements of e-commerce, consumer and competition law. Furthermore, he advises on the drafting of terms of use, general terms and conditions, licensing, cloud and other IT contracts.

With regard to data privacy law, he advises on the general requirements of the GDPR and is particularly focused on issues relating to the internet as well as big data and platform structures. In addition, he closely monitors the developments concerning regulation of artificial intelligence and algorithms.

SKW Schwarz
Wittelsbacherplatz 1
80331 München
Germany

Tel: +49 89 286 40-248
Email: c.krueck@skwschwarz.de
URL: www.skwschwarz.de



Franziska Ladiges advises clients on all questions of IT and data protection law. Thanks to secondments and many years of experience, she has in-depth knowledge of data protection. In this area, she supports companies (from small businesses to listed companies) from various industries with the implementation of data protection compliance. In addition, she advises on various individual data protection issues, including order processing, data subject rights and international data transfer. Finally, she regularly carries out data protection quick checks for companies on site.

In addition, Franziska Ladiges has experience in drafting contracts regulating the creation, use or transfer of software. She also drafts and reviews general terms and conditions (both purchasing and sales and internet platforms) and advises on the development of online shops and internet platforms. She often represents her clients before state courts in contract disputes or data protection matters.

SKW Schwarz
Mörfelder Landstraße 117
60598 Frankfurt
Germany

Tel: +49 69 630001-29
Email: f.ladiges@skwschwarz.de
URL: www.skwschwarz.de



Alexander Möller advises national and international companies on all issues relating to employment law, particularly in connection with reorganisation measures. His practice focuses on strategic and operational support for such measures and the preparing and carrying out of necessary procedural steps towards the works council and the workforce. His work also focuses on drafting and revising the contract portfolio of companies (e.g., employment, termination, and settlement agreements as well as contracts on the use of recruitment agency personnel). Mr. Möller advises and trains company executives to identify potential for action and optimisation at an early stage.

SKW Schwarz
Mörfelder Landstraße 117
60598 Frankfurt
Germany

Tel: +49 69 630001-35
Email: a.moeller@skwschwarz.de
URL: www.skwschwarz.de



Heiko Wunderlich advises companies and private individuals on tax matters, as well as on tax and procedural law. His work includes tax advice on succession planning and estate planning for entrepreneurs and private individuals, as well as on corporate acquisitions, restructuring, and financing. He also advises on international tax law and has special expertise in the media and entertainment sectors.

SKW Schwarz
Wittelsbacherplatz 1
80331 München
Germany

Tel: +49 89 286 40-321
Email: h.wunderlich@skwschwarz.de
URL: www.skwschwarz.de

As one of the leading law firms in Germany, we tackle today what will be the decisive legal issues of tomorrow. Digital change, disruptive technologies, and innovative business models transform markets and societies. As technology challenges the status quo, unprecedented legal questions arise. Enter **SKW Schwarz**. Our lawyers address these questions in prompt and yet sustainable ways. Our point of view is holistic but geared towards innovation. We have four office locations in German business hubs, accommodating more than 130 lawyers. In addition, we network with partner firms worldwide. We advise companies in all fields of national and international business law. Our professional expertise enables us to handle large cases of any complexity. At the same time, we are more personal and more dynamic than the very large law firms.

www.skwschwarz.de

**SKW
Schwarz
Rechtsanwälte**

India

G&W Legal



Disha Mohanty



Arjun Khurana

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

In India, there is a great degree of overlap in legislations governing e-commerce and non-e-commerce businesses, such as the requirements for setting up a business, employment laws, and legal metrology legislations.

The following are the legislations that are specifically applicable to B2B e-commerce:

Foreign Direct Investment (FDI) Policy: The applicable foreign exchange control regulations that govern foreign investments and setting-up of a business in India by foreign entities and individuals are the prevailing Foreign Direct Investment Policy and the Foreign Exchange Management Act, 1999 with the accompanying Rules. The FDI Policy prescribes: the maximum ownership that a foreign individual or a foreign entity can have in an Indian entity engaged in certain business activity; the nature of business entity which can be established; the quantum of investment to be made for setting up or acquiring a business; and various other conditions that an Indian entity with foreign investment should comply with.

100% foreign direct investment is permitted in companies engaged in Cash and Carry Wholesale Trading and B2B e-commerce business. Such investment can be made without prior approval of Government of India.

Cash and Carry Wholesale Trading, including sale through B2B e-commerce, would mean sale of goods or merchandise to retailers, industrial, commercial, institutional or other professional business users as opposed to end-consumer or retail customer for personal consumption.

The following conditions apply on companies with foreign direct investment engaged in B2B e-commerce:

1. **Customers to whom goods can be sold:** Sales should be made to retailers, industrial, commercial, institutional or other professional business users, namely:
 - i. entities holding the applicable tax registration;
 - ii. entities holding trade licences (i.e. a licence or registration certificate, or membership certificate, or registration under the Shops and Establishment Act issued by a Government Authority reflecting that the entity or person holding the licence or registration certificate or membership certificate is engaged in a business involving commercial activity);

iii. entities holding permits or a licence for undertaking retail trade; or

iv. institutions having a certificate of incorporation or registration as a society or registration as a public trust for their self-consumption.

2. **Records to be maintained:** Companies engaged in B2B e-commerce should maintain a complete record of sales on a day-to-day basis, such as the details of customers, their legal nature (whether it is a company, partnership firm, sole proprietorship, trust, or society), their registration, licence or permit numbers, and the value of sale.
3. **Sales to group companies:** Sales of goods to group companies should not exceed 25% of the total turnover of the company engaged in Wholesale Trading.
4. **Other registration and licences:** All other registration and licences under the local laws as may be applicable to other entities engaged in similar business should be obtained.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Certain specific legislations in context of B2C e-commerce are:

- **Foreign Direct Investment (FDI) policy:** The FDI policy categorises models of business as marketplace model (the provision of an information technology platform by an e-commerce entity on a digital and electronic network to act as a facilitator between buyer and seller) and inventory-based model (where the inventory of goods and services is owned by e-commerce entity and sold directly to consumers). FDI is allowed in a marketplace model wherein the e-commerce entity just provides a platform for buyers and sellers. The B2C e-commerce entities with foreign investments will have to comply with the following:
 - (i) Entities providing e-commerce services should be registered as a company under the Companies Act, 2013 (or under the Companies Act, 1956).
 - (ii) E-commerce entities are permitted to enter into transactions with sellers registered on its platform on a B2B basis.
 - (iii) E-commerce entities can provide support services to sellers in respect of warehousing, logistics, order fulfilment, call/customer services, payment collection and other services. Such services could be provided to

vendors on the platform on an arm's length basis, and in a fair and non-discriminatory manner by the e-commerce entity or other entities in which the e-commerce marketplace entity has direct or indirect equity participation or common control.

- (iv) E-commerce entities should not exercise ownership or control over the inventory (i.e. goods purported to be sold). Such an ownership or control over the inventory will render the business an inventory-based model. Inventory of a vendor will be deemed to be controlled by an e-commerce entity if the e-commerce entity permits more 25% of its sales to be affected by one vendor or its group companies.
- (v) An entity having equity participation by an e-commerce entity or its group companies, or having control over its inventory by an e-commerce marketplace entity or its group companies, is not permitted to sell its products on the platform run by such e-commerce entity.
- (vi) The website/platform where goods/services are made available for sale electronically should clearly provide the name, address and other contact details of the seller.
- (vii) Delivery of goods to the customers and customer satisfaction will be the responsibility of sellers of goods.
- (viii) Payments for sale may be facilitated by the e-commerce entities in conformity with the guidelines of the Reserve Bank of India.
- (ix) Any warrantee/guarantee of goods and services sold will be the responsibility of the sellers.
- (x) E-commerce entities cannot directly or indirectly influence the sale price of goods or services and shall maintain a level playing field in a fair and non-discriminatory manner.
- (xi) E-commerce entities will not mandate any seller to sell any product exclusively on its platform only.
- (xii) E-commerce entities will have to obtain a report from a statutory auditor by September 30th of every year for the preceding financial year confirming compliance of the e-commerce guidelines under the FDI Policy.

- **Consumer Protection Act, 2019 (CPA 2019) and the Consumer Protection (E-Commerce) Rules, 2020 (Rules):** These legislations are applicable to all B2C e-commerce entities. The Rules apply to both local and international e-commerce entities irrespective of where they are established. The E-commerce Rules govern, among other things, grievance redressal mechanisms, the requirement to appoint a nodal person to ensure compliance with the provisions of CPA 2019 and the E-commerce Rules, the obligations and liabilities of the e-commerce entity, false representation, violation of intellectual property, and manipulation of prices.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

India does not yet have dedicated data protection legislation. The Information Technology Act, 2000 (IT Act), read with its companion rules and regulations such as the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011, along with a host of other sectoral regulations, seek to cover issues involving

electronic transactions, cybersecurity, cybercrimes, etc., which confer upon citizens some degree of data protection.

The Personal Data Protection Bill (PDP Bill) was introduced in 2019 and is the first ever proposed law in India devoted to data protection, coming on the heels of an Indian Supreme Court judgment that declared privacy a fundamental right. The PDP Bill, which among other things seeks to: classify different kinds of personal data (personal; sensitive; critical); encourage privacy by design and data localisation in specific contexts; include foreign entities that handle personal data of individuals in India; and categorise 'significant data fiduciaries' (with additional compliance based on volume of data, etc.). The PDP Bill has, however, received its fair share of criticism on issues ranging from protectionism to arbitrary exceptions for data collection by the government. That said, the PDP Bill is yet to become law, and there are reports from as recently as late-2020 that it will undergo further revision before that comes to pass.

An allied development came up in February 2021 with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines). These seek to regulate social media intermediaries, streaming platforms and online publishers of news and current affairs by imposing stringent due diligence and compliance requirements – such as identifying the 'first originator' of information (for intermediaries primarily offering messaging services), and the appointment of a chief compliance officer along with a resident grievance officer in India. Once again, the new Intermediary Guidelines have also been rightly criticised for implications such as power to the government for blocking online content on emergency orders.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

India has seen a surge in the digital markets sphere, be it e-commerce, increasing online payments in a traditionally cash-reliant society, or tech-based health and financial services start-ups. By their very nature, such businesses handle large amounts of user data, which could potentially include personal information such as medical history and financial details. With that comes the risk of data being misused (or used beyond mutually accepted terms), especially with private players in various industries vying for access to more and more data/analytics to give themselves an edge – be it for targeted advertising, insurance checks, etc., in addition to hackers geared towards straight-up fraud. Consequently, some of the biggest challenges faced by data-driven businesses include: proper storage and protection of such data; issues of data ownership, consent and sharing with third parties; effective management of digital identities; and cloud-based security risks. In fact, fintech is perhaps a disproportionately likelier target for cyberattacks compared to most other industries, with KYC data being a goldmine for hackers. In March 2021 itself, reports suggested that personal data of over 3.5 million users of a popular Indian payments-app were put on sale on the dark web – though the company denied a leak. Privacy compliance, therefore, becomes a large overhead for companies in this space, sometimes prohibitively so for smaller business. On the other hand, even with the Government recently making a push with the National Digital Health Mission (NDHM – which carries its own privacy concerns in the absence of a dedicated data protection legislation), India's healthcare space remains highly fragmented, with everything from single-doctor clinics to nationwide corporate hospital chains jostling for space – all, understandably, with

different levels of technology capacity. Lack of standardisation and a resultant non-portability of digital health records remains a major challenge for organisations.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

In recent years, the Government has promoted campaigns such as Digital India to improve internet connectivity and online ecosystems – though its efficacy and implementation outcomes are up for debate, when significant portions of the country still lack basic digital infrastructure. At the same time, there has also been a marked increase in FDI into India in retail and digital health, for instance Walmart's acquisition of Indian online marketplace Flipkart, and Tencent's investment into Practo, an Indian app for doctor-consultations and booking appointments.

A large unbanked population has made fintech an especially high-growth segment in India, with periodic regulatory changes having recently created 'Payments Banks' – organisations that cannot offer loans or credit cards, but can carry out other banking functions. Given their existing infrastructures, several fintech and telecom companies are now entering this space. Successive legislative changes of questionable efficacy, for instance demonetisation and the Goods and Services Tax regime, have also led to a concerted push towards cashless technologies and digital payments, which – given the reliance on cash among much of India – have received notable Government promotion. Mechanisms such as Unified Payments Interface (UPI) and e-KYC have been adopted, and the Government has even promoted a homegrown payments app called Bharat Interface for Money or BHIM. The Reserve Bank of India (RBI) has also released guidelines for a regulatory sandbox to allow stakeholders – including regulators, innovators and financial service providers – to test out new products and services in a controlled 'live' environment, with certain regulatory relaxations for the purpose of testing.

The use of AI is increasingly gaining traction as well, with the Government trying to foster a regulatory environment for this. For instance, in January 2020, India's Niti Ayog (the Government's policy think tank) recommended a cloud computing framework running on AI, called "AIRAWAT" (AI Research, Analytics and Knowledge Assimilation platform). Under this programme, the Government aims to promote the use and growth potential of AI by tackling challenges such as: lack of access to computers; assisting in the R&D of new technologies; and facilitating the work of stakeholders including start-ups, students, organisations and independent researchers. The Government also launched the National Artificial Intelligence (AI) Portal as a one-stop platform for all advancements pertaining to AI in India, and partnered with the industry to help AI-based start-ups showcase their products as a part of its 'Atmanibhar Bharat' or 'Self-Reliant India' initiative.

Policies are also being formulated in the digital health space, with the Government's announcement of the National Digital Health Mission (NDHM) in July 2020 aiming to create unique health IDs to hold digital health records – although its potential implementation in the absence of a specific data protection law also carries data abuse and privacy risks. The National Health Authority (NHA) is slated to play a role in the development of these policies and in managing the NDHM as a government regulator.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The Information Technology Act, 2000 (IT Act) and rules made under it are the umbrella legislations which define and govern cybersecurity in India. It covers a wide range of topics within its fold, including granting legitimacy to digital operations by prescribing modes of electronic execution of documents, prescribing data protection measures, penalties for cybercrimes and security of electronic data, to name a few.

The Indian computer emergency response team is responsible for analysing and addressing instances of cyber incidents and disseminating information regarding best practices to be followed for preventing cyber incidents.

Among other issues, the IT Act prescribes that an online business dealing with processing sensitive data must implement reasonable security measures and procedures. This is applicable to both B2B and B2C businesses. Further, if there is collection of sensitive data, there must be consent of the consumer and information regarding how it is collected and used by the company.

Further, the Payment and Settlements System Act, 2007 is a specific law which regulates payment operations and payment intermediaries in the e-commerce space. The Reserve Bank of India also issues guidelines regarding use of payment instruments, which includes debit cards, credit cards, e-wallets or gift cards.

Additionally, the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 impose certain duties on e-commerce entities which are to be duly followed by them. These rules have created distinction between obligations of e-commerce entities and sellers selling through the platform.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

In addition to the legislations listed in question 3.1, under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('SPDI Rules'), reasonable security practices and procedures must be implemented by all companies that process, collect, store, analyse or transfer sensitive data or information. Specific security measures are to be implemented by companies that have protected systems as prescribed under the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

The Companies (Management and Administration) Rules, 2014 require that companies must ensure all electronic records and security systems are insulated from data tampering and unauthorised access. The Indian Penal Code, 1860 also deals with some offences that may take place online, such as obscenity, defamation or cheating.

The intermediaries are regulated through the Information Technology (Intermediaries Guidelines) Rules, 2011, which state that intermediaries must provide reasonable security practices and procedures to provide security to their data resources and information. The intermediaries are required to report all cybersecurity incidents to the Indian Computer Emergency Response Team (CERT-in).

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 are responsible for creating the CERT-in. It is an administrative body responsible for collecting and analysing information on cybersecurity incidents and responsible to take emergency response accordingly.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

According to a 2018 study, over 120 million users were expected to shop online that year, while India's e-commerce industry is expected to reach USD 200 billion by 2026. Even so, conventional brick-and-mortar retail has always dominated the larger retail market, especially in more remote parts of the country that still lack a serviceable digital infrastructure.

In a large and diverse country like India, consumers' attitudes can understandably not be homogenous; they are necessarily affected by, and must be seen in the context of, a multitude of often intersectional issues such as geography, class and economic status, and access to infrastructure. The probability of the average consumer leaning towards e-commerce – and having access to the internet in the first place – will depend upon a combination of these factors. That said, with growing competition and developing technology leading to an increase in internet penetration and affordability, India's active internet user base has crossed 560 million – which, for context, is still less than half the population.

Although the digital payments market in India is projected to grow to USD 1 trillion by 2023, India has traditionally been a cash-reliant society for several reasons. Other initial deterrents for consumers have included the fear of disclosing financial data (through online payments) and the inability to try or test the look-and-feel of a product prior to purchase. Therefore, e-commerce companies have had to innovate aggressively and tailor their business models to suit local needs and compete with the ubiquitous mom-and-pop or *kirana* stores – by offering multiple payment options such as cash-on-delivery and monthly instalments, adopting liberal exchange/return policies and the like.

Most recently, the COVID-19 pandemic has also played a major role in shifting consumers attitudes towards e-commerce, among those who can access and afford it. With strict lockdowns making it impossible (and sometimes illegal) to visit physical stores, consumers increasingly embraced e-commerce for its convenience.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

India has historically been cash-reliant for a variety of reasons, among them being a large unbanked population; a perceived mistrust of, and lack of access to, formal banking systems (and later online payments); tax evasion; and the dependence of small and medium business ecosystems, as well as households on cash transactions. In the context of e-commerce, studies show that a disproportionate majority of Indians prefer cash-on-delivery (CoD) while shopping online, which all major e-commerce players have had to factor into their strategies. CoD options bring their own logistical challenges, and it is not uncommon for

e-tailers to provide additional discounts if buyers opt for digital payments, to promote the latter. Since credit card usage in India is negligible outside urban/metropolitan areas – estimates put it at about 3% of the population – digital payments have also adapted to the Indian landscape, with options including digital wallets such as Paytm and PhonePe and online payment systems such as Google Pay becoming increasingly prevalent.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Indian retailers and e-commerce platforms undoubtedly perform well within their own jurisdiction with Indian consumers. Unicorns like Flipkart, Paytm, Zomato and OYO Rooms have maintained commanding positions in their respective markets due to their perceived insight and understanding of the target audience, although this is not absolute and is affected by industry-specific peculiarities like anything else. In the food-tech space for instance, homegrown Zomato and Swiggy have outperformed UberEats; Paytm leads in the digital payments space, but Google Pay is not insignificant either; among online retailers, Amazon is second only to Flipkart. Practically however, most major Indian platforms increasingly have significant foreign investment – Flipkart is now owned by Walmart, while One97 Communications (Paytm) has raised funding from ANT Financial, SoftBank and Berkshire Hathaway, among others. Interestingly, however, as is the case with both Flipkart and Paytm, these platforms/companies are considered 'Indian' as long as they have Indian founders, regardless of current funding or controlling interest.

As of now, no domestic platform/website occupies a dominant position in any international market. Of the Indian unicorns, OYO Rooms (whose investors include SoftBank and Airbnb) is perhaps one of the few to have seen rapid expansion outside India, though its success is debatable. While e-commerce in India has boomed in recent years, online retail still constitutes only a small percentage of India's total retail market – so it is perhaps good business for Indian platforms to first consolidate domestically, in a high-potential Indian market, before expanding into already saturated foreign jurisdictions. The Government has also been pushing for initiatives such as "Make in India" and is continuously doubling down on nationalistic sentiments by encouraging the public to use and support domestic, locally made/offered products and services.

That said, considering the exponential rise India has seen in the number of mobile (and internet) users over the past few years, there seems to be scope for the growth of e-commerce exports in the future.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Hindi (including its various dialects) is the most widely spoken language in India, with English a distant second, and most e-commerce firms will tend to switch between at least those two for the most part – Amazon's Alexa and Google Assistant 'understand' both Hindi and English. That said, India's size and diversity brings with it a multitude of different cultures, regional identities and languages, which e-commerce firms, like any other business, must cater to. It is not uncommon for multinationals to advertise festive season sales and create brand

campaigns in several Indian languages (along with Indianized/vernacularised English) simultaneously, while local counterparts like Flipkart, Snapdeal and Jabong have been multilingual for some time now. However, since Indian e-commerce firms are yet to make a meaningful expansion abroad, their handling of language barriers are yet to be tested.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

India is a highly complex jurisdiction, where significant inequities in opportunities and outcomes mean that a one-size-fits-all approach can never work. For instance, in spite of smartphone penetration and internet use, a significant section of the population still struggles with literacy. Therefore, platforms with a more visual style of interaction have historically seen more users than those that rely more on a text-based interface. This has also led to companies increasingly tailoring their UI/UX to suit local needs and sensibilities, by eschewing more complicated interfaces in favour of cleaner/simpler ones, such as tap-and-pay/one-touch payments in the digital payments space.

Additionally, a significant majority of Indian internet users access the internet primarily on mobile devices. This bit of local context means that, depending on the target consumer base, interfaces that are more mobile-friendly or 'mobile first' tend to perform better than those optimised for computers; similarly, lighter interfaces/apps that consume lesser mobile data may be preferred by certain sections of consumers.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The pandemic has decidedly had an impact on these norms, albeit among certain consumer bases. Extended lockdowns have shaped consumer behaviours *vis-à-vis* digital payments and using e-tailers for everyday needs such as groceries for instance, but only for consumers with access to that infrastructure. At the same time, it is not unusual to see elders going back to their corner store because of familiarity, or revert to cash for comfort.

That said, the pandemic has certainly made consumers switch from physical retailers to e-tailers, some for the first time. The longevity of this trend, however, remains to be seen.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In India, there are a variety of ways whereby entities can undertake online brand enforcement, depending on the nature of the infringement/violation itself. For instance, finding counterfeits or products under confusing similar brands on online marketplaces is not uncommon, and most major e-tailers like Amazon and Flipkart have a dedicated internal reporting mechanism through which brands/rights owners can flag such listings and ask for their removal. In other cases, where infringements take place on standalone websites or social media platforms, 'take-down' notices are a fairly common and, in most cases, effective remedy sought by brand owners. For situations where a website/domain is itself in violation of a brand owner's rights, proceedings against infringing domain names are possible under the

.IN Domain Name Dispute Resolution Policy or INDRP, which is the UDRP equivalent for .IN domain names. These are apart from formal legal remedies available under the Indian Trademarks Act, 1999, as well as under common law – such as seeking injunctive relief and/or damages.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

While there are no statutory restrictions *per se*, one of the biggest challenges that brand owners face is with cross-border enforcements. In situations involving brands that are unregistered and/or unused in India, establishing a trans-border/spill-over reputation in India becomes paramount, which is easier said than done when it comes to documentary evidence. That said, Indian jurisprudence on this issue has evolved over time; with businesses moving online and borders shrinking, Indian courts are increasingly giving online brand-use the evidentiary value it deserves.

With respect specifically to domain name issues, some domain registrars have begun masking/redacting information about domain owners in compliance with the GDPR, even when the domain owner is located outside the EU. This sometimes makes it difficult for a brand owner to ascertain information about the user/owner of an infringing domain name, in cases where formal proceedings under INDRP/UDRP are being contemplated. However, in the Indian context, there are practical workarounds to this that can be assessed on a case-by-case basis.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The Ministry of Electronics and Information Technology has issued certain Guidelines for Government Departments on Contractual Terms Related to Cloud Services. The Guidelines highlight key contractual terms that should be incorporated by government agencies in their contracts with cloud providers. The Guidelines also state that data provided by the Government Agencies to cloud service providers should be stored in India.

The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations in 2017 apply to insurers registered with the Insurance Regulatory Development Authority of India, with respect to any outsourcing arrangements they may enter into. These Regulations prescribe certain conditions with regards to obligations of service providers regarding confidentiality and security of information of policy holders.

Other than the above, there is no specific law in India on contracting with third-party-owned data centres and cloud providers. However, the entities dealing with personal and sensitive information of natural persons should ensure that they are able to comply with the security standards and other conditions prescribed under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 with regard to collection, storage, processing, sharing and transfer of personal and sensitive information.

The relevant stake holders should also keep a close watch on the draft Personal Data Protection Bill, 2019 (PDPB), which has been tabled before the Parliament and if enacted may introduce additional conditions relating to collection, storage and

processing of personal and sensitive information. This may invariably have some impact on the arrangement with third-party-owned data centres or cloud providers.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

The need to localise data centres and servers is currently mandatory for certain financial and payment-related data. The Reserve Bank of India (RBI) requires that all data collected by the payment system providers should be stored in a system in India.

Internet and telecommunication service providers are subject to the terms of the Unified Access License granted by the Government of India, which among other things, requires that such service provider should not transfer (a) any accounting information relating to subscriber, and (b) user information (except for international roaming/billing or information relating to foreign subscriber) to any person/place outside India.

Other than the abovementioned regulations, there are other sector-specific compliance obligations for location of servers/data centres. Additionally, refer to our response to question 6.1.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The Government of India in the last few years has taken several measures to digitise the cross-border trade process. Some of the key processes where the technologies have been adopted are:

- **Indian Customs and Central Excise Electronic Commerce Gateway (ICEGATE)**, which is the national portal of Indian Customs of Central Board of Indirect Taxes and Customs that provides e-filing services to importers, exporters, cargo carriers and other trading partners electronically. ICEGATE can be used for filing bills of entry and shipping bills, and for electronic payment of customs duty.
- **Portal for e-BRC Services**, which is an integrated platform which enables electronic transmission of Foreign Exchange Realisation Information from Banks directly to Directorate General of Foreign Trade's (DGFT) server. This portal also facilitates the issuance of electronic Bank Realization Certificates by banks to the exporter for the purpose of claiming benefits under the various schemes of the Foreign Trade Policy.
- **Export Data Processing and Monitoring System (EDPMS)** is an online platform for monitoring export returns.
- **Import Data Processing and Monitoring System (IDPMS)** is an online platform for monitoring import returns.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

One of the significant barriers to adoption of technologies is the reluctance of Government officials to use technologies more often to promote trade, resulting in red-tape and demands for bribes. It will need constant efforts from all stake holders to

keep pushing the Government and its officials to promote the use of technology for trade facilitation.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Although the Government provides certain fiscal incentives to small businesses and start-ups in general, there is no specific tax incentive for digital business.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The Government of India has recently imposed Equalisation Levy on the consideration receivable by an e-commerce operator not having permanent establishments in India in respect of transactions relating to online sale of goods and services in India. The levy is to be paid on consideration received by the e-commerce operators from persons resident in India, or a non-resident who buys goods or services, or both, uses an IP address located in India.

The Government also framed law to tax non-resident entities that do not have any establishments in India on the basis of 'Significant Economic Presence' based on factors such as digital presence, number of users and revenue. It is likely that some of the overseas businesses engaged in digital business may come under the ambit of the new tax regime.

It is likely that these two areas may show significant number of future cross-border disputes between digital business and Indian tax authorities.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In India, various state- and centre-specific legislations govern employment. There are around 165 labour laws around which 50 are central legislations. Recently, the Government has amalgamated 44 central labour laws into four labour codes, which are yet to be notified.

These legislations include workmen, skilled employees, unskilled employees, contract laborers, etc. Employment is usually executed through employment agreements which are governed by the Indian Contract Act, 1872. The employment agreements have to be in line with the labour legislations applicable. Terms of agreement which are in contravention of the labour legislations may carry a penalty under the relevant legislation.

The employment is governed through contractual terms and labour laws which provide certain rights to the employees through Maternity Benefit Act, Employees' State Insurance Act, Employees Provident Fund Act, Payment of Gratuity Act, etc.;

such labour legislations make binding obligation on the employer to provide benefits to his employees. The labour laws are a safeguard for employees that protect them from unfair contractual terms. The labour laws provide employees with benefits such as right to leaves, prevention of sexual harassment, appropriate working hours, bonus, etc.

India is heavily regulated in the employment sector. It is pertinent to seek legal assistance in the structuring and hiring of employees to avoid any penalties under the various legislations.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no specific regulations in India relating to carrying out work away from an organisation's physical premises. Though there are no specific regulations, the employee shall be governed by the employment agreement and the internal policies of the company. Also, the company has to fulfil its obligations towards the employees as required by the legislations governing employment.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

The Covid-19 pandemic has brought about a paradigm shift in the work policies in many companies. Many companies are planning to implement hybrid structures of work policies. Such as work from home, work from any location or to work from office. It is likely for various other companies to follow suit.

Additionally, due to the pandemic, there has also been a shift from physical record keeping to digital record keeping, which is a trend we anticipate will continue even post pandemic. Further, changes in meetings, including board meetings, will take place through video conferencing. The Indian legislations already have structures in place to implement such changes.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Absence of well-defined laws to regulate digital business operating in India is the key barrier for growth of digital business in India. However, the Government is taking significant steps to bring about the needed reforms.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

With a 1.3 billion population – significant portions of which are unbanked and may not be online yet – India provides enormous opportunities for the exponential growth of digital business. A sizeable and growing consumer base, along with existing and prospective legislative reforms, are a big positive for digital business in India.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The key areas of focus of regulators in India in the areas of digital business are: (i) extent and conditions for foreign investments in e-commerce business in India; (ii) protection of small business enterprises engaged in retail business from abuse by dominant e-commerce entities; (iii) consumer protections; (iv) protection of personal and sensitive information of natural persons; and (v) taxation of e-commerce operators not having permanent establishments in India on the basis of their significant economic presence in India.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

In India, all regulations relating to payments and settlements are governed by the Regulations that are framed by the Reserve Bank of India (RBI). The significant Regulations include:

- The Payment and Settlement Systems Act 2007 (PSSA): PSSA regulates payment systems in India. The PSSA defines payment systems as a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them.
- Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) Guidelines issued by the RBI from time to time. These Guidelines are applicable to all payment aggregators and gateways under PSSA.
- Reserve Bank of India (Digital Payment Security Controls) Directions 2020, for scheduled commercial banks (excluding regional rural banks), small finance banks, payments banks, and credit card issuing non-banking financial companies to set up governance structures for such systems and implement common minimum standards of security controls for channels like internet, mobile banking, card payments, among others. The Guidelines create an enhanced and enabling environment for customers to use digital payment products in a more safe and secure manner.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

India has a comprehensive law to govern online payment service providers. A number of regulations and guidelines apply to service providers depending on the nature of services provided. The key challenges involve understanding the complex regulatory framework, some of which may not be entirely well defined.



Disha Mohanty is a Principal at G&W Legal. She chairs the firm's Corporate/Commercial practice, and co-heads Digital Business industry group.

Disha has extensive experience advising clients on a broad spectrum of matters, including commercial contracts, franchise and distribution, regulatory compliance, foreign investment, employment law and real estate. She works with clients across multiple sectors ranging from retail and e-commerce, F&B, tech, pharma, consumer electronics, etc. Representatively, Disha assists a multinational apparel company with all aspects of setting up and scaling its operations in India, counsels a global semiconductor company, and helps a large Australian retail chain with employment law and other matters concerning its Indian operations.

G&W Legal
C-9 / 9624, Vasant Kunj
New Delhi – 110070
India

Tel: +91 9958 3485 59
Email: dishamohanty@gnwlegal.com
URL: www.gnwlegal.com



Arjun Khurana is a Principal at G&W Legal. He chairs the firm's IP, Tech & Media practice and co-heads the Digital Business industry group.

Arjun advises Fortune 500 companies as well as startups on IP issues; acts on complex technology and content licensing transactions; advises on advertising regulations and vets campaigns; counsels corporations on data protection and privacy issues; and represents multinationals in commercial disputes and anti-counterfeiting actions before Indian courts and tribunals. Notably, he represents a global media network in IP litigation; assists an international fashion retailer with setting up a tech hub and commercialising their IP in India; counsels corporations on data protection and privacy issues; has advised a major online marketplace on private label arrangements; has formulated and effected pan-India enforcement strategy for one of the largest retail chains in the world; and has counseled a major developer on setting up an e-sports and gaming portal in India.

G&W Legal
C-9 / 9624, Vasant Kunj
New Delhi – 110070
India

Tel: +91 8800 1165 14
Email: arjun@gnwlegal.com
URL: www.gnwlegal.com

Combining the experience of big law with the expertise of a boutique, **G&W Legal** is a full-service business law firm that assists its clients at the intersection of law and pragmatism. Our team spans diverse subject matters and industries, using its robust skill set to become greater than the sum of its parts.

As the world grows smaller in the information age, business is no longer limited by borders. We understand this well, and provide our clients with advice and representation on every aspect of expanding into and doing business in India. Our attorneys bring a rich body of knowledge and accomplishment across (often intersecting) areas such as: Corporate/Commercial; Intellectual Property, Tech and Media; Franchising and Distribution; Advertising and Marketing; Privacy and Data Protection; Product Liability and Consumer Protection; International Trade; Foreign Investment; Private Equity and Venture Capital; Employment; Government Contracts; Corporate Restructuring; Corporate Governance, Ethics, Compliance and Investigations; Anti-trust / Competition; Regulatory Affairs; Real Estate; Dispute Resolution; and everything in between.

www.gnwlegal.com

G&W
Legal

Indonesia



Enrico Iskandar



Bratara Damanik



Jonathan Cheong

Bagus Enrico & Partners

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

The comprehensive umbrella regulation for the e-commerce ecosystem in Indonesia was enacted through Government Regulation No. 80 of 2019 (“**GR 80/2019**”) regarding Trade Through Electronic System / E-commerce (locally known as *Perdagangan Melalui Sistem Elektronik* – “**PMSE**”). The government enacted GR 80/2019 on 25 November 2019 and included a two-year transitional period for existing e-commerce businesses to ensure their operations were compliant with the regulation.

GR 80/2019 has defined any individual or entity – whether a legal entity or a non-legal entity, and which can be either local or foreign – conducting e-commerce activities as business actors (“**Business Actor(s)**”). The definition of Business Actors can also include foreign individuals or business entities incorporated and domiciled outside Indonesia which conduct e-commerce activities within the territory of Indonesia. Furthermore, the regulation has provided three classifications of Business Actors, namely:

- **Merchant:** A merchant is any Business Actor who conducts e-commerce activity (for commercial purposes and not on a temporary basis), either through its own electronic systems or through an electronic system of an e-commerce operator.
- **E-commerce Operator** (locally known as *Penyelenggara Perdagangan Melalui Sistem Elektronik* – “**PPMSE**”): An e-commerce operator is any Business Actor who provides a service and/or an electronic system to facilitate an e-commerce transaction. This may also include any merchant who also provides its own electronic system when conducting e-commerce activity. Other types of business model which can be categorised as an e-commerce operator include online marketplace platforms, online classified ads, price comparison platforms and daily deals.
- **Intermediary Service Operator (“ISP”)**: An intermediary service operator is any Business Actor that provides

intermediary or indirect services to support e-commerce activities, including search engine providers, hosting providers and caching providers.

While there is not yet a legal obligation specifically directed to B2B e-commerce under the prevailing laws and regulations, the government has issued Minister of Trade Regulation No. 50 of 2020 regarding Provisions on Business Licensing, Advertising, Guidance and Supervision of Businesses in Trade through Electronic Systems (“**MoT 50/2020**”) as an implementing regulation of GR 80/2019. Under MoT 50/2020 and GR 80/2019, there are obligations and requirements that must be fulfilled by certain parties, either individual or entities, involved in e-commerce (including B2B and B2C e-commerce), as follows:

- a) **General obligations**
 - compliance with applicable regulation on taxation, data protection, import/export activities, consumer protection and advertising ethics;
 - compliance with general business requirements (for example, technical licences, standardisation of goods/services, among other vital factors);
 - assistance with government programmes, if requested (e.g., prioritisation of the trading of domestically produced goods/services);
 - provision of terms of use or the licence agreement to their users; and
 - provide means of technological control and/or means of receiving public complaints regarding the existence of illegal electronic information in their electronic system in accordance with provisions of applicable laws and regulations.
- b) **Licensing and Registration Requirement**
Under MoT 50/2020, particularly for domestic PPMSEs, non-exempt ISP and domestic merchants that have their own electronic communication facilities used for trade transactions must obtain a specific licence prior to conducting operation in Indonesia, i.e. Trading Business License Through an Electronic System (locally known as *Surat Izin Usaha Perdagangan Melalui Sistem Elektronik* – “**SIUPMSE**”). To secure a SIUPMSE, the Business Actor shall apply to the Minister through the Online Single Submission (“**OSS**”) system.

However, such SIUPMSE shall only be effective upon satisfaction to the following commitments/requirements:

- obtainment of Electronic System Registration (locally known as *Pendaftaran Sistem Elektronik*) Certificate issued by the Ministry of Communications and Informatics (“MCI”) within 14 working days after the issuance of SIUPMSE.
- Electronic System Registration is a straight-forward process which is conducted within MCI’s online system. The registration requires several corporate documents which include, among others: (a) registration form; (b) corporate documents; (c) applicant’s profile; and (d) brief information on the technicality of the Platform. Following the submission of those documents, MCI will generally be able to issue the certificate within seven business days;
- provision of website address and/or application name;
- establish accessible consumer service’s contact details, i.e. contact and/or email address; and
- establish a consumer service which contains contact details of Directorate General of Consumer Protection and Trade Compliance.

In addition, a PPMSE can use an electronic certificate in relation to an e-commerce transaction. There is no mandatory requirement to use an electronic certificate issued by the authorised Indonesian electronic certification organisers; however, the government will not view an e-commerce transaction which uses an electronic certificate issued by foreign electronic certification organisers as authentic evidence in Indonesia.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Please revert to our answer to question 1.1 as it is also applicable to B2C e-commerce.

Additionally, in doing B2C e-commerce, GR 80/2019 stipulates some standards related to offers, acceptances and confirmations. Each of these provisions possess specific criterion, as follows:

- a) An offering shall be valid and have binding legal force if there is a clear and specific statement of intention in the offering, as well as terms and conditions, by way of truthful, fair and balanced offerings, as well as certain time restrictions.
- b) Acceptances are deemed to be accepted if the accepting party already shows that it has accepted the terms and conditions delivered in the offerings.
- c) Confirmations can be electronic or non-electronic given by Business Actors to consumers as a response to the consumers’ acceptance. The contents of a confirmation must be the same as the offering information.

Particularly in the case where the PPMSE is a foreign individual or business entity incorporated and domiciled outside of the territory of Indonesia, but actively conducting offerings to consumers residing within Indonesia, GR 80/2019 has put certain thresholds which may classify the abovementioned foreign Business Actor as physically present and operational as a permanent business establishment in Indonesia, such as: (i) transaction volume; (ii) transaction value; (iii) volume of packages to be shipped; and/or (iv) volume of traffic or people who access the foreign Business Actor. Once the foreign PPMSE

has satisfied the criteria above, they will be required to appoint an Indonesia representative that will act on their behalf in the form of Representative Office of Foreign Trade Companies (locally known as *Kantor Perwakilan Perusahaan Perdagangan Asing* – “**KP3A**”) within the sector of Trade through Electronic.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Through 2020, there was no new and/or updated data protection regulation. The latest regulations issued in 2019, which partially cover data issues, include:

- i) Government Regulation No. 71 of 2019 regarding Implementation of the Electronic System and Transaction (“**GR 71/2019**”), an update and replacement to the obsolete Government Regulation No. 82 of 2012 regarding the same;
- ii) Government Regulation No. 80 of 2019 regarding trade through electronic systems (“**GR 80/2019**”);
- iii) Ministry of Communications and Informatics (“MCI”) Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic System (“**MCI Regulation 20/2016**”); and
- iv) Law No. 11 of 2008 regarding Electronic Information and Transaction as lastly amended by Law No. 19 of 2016 (“**EIT Law**”).

Even though the latest regulations have been enacted, i.e., GR 71/2019 and GR 80/2019, it does not cause radical changes to the currently prevailing data protection environment in Indonesia; however, both show the Indonesian government’s emphasis on the importance of data protection regulations within Indonesia’s regulatory framework.

For your reference, the Indonesian government has already drafted and submitted a draft bill on data protection (“**PDP Bill**”), in which approval is being deliberated. Enactment of the PDP Bill would establish more detailed rulings on data protection. Enactment of the PDP Bill may effectively introduce new provisions similar to the EU General Data Protection Regulation.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

In general, the main challenges happened due to the absence of comprehensive rulings in data privacy and data protection in Indonesia, as we will describe below.

a) Financial Technology (Fintech)

Fintech that has been developed in Indonesia include, among others: (i) online payment; (ii) peer-to-peer lending; (iii) insurance-tech; (iv) aggregator; and (v) crowdfunding. Such type of Fintech is closely supervised by our central bank (Bank Indonesia – “**BI**”) and financial authorities (Financial Services Authorities, locally known as *Otoritas Jasa Keuangan* – “**OJK**”) through a regulatory sandbox and determined based on the nature of its transaction. We understand that the lack of data privacy and data protection regulation has hindered certain Fintech companies in providing services to their consumers. However, the regulator has set certain requirements to reduce the risks that might occur for Fintech companies who will operate in Indonesia, including to maintain the confidentiality of consumer data and/or transaction data. For instance, in

the absence of such rulings, there is a case where Fintech companies particularly those operating in peer-to-peer lending are restricted by OJK to only have access to certain consumers' personal data when providing services through a smartphone application i.e., camera, microphone, location.

b) Digital Health

Currently, the provisions related to digital health privacy are only on the management of a patient's 'medical records', which is regulated under Ministry of Health Regulation No. 269 of 2008 regarding Health Records. Medical record incorporates several pieces of information, among others: patient's identity, diagnosis, anamnesis/medical history, examinations history, and medication history (hereinafter referred as "**Patient Data**"). The concept of data privacy in the healthcare sector is slightly different to data privacy in general due to fact that the medical record document is owned by the healthcare provider; however, please note that the content of the medical record is still owned by patients. Thus, any disclosure of Patient Data must be authorised by the patient.

c) Other Sectors (i.e., Retail and AI)

Regarding retail and AI, being relatively new concepts, these are yet to be specifically governed by significant regulations that oversee and tackle the vast privacy issues.

As to the extent of utilising collected data, it is extremely important to first provide an explanation on the purpose of collection and obtain consent from the data owner.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

While retail, AI and digital health have not yet been given significant attention in Indonesia's regulatory framework, BI and OJK provide a regulatory sandbox for Fintech companies to test their products, services, technologies, and business models under their supervision. In order to accommodate the innovative products provided by Fintech companies, and in the absence of specific regulation, both BI and OJK have their own regulatory sandbox in which Fintech companies are able to operate under special exemptions for a limited period of time. Under the practice, Fintech companies who are connected to payment systems are under BI's jurisdiction, while others (outside of payment systems), such as insurance-tech, peer-to-peer lending, robot advisory, or credit scoring services, will be under OJK's jurisdiction.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The prevailing legal framework for cybersecurity in Indonesia is dispersed within various regulations. Nonetheless, the main reference for cybersecurity in Indonesia is Law No. 11 of 2008 regarding Information and Electronic Transactions as lastly amended by Law No. 19 of 2016 ("**EIT Law**"). However, EIT Law regulates more so on the prohibition of cyber incidents (including hacking, denial-of-service, phishing, identity theft), rather than outlining the specific forms of cybersecurity that can be applied in Indonesia. Depending on the context, other regulations may have specific cybersecurity framework applicable to e-commerce businesses.

In relation to personal data, in 2016, the Ministry of Communication and Informatics ("**MCI**") enacted specific regulation through MCI Regulation 20/2016. MCI Regulation 20/2016 requires all electronic system operators in Indonesia to store any personal data in its possession in an encrypted form, although there is no further stipulation on the encryption mechanism to be implemented. This is also directed to the e-commerce sector, which, to an extent, is stipulated in GR 80/2019 where an e-commerce operator can use encryption or cryptographic products in e-commerce activity.

Meanwhile, under GR 71/2019, any parties which provide, manage, and/or operate electronic systems for their own purposes and/or for other parties' purposes would be categorised as an Electronic System Operators ("**ESOs**"). As such, e-commerce operators are also considered ESOs and are obliged to implement measures to protect their electronic system operational activity, wherein they must:

- provide an audit trail for all activities of the electronic system for the purpose of supervision, law enforcement, dispute resolution, verification, testing and other examinations;
- conduct security checks for the components of the electronic system;
- own and operate procedures and facilities for the security of the electronic system in preventing disturbance, failure and loss;
- maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or electronic documents; and
- provide features in accordance with the characteristics of the utilised electronic system at least in the form of facilities to: (i) make corrections; (ii) cancel a command; (iii) provide a confirmation or reconfirmation; (iv) choose to continue or to stop the next activity; (v) view the submitted information in the form of an electronic contract offer or advertisement; (vi) check the success or failure of an electronic transaction; and (vii) read the agreement before conducting an electronic transaction.

A notable mention that may affect the future of cybersecurity is that the government previously submitted a draft bill on cybersecurity in 2019 which failed to fulfil the requirements to be enacted. However, to date, there is no clear timeline on the enactment of such draft bill in the future.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

a) Financial Services Sector

The use of information and technology in the banking sector is regulated under Financial Services Authority No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks as lastly amended by OJK Regulation No. 13/2020 ("**OJK Regulation 38/2016**"). The following are examples of compliance requirements under OJK Regulation 38/2016 that are related to cybersecurity matters:

- forming an Information Technology Steering Committee;
- at least once a year, performing a trial of a Disaster Recovery Plan involving all critical applications and infrastructures in conformity with the business impact analysis result;

- background check of criminal records during the recruitment of IT staff, including staff of the IT service provider, and network administrator or system administrator positions;
- to have an IT operational security procedure;
- consider the formation of an Incident Response Team in Information Security, in accordance with the bank's business complexity;
- within seven days after the event has come into realisation, reporting any critical events, abuse, and/or criminal offences in the implementation of information technology which may and/or have caused significant financial losses and/or disrupted the bank's operational continuity, in the form as stipulated by OJK; and
- a Data Centre/Disaster Recovery Centre may be located outside the territory of Indonesia, provided that an approval from OJK has been obtained; such approval will be granted subject to satisfaction of certain requirements.

Any non-compliance with such provisions may be subject to penalties in the form of administrative sanctions and fines.

b) Telecommunications Sector

The procedures for telecommunication services are regulated in MCI Regulation No. 13 of 2019 regarding Implementation of Telecommunication Services. The regulation provides that the Telecommunications Service Provider is required to make the following efforts as a form of implementation of cybersecurity:

- use telecommunication tools and/or devices that have met specified and certified technical requirements;
- the Telecommunications Service Provider must keep customer data at least in the form the customer's name and customer identification number; and
- for the purposes of the criminal justice process, the Telecommunications Service Provider is obliged to keep recorded data directly related to the court process referred to until the court decision is legally binding.

c) National Strategic Sector

According to Presidential Regulation No. 133 of 2017 regarding Amendment to Presidential Regulation No. 53 of 2017 regarding State Cyber and Code Agency ("BSSN"), BSSN is a government institution that carries out cybersecurity as effectively and efficiently as possible by utilising, developing and consolidating all elements related to cybersecurity. BSSN coordinates with all ministries within the cabinet including the national critical industries, such as ICT, energy, transportation, health, national defence and security, in order to enforce their scope of cyber protection. Furthermore, to secure an operation in every electronic system, BSSN has enacted BSSN Regulation No. 8 of 2020 regarding security system in the operation of electronic system ("BSSN Regulation 8/2020"). It stipulates that every ESO operated in Indonesia is required to comply with the implementation of information security management based on the principal risk (locally known as *Sistem Manajemen Pengamanan Informasi* – "SMPI"). SMPI standards will be adjusted to the level/category of relevant electronic system i.e.: (i) strategic; (ii) high; and (iii) low. For your reference, the higher the level/category of the electronic system, the more complex the standards that need to be applied, such as: (a) SNI ISO/IEC 27001; (b) other security standards related to cybersecurity established by BSSN; and (c) other security standards related to cybersecurity established by the Ministry or Institution.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

The COVID-19 pandemic has undoubtedly caused a huge shift towards consumers' attitudes towards e-commerce. According to a Bank Indonesia survey, the value of e-commerce transactions reached a record-high of USD18.2 billion, a modest 29.6% increase from USD14 billion in 2019 despite the negative sentiment brought by the pandemic. Such increase is also coupled with a boost in the usage of e-wallet/digital payment methods.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

According to a 2020 Bank Indonesia report, the most favoured payment method for e-commerce transaction is e-wallet/digital payment with 41.71% usage, while the more conservative bank transfers and cash-on-delivery payment method accounts for only 20.23% and 19.01%, respectively. Consistent with payment in the e-commerce sector, the use of cashless payment methods is also significantly increasing today with many consumers avoiding direct contact during the ongoing COVID-19 pandemic, which can be seen from some surveys highlighting significant increases of new users in some e-wallet and digital payment service providers in Indonesia throughout 2020.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

We believe that in some countries which already have a more advanced and detailed IT-related regulatory framework (e.g., on data protection and cybersecurity), home-state retailer websites/e-commerce platforms may perform better. For example, in Indonesia, if a new type of financial-related business model that is meant to support an e-commerce business is not covered in any regulation, it will need to obtain a regulatory sandbox approval from the relevant authority. In order to obtain the approval, it will have to go through an initial inspection and analysis of the platform, which may take significant time.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Most Indonesian e-commerce platforms are still displayed in the Indonesian language only (*Bahasa*), as currently most Indonesian e-commerce business still target domestic consumers and it can also be seen that most Indonesian e-commerce firms do not provide an option for international shipping. This is also due to the mandatory requirement of presenting information of the operation of electronic systems in an understandable manner, including using Bahasa within electronic contracts that are addressed to Indonesia's consumers.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

As in most jurisdictions, having web-interface concepts presented in the local language is always the first stage in order to appeal to the specific market. Other design concepts that may impact consumer interactivity truly depend on the specific market and product that is being sold and marketed.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Yes, especially in the payment method and e-commerce sector. Previously, cash on delivery was popular and often used as the preferred payment method. The same goes for offline shopping, where many still preferred to shop directly at retail stores. However, the COVID-19 pandemic has significantly shifted the trends, and we are seeing that cashless payment methods and online shopping are becoming more and more preferable today.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In order to obtain protection for a brand, a brand owner should first register its product's trademark to the Indonesian Trademark Office. Once the trademark office validates the registration, the registered brand/trademark will be protected for a period of 10 years and can be renewed. Further, as Indonesia is also a contracting party to the Protocol relating to the Madrid Agreement on the International Registration of Trademarks, a foreign brand owner can register an international brand in Indonesia through the international bureau, provided that it has commercial activity in Indonesia.

The Ministry of Law and Human Rights ("MoLHR") and MCI jointly issue Decree No. 14 of 2015 and No. 26 of 2015, respectively, regarding the Implementation of Closing Down Content and/or User Right to Access on Copyright Infringement and/or Related Rights in Electronic System. The joint decree stipulates, among others, the procedure on filing a report on copyright infringement in electronic systems, the verification procedure of filed reports, as well as the procedure for closing down the content and/or access rights related to copyright infringement. Furthermore, GR 80/2019 also provides that PPMSE can be held responsible for any illegal contents within their platforms, although such responsibility does not apply if the PPMSE swiftly removes such illegal contents at the first instances after it became aware of such illegal content within their platforms.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Trademark law only gives the right to a registered trademark owner or an unregistered famous trademark owner to file a lawsuit regarding its trademark infringement. Additionally, a trademark owner may also file a lawsuit to a facilitator or re-seller of counterfeit goods or unlicensed services.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Indonesia data protection regulation has not yet provided a detailed outline of the division of responsibilities between a data controller and a data processor. Accordingly, as data processed or stored by third-party data centres or cloud providers are collected by a service provider (as data controller), any mishandling or privacy breach conducted by the third-party data centres or cloud providers may fall under the service provider's responsibility.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Generally, electronic service providers may locate their data centres outside Indonesia and send personal data to an area outside Indonesia, provided that the area has been declared as having the same protection level and standard as Indonesia by the relevant authority. However, stricter additional requirements of data localisation may apply to electronic service providers in public sectors and other specific sectors, such as the financial sector.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Whilst currently there is no one specific type of technology being adopted, there are numerous efforts carried out by the government specifically focused on logistics, consumer protection and other e-commerce matters in order to accommodate the rapid growth of the digital market. The issuance of GR 80/2019 is one of the key regulations mandated under Presidential Regulation No.74 of 2017 on the National E-Commerce Road Map 2017–2019 ("PR 74"). Enactment of this specific regulation provides great clarity through improvements in the government's governance related to the increasingly rapid development in all e-commerce practices within Indonesia.

Nevertheless, under the Indonesia blueprint on National Logistic System, there will be more utilisation of technology and further development of MSME logistics data transfer to ensure further digitalisation of international trade in Indonesia. The government wants to develop a National e-Logistics which would provide services such as the transfer of data, logistics documentation and any reliable information in order to facilitate G2G, B2G and B2B transactions, either domestic or international, by also connecting with ASEAN and global logistic networks.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Indonesia, being one of the fastest growing digital market economies in the South East Asian region, continuously strives to overcome barriers and accommodate rapid growth of the digital economy. Notable aspects that must be accounted for include the encompassment and facilitation of the different desires of

customers and demographics, improvements on data analytics and cybersecurity. These are key factors that continually enable Indonesia to further advance in such a large e-commerce sector. The government has already begun to anticipate such growth by the revolutionary enactment of GR 80/2019, which comprehensively stipulates the guidelines governing extensive matters relating to e-commerce within Indonesia, including compliance checklists for e-commerce businesses. GR 80/2019 has been key in establishing the clarification of the different recognised e-commerce parties, requirements for e-commerce business practitioners, and the importance of consumer protection obligations, including enforcement of personal data protection requirements.

Note that in the near future there may be further regulations governing trade practices such as taxation and logistics.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

The Ministry of Finance (“**MoF**”) in Indonesia has provided several tax incentives (such as tax allowance and tax holiday) on income tax that are applicable to relevant digital businesses. The award of such tax incentives is subject to the MoF’s approval following the fulfilment of certain requirements, among others: (i) the nature of business is part of a pioneering industry which is entitled to such tax incentive; and (ii) the business’ investment value in Indonesia will determine the amount and period of tax holiday.

Unfortunately, there has not yet been a tax incentive in relation to research and development conducted by entities; however, we understand that there is an ongoing discussion between government entities on regulating such tax incentive.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Previously, the government did not specify the taxation mechanisms specific to over-the-top (“**OTT**”) service providers that operate remotely outside of Indonesia.

For instance, under the current prevailing law and regulations, foreign digital businesses (including Business Actors) will be required to collect and deliver value added tax (“**VAT**”) to the tax authority by appointing a representative in Indonesia. Additionally, a foreign digital business which is categorised as having a significant economic presence in Indonesia is to be treated as a permanent establishment, which will be subject to income tax. The criterions used to determine significant economic presence are (i) gross distribution of business group consolidation, (ii) sales value within the Indonesia territory, and/or (iii) active users of digital media in Indonesia.

Furthermore, due to the COVID-19 pandemic, the Indonesian Government has decided to accelerate the tax collection on overseas digital businesses by enacting Government Regulation No. 1 of 2020 relating to Financial State Policy and Stability of Financial System during the Coronavirus Disease (“**GR No. 1/2020**”). GR No. 1/2020 has incorporated the above criterions of foreign digital businesses having significant economic presence in Indonesia who shall comply with prevailing income tax or an electronic transaction tax. Furthermore, any utilisation of non-material taxable goods and/or taxable services from outside custom areas to within custom areas through an e-commerce system will

be subject to prevailing VAT regulations. Those failing to comply with the above shall be subject to a warning, administrative sanction and a potential access termination upon businesses’ electronic systems by MCI.

Clarification of procedures as above-mentioned have been provided through the enactment of the implementing regulation of PER-12/PJ/2020 on Certain Criteria relating to the Appointment of Collectors, Collection, and Deposit, and Reporting of Value Added Tax in the Utilization of Intangible Taxable Goods and/or Taxable Services from Outside of Customs Area in the Customs Area Through Trade via Electronic Systems (“**PER-12/PJ/2020**”). This has solidified that generally digital businesses and any other foreign services are subjected to electronic tax due to sales of digital products by overseas sellers to consumers within the customs area of Indonesia. Foreign OTT services will be charged with VAT (or locally known as *Pajak Pertambahan Nilai*) of 10% from the transaction value as per the taxation policies of the Directorate General of Taxes (“**DGT**”). This VAT rate is applied at the point-of-sale against the taxable amount which is the amount payable by the customer before any taxes.

Digital products/services included, but not limited to:

- movies, music, and other audio-visual contents;
- computer software, mobile apps, games;
- electronic books, magazines, and comics;
- web hosting;
- videoconferencing services; and
- other services delivered through computer networks.

Although GR No. 1/2020 was originally issued to ensure economic stability during the COVID-19 pandemic, it provides us with a better view on how the government will regulate the taxation for foreign digital businesses in the future.

The regulations have provided clarity related to the amount of the tax fee, collection procedure, representative appointment procedure, and thresholds for determining significant economic presence for digital business and OTT services. Despite the clarifications, it will undoubtedly take time for the government’s significant enforcement of these taxation policies. Nevertheless, it is fair to state that there are no longer any misconceptions or disputes as to whether specific digital businesses and/or OTT services are to be taxed.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

There are two types of employment status based on Law No. 13 of 2003 regarding Manpower (“**Manpower Law**”), namely: Specified Time Work Agreement (“**PKWT**”); and Permanent Work Agreement (“**PKWTT**”). The difference between the two agreements lies in the agreed working period. A PKWT is given for certain types of work which are temporary and relatively short. The contract period is for a maximum of five years. The termination of the PKWT and PKWTT made by the company causes the company to pay certain severance payments.

Manpower Law also stipulates that companies that hire employees for supporting activities and not the main activity of the company (e.g. chauffeurs, housemaids, etc.) can contract their employees either on a PKWT or PKWTT through outsourcing. An advantage of outsourcing is the recruitment process where

companies are able to reduce their budget and the time taken to hire as it is the paid responsibility of the service provider.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no specific laws and regulations governing work performed outside of the office. Manpower Law gives employees and employers the freedom to determine their own policies in carrying out jointly agreed business activities in work contracts, company regulations and collective labour agreements.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Due to the COVID-19 pandemic, the Indonesian government has enacted several new manpower regulations in continuation with the Omnibus Law for the purpose of attracting more investments into Indonesia. As the previous manpower regulations were quite rigid and the regulations were deemed more beneficial to employees compared to businesses, the newly enacted manpower regulations have set further details in case of an employee's termination, including the calculation of the termination package for each event of termination. This has provided further confidence to employers since the calculation of termination package is seen more reasonable compared to that in the previous regulation.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The amount of dispersed regulations relevant to digital business may affect the development of an e-commerce ecosystem. Since the relatively recent enactment of GR 80/2019, digital businesses now have a clearer vision on various legal aspects such as requirements, registration, payment methods, formation of electronic contracts, consumer protection and mechanisms of resolving disputes within the e-commerce realm that must be abided by. Put aside the implementation of regulation GR 80/2019, the government has also prepared a draft bill on data protection which will impose further obligations on digital businesses. It is important for the government to find a balance in protecting the interest of the e-commerce ecosystem by providing regulatory effectiveness in the era of digitalisation.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Indonesia being the fourth most populous nation in the world, and having the largest population in Southeast Asia, holds endless advantages for any digital business looking to expand their operations. As one of the biggest e-commerce economies in Southeast Asia, Indonesia's e-commerce industry is expected to reach USD40 billion by 2022 and is estimated to see an additional estimated 42.1 million e-commerce shoppers by 2021. An estimation by global tech giants Google and Singapore's Temasek places Indonesia's e-commerce economy at USD53 billion in 2025.

We believe digital businesses are capable of utilising and investing in some of the advantages offered in Indonesia,

including: (i) secure and scalable payment opportunities; (ii) large, strong talent pool; and (iii) an increasing digital-commerce ecosystem. These factors will provide great advantages for digital businesses operating in Indonesia.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The Indonesian regulator is currently focusing on establishing the detailed regulatory framework on data protection as more businesses in Indonesia collect and process personal data. The discussions on the bill of personal data protection has been ongoing for the last couple of years; however, the enactment of such bill has not materialised until to date.

Furthermore, the regulator is also preparing a specific licensing framework for foreign digital businesses, where such businesses will still need to conduct certain registration such as Electronic System Registration and specific registration for foreign offshore entity. Therefore, OTT service providers may generally provide their services directly from offshore but with certain registration and compliance requirements in Indonesia.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Generally, GR 80/2019 covers provisions on online payments related to e-commerce activity in Indonesia. E-commerce firms may provide an online payment option as one of its payment methods, by engaging in a partnership agreement with an online payment provider which has obtained approval from an authorised financial institution such as Bank Indonesia (as the Indonesian central bank).

Therefore, for the online payment sector, there are several regulations which may apply, among others: (i) Bank Indonesia Regulation No. 22 of 2020 on Payment System; (ii) Bank Indonesia Regulation No. 18 of 2016 on Operation of Payment Transaction Process; (iii) Bank Indonesia Regulation No. 20 of 2018 on Electronic Money; and (iv) Bank Indonesia Regulation No. 19 of 2017 on Operation of Financial Technology.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The issue was mainly focussed on the various infrastructure of e-money payments where e-money providers develop their own products and subsequently, in certain cases, they were able to have exclusive partnerships with several merchants in order to prevent the use of other e-money. However, this has been resolved by the utilisation of National Payment Gateway in Indonesia where the government has established interconnected switching and guarantee the interoperability of each payment channels.

Another thing which should be noted is that whilst the government does not prohibit overseas delivery and purchases, all payments conducted by any parties that concern Indonesia are subject to the obligatory use of the Indonesian Rupiah only. New types of payment methods are yet to be recognised by any prevailing regulation. An example is the use of cryptocurrencies, which is recognised as a form of payment in a small number of jurisdictions. However, cryptocurrencies are not recognised by law as a form of payment in Indonesia.



Enrico Iskandar is a founding partner of Bagus Enrico & Partners, a firm which advises companies in corporate and commercial transactions, with an emphasis on mergers and acquisitions, corporate restructurings, property, hotels and real estate, technology, media and telecommunications.

In his technology, media and telecommunications practices, Enrico has worked on a broad range of transactional, advisory and contentious matters, and regularly advises on regulatory issues on telecommunications (including market entry advice), networks and satellite operations, data protection/privacy, cloud data, payments, outsourcing, IT contracts, e-commerce, IoT and supply chain transactions. Enrico's considerable experience in relation to technology, media and telecommunications has enabled him to steer investors through inherent practical and regulatory hurdles.

Enrico's team has been recognised by the Asia Pacific Legal 500 over the last five years (2017–2021 editions) as Indonesia's 1st Tier law firm in IT & Telecoms practice. He has also been recognised by The International Who's Who Legal for the last seven years (from 2013 to 2019), as a leading individual in Data, Information Technology and Telecoms & Media practices.

Bagus Enrico & Partners

DBS Bank Tower 17th Floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3-5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Email: enrico@bepartners.co.id
URL: www.bepartners.co.id



Bratara Damanik is a senior associate of Bagus Enrico & Partners who has been primarily involved in various work in the technology, media and telecommunication areas. In addition, he also regularly advises clients within a wide spectrum of corporate and commercial matters on various sectors including M&A, construction, employment, as well as advising numerous corporate clients.

Bratara has been involved in a broad range of advisory work on regulatory issues regarding data protection, telecommunications and networks operation, IT contracts, cloud services, and in the e-commerce and fintech industries. He has also shown particular interest in the tech industry by studying and writing his master's thesis on blockchain at Queen Mary University, London.

Particularly for the technology sector, Bratara's recent representations include advising a major US-based tech company in the preparation of a streaming service activity in Indonesia and assisting venture capitals on their financing transactions into Indonesian-based tech companies.

Bagus Enrico & Partners

DBS Bank Tower 17th Floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3-5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Email: bratara@bepartners.co.id
URL: www.bepartners.co.id



Jonathan Cheong is a consultant at Bagus Enrico & Partners. He is heavily involved in numerous works pertaining to assisting both international and local clients on several non-contentious matters in relation to Technology, Media, Telecommunications (TMT) and digital businesses.

He undertakes works comprising advisory and legal compliance related to regulatory matters including data protection, cybersecurity, and IT contracts. Some of Jonathan's work includes advisory for an international tech company in their market entry strategy whilst ensuring compliance to the existing legal frameworks. His most recent matter encompassed representational and advisory work for the potential entry of a US-based cryptocurrency. He is also the coordinator for the firm's publications and articles which are published on regulatory research platforms and legal guides.

Bagus Enrico & Partners

DBS Bank Tower 17th Floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3-5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Email: jonathan@bepartners.co.id
URL: www.bepartners.co.id

Bagus Enrico & Partners ("BE Partners") is one of Indonesia's leading corporate and commercial law firms. Founded by professionals who are recognised for their experience in handling various notable transactions in Indonesia, BE Partners continues its growth with an equal commitment to our reputation as a "boutique practice focuses on client service", and provides its domestic and international clients with high-quality advice which is commercially focused and personally delivered.

BE Partners has received recognition from the main legal market reviewers. Some of the most international and respected reviewers have placed BE Partners' team as Indonesia's leading professionals in various practices. BE Partners' reputation in diverse aspects of Indonesian law, especially in relation to corporate/commercial law, banking, finance and insurance,

mergers and acquisitions, IT, media and telecommunications, energy and resources, property, hotels and real estate, as well as infrastructure, is outstanding.

www.bepartners.co.id



BAGUS ENRICO & PARTNERS
COUNSELLORS AT LAW

Ireland

Lewis Silkin LLP



Victor Timon

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

B2B e-commerce in Ireland is treated very much the same as non-e-commerce B2B business, in that much of the same legislation will apply. So, the Sale of Goods Act 1893 and Sale of Goods and Supply of Services Act 1980 would be the basic legislation covering either type of transaction. These include a buyer's rights in terms of merchantable quality, right to free possession and the like.

However, there are some laws that apply particularly to e-commerce transactions. These are a mix of directly applicable EU law and Irish implementations of EU legislation.

The Electronic Commerce Act 2000 regulates the manner in which business is to be conducted online and introduced electronic signatures.

The European Communities (Directive 2000/31/EC) Regulations 2003 (E-Commerce Regulations) further governs the use of online contracts.

The Eidas Regulation ((EU) 910/2014) regulates electronic signatures and electronic transactions, to provide a safe way for conducting business online.

The General Data Protection Regulation (Regulation (EU) 679/2016) also applies as does the Data Protection Act 2018 (DPA), which transposes its provisions into Irish law.

Ireland is also subject to the Geo Blocking Regulation (Regulation (EU) 2018/302) for online (and offline) sales under which a trader may not restrict access to its website through the use of geo-factors such as location or IP address.

The new Copyright Directive 2019/790 must be transposed into Irish law by 7 June 2021 and is intended to make copyright fit for the digital age. It gives content creators new rights to be rewarded for their efforts through licensing arrangements with information society service providers (ISSPs). It imposes new responsibilities on ISSPs and other platform providers to negotiate those licences fairly. It also obliges them to prevent infringing content appearing in their services or on their platforms.

There is no registration required in Ireland in general to conduct an e-commerce business, though see question 11.2 for the regulations applicable to online payment providers.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The legislation described in question 1.1 will also apply to B2C e-commerce transactions, but there are also additional legal provisions which are designed to protect consumers.

The Consumer Protection Act 2007 provides general protection for consumers in transacting with traders either through e-commerce or offline. These include provisions which prohibit a trader making false claims about a product or service. It also prohibits misleading advertising. In all, the Act lists 32 practices which are prohibited, backed up by a series of fines and other enforcement measures.

The European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013 implemented Directive 2011/83/EU (the Consumer Rights Directive) in Ireland. It governs so-called "distance contracts". The Regulations provide consumers with a 14-day "cooling off period" during which they can change their mind and cancel a purchase (with limited exceptions, such as for perishables and digital products). Goods must be delivered in 30 days. A trader cannot force a consumer to use a premium rate phone number in connection with his/her purchase.

In addition, the Regulations set out the information which a trader must provide to a consumer, such as a full description of the goods, the total price including any taxes and certain information required to identify the trader.

The European Communities (Unfair Terms in Consumer Contracts) Regulations 1995 (as amended) introduced a test of fairness for consumer contracts. They require that standard terms are written in plain and understandable language. The Regulations list certain terms that could be considered unfair, for example terms which provide for an automatic renewal of a contract without the consumer's agreement.

The European Communities (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003 further strengthened a consumer's rights. They stipulate that goods must comply with their description and provide for repair and replace remedies where that is not the case.

The Consumer Protection (Gift Vouchers) Act 2019 introduced a minimum five-year validity period for most gift vouchers.

The Consumer Insurance Contracts Act 2019 introduced specific requirements for insurance contracts with consumers (note for the purposes of this Act, “consumer” also includes small businesses with an annual turnover of less than €3 million). It will not be fully in effect until 1 September 2021.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

It is now nearly three years since the GDPR came into force in Ireland; the Data Protection Commission’s (DPC) Annual Report issued in February 2021 showed some interesting trends since its introduction as well as some shifts in focus from last year.

In the calendar year 2020, complaints to the DPC dropped significantly as perhaps the newness and interest in the GDPR started to wain. There were 4,660 domestic complaints – down from over 7,000 in 2019. Access requests continue to be the largest category of complaints (30%), followed by fair processing (27%) and disclosures (26%).

The DPC handled a total of 10,151 cases in 2020, up 9% on 2019 figures (9,337).

Valid data breaches notified to the DPC in 2020 (6,628) were up 10% on the previous year’s figure. Unauthorised disclosures made up 86% of breaches (up 3%).

As of 31 December 2020, the DPC had 83 ongoing statutory inquiries (up 12), including 27 cross-border inquiries (up six). In the technology sector, the DPC is currently involved in six statutory inquiries in relation to several high-profile multinational tech companies.

Decisions and fines from two enquiries into “big tech” companies are expected later in 2020.

Having considerably increased its manpower and resources over the last couple of years, the DPC has become much more active in relation to investigations and prosecutions. The area of direct marketing offences continues to be a target and last year 147 electronic direct marketing cases were concluded.

The DPC is the lead supervisory authority for a number of multinationals, and under the “One Stop Shop” (OSS) system set out in the GDPR. As a result, the DPC received 354 cross-border processing complaints under the OSS (down from 457), which were lodged by individuals via other EU data protection authorities last year.

The DPC again spent significant time engaging with stakeholders to provide information on Brexit, particularly in relation to Irish companies transferring personal data to the UK.

Having reported in April 2020 on the mis-use of cookies (which it followed up with guidance), and because of the widespread non-compliance, it issued a deadline of October 2020 for firms to comply. By year-end the DPC had investigated and commenced enforcement action against a number of website operators in respect of their use of cookies. The Report confirms that this process of cookie investigations followed by enforcement action will continue throughout 2021.

In May 2020, the DPC issued its first fine under GDPR. Tulsa, the State’s child and family agency, was fined €75,000 for three data breaches.

In December 2020, the DPC issued its first fine in a cross-border case, fining Twitter International Company €450,000.

A new trend in 2020, which the Report finds disturbing and a waste of resource, has been the use of the DPC’s complaints service to deal with other grievances that are not data protection issues. A growing trend is to use DSARs (Data Subject Access Requests) in disputes with employers.

Another significant piece of work in 2020 was consultation and engagement between the DPC and public health authorities on the rollout of the Covid-19 contact-tracing app.

The DPC has faced much criticism in the past year for its slow responses and was recently called before a parliamentary committee in Ireland to make its case. In fact, the DPC claims that it continued to reduce conclusion times for cases (average days taken to conclude a case has reduced by 53% since the GDPR came into application, according to their Report). However, expect pressure from other national supervising authorities for speedier resolutions to continue in 2021.

Finally, 2020 was the year that the Schrems II decision was finally published following referral by the Irish High Court on the request of the DPC.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Fintech

Privacy challenges faced by fintech companies are not dissimilar to those in other industries. However, one key area where they may be ahead of other industries is the drive to use biometric data to increase security. Biometric data is regarded as “special category data” under Article 9 of the GDPR (section 2/45 DPA). As such, it would require the explicit consent of the data subject before it could be processed.

The systems for deploying biometric data would need to be developed on the basis of “privacy by design” set out in Article 25 of the GDPR (section 76 DPA), which requires embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage.

It is also likely that a Data Protection Impact Assessment would need to be carried out and documented under Article 35 of the GDPR (section 84 DPA) to analyse the risks involved for a data subject’s rights and to determine if a deployment could go ahead based on the benefits involved.

Many fintech companies operating in Ireland are part of much bigger international organisations and they face the challenge of ensuring that any transfers of data outside of the jurisdiction meet the requirements for international transfers under Chapter 5 of the GDPR (Chapter 5 DPA).

While Brexit had been on the horizon as a possible challenge, this should no longer be the case as at the time of writing it looks like an adequacy decision for the UK will be approved by the Member States of the EU. Finally, those fintech companies based outside of Ireland but marketing their services to Irish citizens will also have to comply with the GDPR.

Retail

Recent challenges for the retail industry have largely focussed on dealing with Covid-19. There has been an explosion in online shopping for example and many retailers who previously did not have transactional websites have introduced them. There has been a consequent need to introduce appropriate privacy policies and deal with the security issues that come with accepting and storing credit card details and the like.

Brexit also brought its own problems for British retailers who target the Irish market. If they do not have a presence in Ireland or another Member State of the EU, then following Brexit, they are obliged under Article 27 of the GDPR to appoint a representative for GDPR compliance purposes inside the EU.

Retailers as employers may also have to deal with additional privacy issues on a return to work, depending on their use of the contact tracing app or digital vaccine passports (see under Digital Health at the end of this Section).

AI

Due to the very nature of AI, there seem to be two aspects of the GDPR which are going to be regularly applicable.

The first is Article 25 of the GDPR (section 76 DPA), which obliges a controller to build privacy by design and default into any new systems.

The second is Article 35 (section 84 DPA), which states that where a type of processing uses new technologies, likely to result in a high risk to the rights and freedoms of people, the controller must carry out a risk assessment. In particular, for instances of automated processing on which decisions are based that produce legal effects, a Data Protection Impact Assessment (DPIA) must be conducted.

In deploying an AI system, a company will also have obligations pursuant to Article 22 (sections 57/89 DPA) and the European Data Protection Advisory Board's guidance to explain the logic behind an automated processing system. In terms of transparency, a controller will need to explain its processing anyway. Where the machine itself is making the rules, that may be difficult.

The fact that a machine may make decisions without human involvement may make any need to obtain specific consent much more difficult, unless of course that too is built into the algorithm.

While in the UK the ICO has issued guidance on how to explain AI decisions to data subjects, so far there has been no similar advice in Ireland.

Digital Health

Health data classifies of course as special category data under Article 9 of the GDPR (section 2/45 DPA), and so needs special protection.

As Ireland's health system continues to adopt more technological solutions and moves further away from an unconnected and manual approach, it will face the same challenges as other industries in terms of cyber security and protection of information that is now stored in the cloud.

New digital technologies that allow for remote patient monitoring, consultations by video link, and real-time data being obtained from medical devices and wearables, with the ensuing increase in the volume of data, will undoubtedly provide more privacy and security challenges.

Stakeholders in the digital health industry, whether controllers or processors, will need to continually review their internal procedures, training and technology to ensure that they can meet the demands of an explosion of data and data sources.

In 2020 the health industry faced the challenges of Covid-19 and remote consultations became more common. Obviously this introduced challenges for compliance such as the recording of video calls and the like.

In addition, in 2020 the Health Service Executive introduced a contact tracing app for Covid-19 which was implemented in consultation with the DPC. This app may pose data protection issues in the near future if employers for example insist on it being used by employees. Similar challenges may arise if a digital vaccine passport is introduced. If that passport is to be used say to gain access to sports events or other events open to the public then those seeking to use it will likely be required to conduct DPIAs before implementing it.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

There are government and government agency initiatives for

the development of products in these areas. None of these are particularly steered towards testing.

In fintech, the Government's IFS2020 programme was established in 2015 to support the development of fintech products. The Central Bank of Ireland (CBI) also runs an innovation hub.

In respect of retail, Enterprise Ireland, a government agency which supports domestic businesses, put together a funding package to encourage small retailers to go online during Covid-19. The purpose of the fund is to enable Irish-owned retailers to enhance their digital capability and to develop a more competitive online offer. Grants of up to €40,000 or 80% of project costs were made available to help small retailers develop a sophisticated and transactional online presence. This is to include research, consultancy costs for strategy development, implementation and training.

In respect of the development of AI products, CeADAR is an AI innovation hub supported by two government agencies, Enterprise Ireland and IDA Ireland.

For digital health products, the Health Innovation Hub Ireland was established by the Department of Business, Enterprise and Innovation and the Department of Health, supported by Enterprise Ireland (EI) and the Health Service Executive (HSE) to drive collaboration between the health service and enterprise.

The DPC does not play any defined statutory role in the development or testing of such products, other than its overriding role of enforcing the GDPR. In particular, the DPC has issued guidance in respect of the situations in which it believes a DPIA should be carried out.

In addition, where a DPIA is required for the deployment of any of these types of products and, following its completion any identified risks cannot be managed and the residual risk remains high, then the instigator of that DPIA is obliged, pursuant to Article 36 of the GDPR (section 84 DPA), to consult with the DPC for its opinion before progressing with the project.

Even if a consultation is not required, the DPIA can of course be reviewed by the DPC at any time.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

There are a number of international standards applicable to e-commerce which also operate in Ireland.

PCI DSS (Payment Card Industry Data Security Standard)

This sets out a widely accepted international set of security controls that was established to help businesses safely process credit card, debit card, and cash card transactions. The standards are applicable to any businesses that store, process or transmit cardholder data.

Payment Services Regulations (S.I. No. 6/2018 – European Union (Payment Services) Regulations 2018)

This implemented the revised Payment Services Directive – Directive on payment services in the internal market (EU) 2015/2366.

For further details see question 11.1.

ISO 27001/27002 (International Organization for Standardization)

This sets out the specification for an information security management system. This is seen as the 'gold standard'. Its best-practice approach helps organisations manage their information security by addressing people and processes as well as

technology. It is mostly for large organisations, and was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The Criminal Justice (Offences Relating to Information Systems) Act 2017

This piece of legislation sets out essentially five types of hacking or cyber-crime offences. These are:

- accessing an information system without lawful authority;
- interference with an information system without lawful authority;
- interference with data without lawful authority;
- intercepting the transmission of data without lawful authority; and
- use of a computer program, password, code or data for any of the above.

The GDPR/Data Protection Act 2018

The Data Protection Act 2018 implemented the GDPR in Ireland and governs how personal data is collected in Ireland. It requires that businesses keep personal data secure and only permit third parties' access to personal data subject to sufficient guarantees regarding the security of the processing services. Businesses must implement measures that are both technical (e.g., firewalls, anti-virus programs, perimeter scanning tools) and organisational (e.g., policies and procedures that must be followed by personnel regarding cybersecurity) to safeguard personal data. Businesses are required to protect against unauthorised or unlawful use of personal data and against loss, destruction and damage of the same.

Article 32 GDPR (section 72 DPA) requires controllers and processors to implement technical and organisational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data.

The e-Privacy Regulations (S.I. No. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011)

The e-Privacy Regulations govern the use of electronic communications. In particular they set out the rules applicable to marketing emails, texts and phone calls; they also govern the use of cookies; however, note that the consent required for the use of cookies has now changed to a GDPR standard (see question 2.1 above). In addition, they also cover the security of public electronic communications services and data privacy.

A new EU e-Privacy Regulation has been under discussion for a number of years now, but at the time of writing is still in draft form. It will be broader in scope than the current regime applying not only to traditional telecommunications operators but all communications service providers including instant messaging apps and the like.

The NISD Regulations (the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018)

The NISD Regulations implement the Security of Network and Information Systems Directive 2016/1148/EU in Ireland. That Directive sets out to harmonise cybersecurity measures for operators of “essential services” (such as businesses in the energy,

transport and/or health sector) and “digital service providers” (such as cloud service providers and providers of online marketplaces) that offer services to individuals.

Businesses subject to the NISD Regulations are required to implement appropriate and proportionate measures to manage risks posed to network and information systems and to prevent, and minimise the impact of, incidents affecting the security of the network and information systems.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In general, Irish people have embraced new technologies and the numbers shopping online continue to grow. A report published in the first quarter of 2021 by Ireland Online in conjunction with Digital Business Ireland (the .IE Tipping Point Report) noticed some trends for Ireland's online shoppers in 2020 as a result of Covid-19:

- Firstly, it notes that while there was an initial patriotic surge during the earlier months of the pandemic, with shoppers seeking to fulfil their requirements from Irish retailers, the majority of online shoppers have swung back from indigenous SMEs to international retailers.
- It found that 68% of consumers said they spent more online in 2020 than they did in 2019.
- 30% of SMEs surveyed now claim to sell their products via an online store, up from 25% in 2020.
- And finally, 86% of Irish SME retailers say they have experienced an increase in sales or sales enquiries from their online store since the pandemic began.

Also, the impact of Brexit on online shopping should not be underestimated. Many Irish shoppers would have used sites like amazon UK to buy goods and instead now look to sites like amazon Germany which has introduced an English language version. There is a fear that customs duties will be added to all goods bought from the UK (which is not currently correct as none are levied on orders under €150 for example and many popular goods such as books and computers are not liable for import duty).

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Ireland has a relatively young population which adapts quickly to change and new opportunities. While cash may have been key for the older generation, even most of those have become comfortable with the use of cards. Also, as a result of Covid-19, use of cards and contactless payments was preferred to cash.

Apple Pay and Google Pay are now also increasingly popular. In a 2020 survey carried out by AIB bank, it found that consumers are spending 30% more per transaction using contactless on their debit cards – in many cases to avoid unnecessary interactions in shops.

The survey showed that the debit card is the most popular choice of instore payment method among all age cohorts, except those under 25 where it accounts for 28% of spend.

Apple Pay and Google Pay now account for 37% of all instore transactions by those who are under 25, with the average amount this age cohort are spending in store also up 24% and 35%, respectively.

Customers over the age of 45 are spending 31% more using their digital wallets, the figures also show.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

According to Ireland's Central Statistics Office, fewer internet users report purchasing goods from sellers from other EU countries (56% of internet users in 2020 compared to 68% in 2019), with a marginal increase in internet purchasing from sellers from the rest of the world (38% of internet users in 2020 compared to 37% in 2019).

Large global e-commerce websites such as amazon and ebay continue to take a huge slice of the market, as well as globally branded retailers. According to Wolfgang Digital, in 2020, the top 15% of e-commerce businesses captured 84% of consumer spend.

In the Ireland Online and Digital Business Report mentioned in question 4.1 above, Irish consumers surveyed said that they view international retailers as more competitive on price, range and online experience, but they view Irish SME retailers as more reliable and trustworthy.

As mentioned in question 2.3 above, in April 2020, a scheme was introduced to assist Irish online traders. Administered by Enterprise Ireland, retailers can now avail of grants up to €40,000 to help them develop their online trading capacity.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Ireland has a huge technology base with many of the world's largest technology and social media companies having their EMEA headquarters or manufacturing facilities here. So, it is no surprise therefore that companies such as Apple and Microsoft are among Ireland's biggest exporters.

Some well-known indigenous brands which would be seen as "typically Irish", such as Waterford Crystal, have been very successful in selling abroad and trade substantially through their websites. Another successful growth area is clothes. Magee, an Irish suit maker, saw an 80% growth in foreign online sales after re-purposing its website.

However, as you would expect with Covid-19 Irish medicine and pharmaceutical exports soared in 2020. They rose by 25% to €62 billion last year, accounting for 39% of all Irish goods exports in 2020.

According to the CSO, the EU accounted for €63.9 billion (40%) of total exports in 2020, an increase of €7.2 billion on 2019. The US was the largest export destination in 2020, accounting for €49.9 billion or 31% of total exports. Interestingly, the value of exports to Britain in 2020 fell by 9% to €12.4 million and accounted for 8% of total Irish exports. Irish exports going to Asia were 12.1%.

Enterprise Ireland assists companies in their drive into global markets.

Language is not seen as a barrier as most Europeans in particular have English as a second language.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

There are no particular trends that are peculiar to Ireland. All website operators are encouraged to make navigation simple and their websites must be mobile-friendly. Of the top 10 most popular websites in Ireland, only two belong to Irish companies.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

In Wolfgang Digital's Annual Report on e-commerce (On The Money: The Irish E-commerce Report 2021), e-commerce revenue for retailers is stated to have grown by 159% in 2020. Compare that to average annual growth from 2017 until 2019 at 32%.

Covid-19, they believe, has revolutionised online retail in two ways. Firstly, while the growth in online shopping was always going to increase in time, the pandemic accelerated that growth faster than anyone would have predicted. Secondly, Covid-19 has brought new people into the e-commerce economy who likely would not have participated otherwise. The Report highlights wealthy over 65s as the least likely to shop online pre-Covid-19. They are now a large proportion of the Tesco delivery spots.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

There are a number of pieces of legislation that can be used to protect brands and prosecute offenders.

Trademarks

These can be registered in Ireland or in the European Intellectual Property Office, or the World Intellectual Property Office depending on the international scope of protection required.

Actions for infringement can be brought by the trademark owner under the Trade Marks Act 1996, or the EU Trademark Regulation (Regulation (EC) 207/2009) for EIPO trademarks.

The Director of Public Prosecutions can also initiate criminal proceedings under the Trade Marks Act 1996 for trademark infringement.

Unregistered trademarks can be protected by taking an action for passing off, which is a common law tort – where one party attempts to mislead the public into thinking that their brand is associated with another brand.

Copyright

Copyright is protected in Irish law by the Copyright and Related Rights Act, 2000 (CRRA). Protection is automatic and there is no system of registration in Ireland.

Subject to some small fair dealing exceptions, a copyright owner can prevent another party from using its work without permission (usually granted by way of a licence for a royalty). A copyright owner can sue for infringement under the CRRA.

Domain Names

These are now a crucial part of a company's branding. The most common issues are firstly cyber-squatting, where someone registers a name to thwart a genuine user's ability to register it

in the hope of extracting a large price for it; the second is where different companies may have legitimate interests in the same domain name.

Under ICANN rules, an aggrieved trademark holder can use the Uniform Domain Name Dispute Resolution Policy to try and resolve these issues.

Designs

For infringement of design rights in the EU, an injured party can avail of the regime under the European Community Designs Regulation (6/2002/EC) (CDR). The CDR is augmented by EIPO guidelines issued from time to time.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Ireland does not have a separate court for intellectual property litigation, and instead such disputes go through the regular court system.

Litigation in Ireland tends to be an expensive undertaking, especially in the higher courts and many digital businesses are early stage companies, which may not have the resources to fund a long court case. Alternative dispute mechanisms are available in Ireland and many such companies now seek to use these.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

If a company is using the infrastructure located in a data centre to run its business or contracting with a cloud services provider for that purpose, it will need to ensure its data will remain secure, available and accessible. This is typically done through a services agreement, which should contain a commitment to those matters as well as to service levels.

If a company is a controller of personal data, then it will be required to include a data processing agreement or addendum as part of its contractual arrangements with the service provider, to meet its obligations under Article 28 of the GDPR (section 80 DPA).

The DPC has published guidance on its website as to what conditions they consider to be mandatory for such contracts.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

There are none. However, a controller is subject to Chapter 5 of the GDPR, which governs transfers of personal data to third countries and international organisations. Article 44 of the GDPR (and a number of sections of the DPA) states that if a controller transfers personal data out of the EU, it must enjoy the same level of protection as it gets under the GDPR.

In the absence of an adequacy decision or consent, personal data may still be transferred to a non-EEA country subject to the putting in place one of the appropriate safeguards set out in Article 46 of the GDPR (section 98 DPA). These include the “Standard Contractual Clauses” or “Binding Corporate Rules”. The safeguards must be outlined in a legally binding contract between the transferring and recipient parties.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

In 2017, Ireland adopted a new trade and investment strategy, “Ireland Connected: Trading and Investing in a Dynamic World”. Part of that strategy includes “connectedness” and the harnessing of digital technologies to increase and facilitate trade.

Irish Revenue and Customs already only use automated processes for interacting with traders importing goods into Ireland.

Paperless trading, registration of information online and e-certificates continue to be examined, particularly in the context of Brexit and speeding up the movement of goods, following the additional requirements resulting from the UK being outside the EU.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

While digital technologies for trade in general, such as those used by the Irish Revenue and Customs Service, will no doubt continue to develop and the WTO and OECD are very active in this area.

Of more immediate concern in Ireland because it is on our doorstep is the Northern Ireland Protocol (part of the Brexit trade deal signed between the EU and UK). It was hoped that technology would make the border between the Republic of Ireland and Northern Ireland seamless, but so far this has not happened.

Northern Ireland has remained within the EU for the purpose of the supply of goods, whilst Great Britain (the rest of the UK) is now a “third country”.

While many solutions have been promulgated in general terms, none of the stakeholders have so far come up with a technology solution that all parties can agree as workable.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Ireland has a number of tax incentives which are available to digital businesses.

There is a 25% tax credit available to companies for research and development expenditure. This can be claimed for activity prior to trading also. The credit can be offset against the company’s corporation tax liability in the year in which it occurred. It can be claimed in addition to a 12.5% deduction for the expenditure, giving an effective rate of 37.5%.

The tax legislation also provides for a tax deduction for trading companies which expend capital on qualifying intellectual property assets. They are defined quite broadly and include patents, trademarks, copyright goodwill, domain names and customer lists.

The Knowledge Development Box provides for a lower corporation tax rate of 6.25% on profits arising from qualifying assets, which are themselves the product of qualifying R&D. This incentive is fully compliant with the OECD's modified nexus approach (linking the relief to R&D and IP). To avail of the relief, a company must be earning income from those qualifying assets (such as through licensing or other exploitation).

Under the Taxes Consolidation Act 1997 (as updated each year by the Finance Act), there is also currently a tax relief available for start-up companies up to the end of 2021 with corporation tax due of €40,000 or less in a tax year (and partial relief if it is between €40,000 and €60,000). The exact amount of the relief will depend on the number of employees in the company.

Acquisitions of IP are also exempt from stamp duty in Ireland.

There are additional grants and services made available through the IDA (Ireland's agency for inward investment) to foreign companies who are considering investing in Ireland.

Finally, Ireland has a low corporate tax rate of 12.5% which makes it attractive for companies to locate here.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

VAT would seem the most likely area where disputes will arise for a number of reasons.

VAT distinguishes between goods and services (services being everything that is not a good!). In the world of digital and downloads, the distinction may become more difficult (which is important in terms of determining place of supply and accountability).

From July this year, there will be changes to how the current tax thresholds for B2C will operate. Currently, a B2C online trader can apply VAT in its home country on its distance sales of goods until the point that they exceed the relevant threshold in the customer's EU Member State. From July 2021, the individual thresholds in each Member State will be replaced by a single EU-wide threshold of €10,000. Thereafter, once the trader has achieved those sales across the whole of the EU, it will be forced to apply the rate applicable in the customer's home country. This will require knowledge of all the different VAT rates applicable in the different Member States. This is by no means a simple task and may lead to miscalculations and disputes.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In Ireland, individuals are either employees or self-employed, independent contractors; there is no intermediate or hybrid status. How the relationship is described in the written agreement between the parties is only one of a number of factors that will be taken into account when determining whether an individual is an employee or an independent contractor; what is important is how the relationship works in practice. The level of "control" exercised by a company over an individual and their work is the most common factor used to determine whether

someone is an employee or not. A company should consider how the arrangement works in practice and should ensure that the written agreement accurately reflects this.

The vast majority of employment rights are afforded to employees only, for example, the right to be paid for annual leave and minimum wage, protection from unfair dismissal and the right to a redundancy payment. Both employees and independent contractors will benefit from the protections afforded by whistleblowing and equality legislation. Independent contractor arrangements work best where the individual is in business on their own account and they provide services to more than one client. This type of agreement provides flexibility to both parties and can be advantageous from a tax perspective as no employer PRSI (social insurance) is payable. However, mis-classifying an individual as self-employed when in reality they are an employee could result in significant costs for a company which will be liable for any underpayment of tax and social security plus interests and penalties. It also means that the individual will have accrued statutory employment law rights as against that company.

There are a number of different types of employment arrangements, depending on what type of resourcing a company requires. For example, a company may want to employ individuals on a part-time basis or for a specific project or fixed duration. Alternatively, companies may choose to engage an employment agency to supply staff, rather than hire them directly. Irish employment law generally does not distinguish between these different categories of employees and there is much legislation in place to ensure that these categories of employees are treated no less favourably than permanent, full-time employees. "Zero-hour" contracts which require individuals to be available for work but with no guaranteed hours are prohibited by the Employment (Miscellaneous Provisions) Act 2018 except for in very limited circumstances.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

A company has obligations under employment law in respect of all its employees, whether they carry out work on or away from its physical premises. While there is no specific regulation in place in Ireland which regulates remote working, employers should pay particular regard to their obligations under health and safety, working time and data protection legislation.

Under the Safety, Health and Welfare at Work Act 2005, employers have specific duties to ensure the safety, health and welfare at work of all employees, whether or not that work is being done at the employer's premises. This includes providing and maintaining a safe workplace, preventing any improper conduct or behaviour likely to put the safety, health and welfare of employees at risk and providing instruction and training to employees on health and safety. Employers must carry out a risk assessment of the workplace, even where this is not the employer's premises (for example, an employee's home office). Organisations should have policies in place which clearly set out the employer's and employees' health and safety obligations including an obligation on employees to report health and safety risks and work-related accidents.

The Organisation of Working Time Act 1997 governs minimum working hours and rest breaks. Under the Act, employers are obliged to record employees' working time on a daily basis including start and finish times and rest breaks. Remote working can make it particularly challenging for organisations to comply with their working time obligations.

Employers should put in place policies and systems for recording employees' working hours and rest breaks when working away from their premises.

Compliance with the GDPR/DPA will also be an issue where employees are not based at a company's premises. Companies should put in place robust data protection policies including procedures for reporting data breaches and ensure ongoing training for all staff on their data protection obligations. Extra security measures may need to be taken for employees working remotely, such as the provision of encrypted laptops.

As part of the Strategy for Remote Work (a policy launched by the Government to acknowledge the changes to the working environment brought about by Covid-19 which are likely to continue beyond the pandemic), the Department of Enterprise Trade and Employment has introduced a new Code of Practice on the right to disconnect. Its purpose is to promote a culture of good work/life balance and breaking bad habits whereby people feel obliged to respond to messages out of hours. The Code primarily addresses rights which already exist under Irish employment law. However, it does go slightly further, to address the fact that working outside of normal working hours has become a "bad habit" which needs to be broken.

The Code emphasises that employers cannot generally allow employees to work for more than an average of 48 hours a week and should be keeping records of hours worked. It highlights the employer's duty to "manage and conduct work activities in such a way as to prevent, so far as is reasonably practicable, any improper conduct or behaviour likely to put the safety, health and welfare [of employees] at risk". Further it reaffirms that employment contracts should include the hours of work that the employer reasonably expects the employee to work in a normal working day and a normal working week. However, the Code helpfully makes clear that the right to disconnect is not an absolute right. The Code recognises that there may be occasional legitimate situations where business and operational reasons require contact out of normal working hours.

The Strategy for Remote Work is also expected to lead to the introduction of a formal right of employees to request remote working arrangements from their employer but legislation has not yet been published on what this right might entail and the reasons an employer may be able to rely on to justify refusing a request.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

In Ireland the Government recognises that remote and home working is at least to some extent here to stay following Covid-19. The Strategy for Remote Work referred to in question 9.2 above aims to build on the progress made in the adoption of remote work during the pandemic period and its objective is to ensure that remote working is a permanent feature in the Irish workplace in a way that maximises economic, social and environmental benefits. Highlights include mandating that home and remote work should be the norm for 20% of public sector employment; mapping and investing in a network of remote working hubs across Ireland; and legislating for the right to request remote working.

Managing mental health issues arising from home working is also likely to be a key requirement for employers as part of their health and safety obligations.

Employers will have to consider whether remote working should include allowing employees to working from a different country. It would be necessary firstly to have knowledge of an employee's local laws and whether they could automatically

apply. Such local laws could for example specify longer holiday periods or minimum pay. Employers would also need to be aware of any implications for payroll taxes along with any permanent establishment risks from a corporate tax perspective depending on the type of work the employee carries out.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

There are no real legal barriers to entry, such as registration for example, but there is much legislation and regulation to deal with as set out elsewhere in this chapter.

A B2B offering will of course be easier to set up and manage than a B2C offering, as in the latter, the trader will not have to deal with consumer legislation.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

There are considerable advantages for a digital business operating in Ireland.

In section 8, the various tax incentives are described, as well as the grants available from the IDA for foreign companies setting up in Ireland.

In addition, we have a well-educated and trained workforce able to work easily in the technology industry generally.

Ireland is strategically situated between Europe the UK and the United States.

As of the beginning of this year, it is the only English-speaking country in the EU.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

There is currently no designated regulator in Ireland tasked with overseeing digital business.

The most relevant regulator is the Data Protection Commission, but it focuses solely on privacy issues. From reviewing its annual report, it seems likely that this year, there will be a focus on cookie compliance and the treatment of children's personal data.

The Advertising Standards Authority for Ireland is a non-statutory body which reviews and reports on advertising including digital advertising. While it can request changes to or the withdrawal of adverts, it has no enforcement powers.

A couple of changes are on the horizon. Firstly, the Government has published the "The Online Safety and Media Regulation Bill", which will introduce new online safety laws to bring legislation up-to-date with the EU Audio-visual Media Services Directive. This legislation when passed will introduce a new regulatory body, the Media Commission, which will include an Online Safety Commissioner to police online safety codes and how online video sharing services deal with harmful content.

In December 2020, the EU Commission published the Digital Services Act (DSA), which will operate as an EU Regulation having direct effect in the Member States. The purpose of the DSA is to compel providers of online intermediate services to take more responsibility for illegal content on their platforms. Every Member State including Ireland will be required

to appoint a Digital Services Coordinator (DSC) to oversee compliance and enforcement.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Payment Services Regulations 2018 (S.I. No. 6/2018 – European Union (Payment Services) Regulations 2018 (PSR))

These implemented the revised Payment Services Directive (EU) 2015/2366 – PSD2) and replaced the 2009 Regulations (PSD1). They are the most important piece of legislation in respect of online payments.

The PSR are intended to reduce fraud while opening up payment markets to new entrants. Their operation in Ireland is governed by the Central Bank of Ireland (CBI).

PSD2 is intended to be a positive development for all users of payment services, but particularly consumers. It introduced the concept of Strong Customer Authentication.

E-Money Regulations (the European Communities (Electronic Money) Regulations 2011)

The E-Money Regulations transposed Directive 2009/110/EC into Irish law and apply to providers of e-money services. The E-Money Regulations have been further updated by PSD2.

The GDPR/Data Protection Act 2018

This will also be applicable to online payment service providers. For more detailed analysis, see elsewhere in this chapter.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Online payment providers must comply with the provisions of PSD2 as described in question 11.1. This will involve initially an authorisation and approval process carried out by the Central Bank of Ireland (CBI), before any service can begin.

An authorisation process is also required for e-money service providers under the E-Money Regulations.

PSD2 and the E-Money Regulations set out various capital and probity measures which a company must meet in order to be authorised.

The CBI places much emphasis on having “hearts and minds” located in Ireland. This essentially means that the CBI will need to be satisfied that the applicant will be properly run in Ireland and that the CBI will be able to supervise it effectively. As a minimum, it requires a senior management team overseen by a strong board and an appropriate organisation structure with reporting lines.

Online payment providers will also need to be mindful of the GDPR and where applicable consumer legislation, described elsewhere in this chapter. In addition, the CBI has published a number of consumer codes which may be relevant.

Finally, they may also be subject to anti-money laundering legislation.



Victor Timon is a partner in the Dublin office of the international law firm Lewis Silkin, where he heads up the Commercial, Technology and Data practice of the firm.

He has over 35 years of legal experience having been an in-house counsel and then a partner in leading law firms in London and Dublin. Victor is qualified to practice in both England and Ireland. He regularly speaks at conferences on e-commerce, technology and data privacy issues in particular.

Victor is a member of ITechLaw, the global association for technology lawyers which spans more than 60 countries and helped organise their European Conference in Dublin in 2019.

Lewis Silkin LLP
26 Lower Baggot Street
Dublin 2
Ireland

Tel: +353 1 566 4508
Email: victor.timon@lewissilkin.com
URL: www.lewissilkin.com

In a world full of possibilities, we help make the most of what really matters to you – your Ideas, your People, your Future. We pride ourselves on providing solutions to your most complex business challenges, with a pragmatic and human touch.

We have renowned expertise advising creative, innovative and tech-focused businesses across all sectors and our multi-disciplinary teams provide clients with commercial insight and specialist knowledge from a range of legal disciplines including: commercial, IP, data and privacy, corporate, employment, immigration, dispute resolution and real estate.

We work with an international community of clients, helping them achieve their business objectives worldwide through a combination of our own offices, international desks and strategic alliances.

Our people are at the heart of what we do, and are committed to building strong, long-lasting relationships, to providing efficient, high quality and cost-effective legal services, and to constantly challenge ourselves to provide creative solutions.

www.lewissilkin.com



LEWIS SILKIN

Italy

Portolano Cavallo



Irene Picciano



Fabiana Bisceglia



Donata Cordone



Livia Petrucci

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

No prior authorisation is needed for launching a B2B platform in Italy but a notification of start of activity ("*Segnalazione Certificata di Inizio Attività*", sc. "SCIA") must be submitted to the Municipality where the business will be started; other fulfilments may be required in the food sector.

Further, online traders must comply with the requirements set forth by the Italian E-commerce Decree (Legislative Decree No. 70/2003) including, among others, (i) the obligation to provide certain information (*e.g.*, trader's name, address, contact details, *etc.*) before the conclusion of the contract, and (ii) the obligation to acknowledge the customer order, unless agreed otherwise with the customer.

It is highly recommended to collect evidence that the customer was aware of the contract's content before it becomes binding (for example, by requiring the customer to accept it through a proper tick-box). A double-tick mechanism would need to be adopted, as per standard market practice, to provide acceptance of the "burdensome" clauses.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

An online trader that provides B2C e-commerce shall comply with all the E-commerce Decree's obligations (as none can be waived in B2C arrangements), as well as with the additional rules set forth by the Consumer's Code (Legislative Decree No. 206/2005), including, among others, the ones below.

A minimum set of information shall be clearly provided to consumers before the conclusion of the contract (*e.g.*, on the goods/services, withdrawal right, legal warranty, *etc.*). Prices shall be shown as already inclusive of taxes and all additional shipping, delivery or postal charges.

Consumers shall also be provided with confirmation of the concluded contract and the minimum set of information above, through a durable medium (*e.g.*, by email, either as an attachment or within its body), at the latest at the time of delivery of

the items. Further, online traders are required to make clear that clicking any 'order button' entails an obligation on the consumer to pay money.

Consumers are entitled to withdraw from online contracts within a period of 14 days from the receipt of the item (for contracts of sale of items) and receive a refund.

Lastly, it is highly recommended to translate into Italian language all the information directed to Italian consumers.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

In the last year and a half, the Italian Data Protection Code (Legislative Decree No. 196/2003, "IDP Code") has been amended by the GDPR Decree (Legislative Decree No. 101/2018), which was issued to adapt the former data protection legislation to the provisions of the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"). Among others, the amended IDP Code requires a series of implementation measures to be issued by the Italian Data Protection Authority (*Garante per la protezione dei dati personali* – "Garante"). By way of example, the Garante: (i) revised the so-called "general authorisations" applying to the processing of "sensitive" data in different fields (*e.g.*, employment, scientific research, *etc.*) to identify the provisions that were compatible with the GDPR and that continue to apply as additional limitations imposed by Italy to the processing of such data; and (ii) assessed to what extent the provisions set out in some of the Codes of practice and conduct attached to the IDP Code were compatible with the GDPR. A number of implementation measures concerning, among others, data belonging to particular categories and judicial data, however, have yet to be taken. Furthermore, the Garante has drafted new Guidelines on cookies which have been under public consultation; the publication of the final text is pending.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

The main issues in fintech, retail, AI and digital health are represented by security standards, governance models and transparency requirements.

In the first place, the development of new technological means and their pervasive use puts a strain on security systems, which should be able to face the risks connected to the data processing activities, as well as avoid and remedy any data breaches. This is

most evidently the case for the sectors under analysis which tend to process particularly sensitive data that require even higher security standards.

Secondly, the new accountability principle introduced by the GDPR demands organisations to define data processing activities and data flows in advance and accurately, which may require organisations to rethink some aspects of their business – for instance, the choice of their providers – to ensure that the governance of the data flow is not only efficient, but also compliant with data protection requirements.

Thirdly, in response to the obligation of transparency, organisations have to carefully evaluate the use of AI algorithms, especially in areas such as fintech and digital health. Indeed, such systems are characterised by the opacity of the logic involved, which can be an obstacle to understand and explain the processing activities, as required by the GDPR. Generally, the more the algorithm will perform the less the logics behind the process will be intelligible. This *impassé* deeply affects the digital health sector, where the growing interest in providing patient care through automated decision-making systems is often held back by the impossibility to ensure transparency. Furthermore, the governance issues mentioned above are heightened by the use of AI systems that often involve interaction between various and divergent actors in the data processing, requiring a complex structure from a data protection point of view. Critical issues that will need to be dealt with at a contractual level include: auditing mechanisms; management of the data flows, including data transfers in countries that do not ensure sufficient guarantees for the personal data; and management of the cyber risk in the production chain.

Lastly, in these sectors, there is an increasing interest in the use of biometric data for several purposes (*e.g.*, to identify a user, to improve the customer experience, *etc.*) which, in addition to the issues mentioned above, requires further specific assessments on the necessity and proportionality of the processing.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The Italian Government and regulatory authorities have been proactive and adopted various measures to support the spread of AI systems and the development of fintech and digital health sectors. As to retail, the Government has included retail activities among those that can access the support for digital transformation, *i.e.*, an incentive aimed at encouraging the technological and digital transformation of the production processes of micro, small and medium-sized enterprises.

As regards AI, the Agency for Digital Italy (“AgID”) – the technical agency of the Presidency of the Council of Ministers – has established an AI Task Force which has published a *White Paper on AI at the service of the citizen* analysing the effects of AI tools on the state-citizen relationship and giving recommendations on the use of AI in the public sector. Moreover, the Ministry of Economic Development (“MISE”) published the “AI National Strategy”, based on proposals of a group of experts, which have been under public consultation – the publication of the final text is pending. In addition, the MISE launched the idea of “I3A”, an Italian Institute for AI to connect research and technology transfer. Furthermore, the Ministry for Technological Innovation and Digital Transition has launched the Italian version of the online course Elements of AI, a free introduction to AI for everyone, as well as dedicated workshops. On this side, in 2020, the Garante published the findings of a joint sector inquiry into the field of Big Data, carried out jointly with the Italian Authority for Communications (*Autorità per le*

Garanzie nelle Comunicazioni – “AgCom”) and the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato* – “AGCM”), assessing to what extent GDPR may help handling data protection concerns raised by Big Data. The Garante also published a page on its website dedicated to AI which is constantly updated, and has shown a strong interest in the subject, for example by organising and taking part in online conferences.

Concerning the fintech sector, at the European level, the Directive (EU) 2015/2366 on payment services in the internal market (“PSD2”, implemented in Italy by the Legislative Decree No. 218/2017), required payment institutions to set enhanced authentication means aimed at further protecting users’ accounts and payment cards in case of fraud or unauthorised use. At the national level, a regulatory sandbox has been launched to stimulate the innovation of services and products in the financial, credit, insurance and regulated markets sectors through new technologies, such as AI.

With respect to digital health, the Garante has issued several opinions both to clarify the legal basis for the processing of health data, especially in the context of telemedicine (which is now officially a part of the National Healthcare Service following the approval of the “National guidelines for the provision of telemedicine services” by the State-Regions Conference), and to provide guidance on the security measures to be implemented when sending the dematerialised memorandum of the electronic prescription. The Garante also addressed the processing of health data in the calls for tenders underlining the importance of the governance, the data protection by design and by default, and the security measures. Furthermore, the Garante updated the Frequently Asked Questions on the electronic health record and on online reports to clarify the impact of the amended legal framework under a data protection perspective.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The NIS Decree (Legislative Decree No. 65/2018) implemented the NIS Directive (Directive (EU) 2016/1148) on security of network and information systems (jointly the “NIS Framework”). The NIS Decree sets forth security and notification requirements for operators of essential services (“OES”), identified as such by the Ministry of Economy and Finance, and for Digital Service Providers (“DSP”), *i.e.* online marketplaces, online search engines and cloud services. Concerning the latter, the obligations set out in the NIS Framework do not apply to small enterprises.

Under the NIS Framework, both OES and DSP must: (i) take appropriate and proportionate technical and organisational measures to manage the risks; (ii) prevent and minimise the impact of incidents affecting the security of the network and information systems; and (iii) notify, without undue delay, incidents having a significant impact on the continuity and provision of the service and shall also inform the competent national NIS authority of such incidents.

Further specification of the elements to be taken into account by DSP for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an incident has a substantial impact, are set out in Regulation (EU) 2018/151, which specified the elements to be taken into account by DSP for managing the network security risks and the parameters for determining whether an incident has a substantial impact. Against this backdrop, Regulation 2019/881 (known as the “EU Cybersecurity Act”) came into

force on 27 June 2019 strengthening the European Union Agency for Cybersecurity (“ENISA”) mandate and establishing an EU cybersecurity certification framework. Specific decrees implementing EU Cybersecurity Act will be issued.

However, since the Commission has submitted a proposal to replace the NIS Directive, the NIS Decree will probably be amended in the future to implement such changes. In addition, e-commerce businesses must comply with the provisions of the GDPR, which includes integrity and confidentiality of the personal data among the fundamental principles relating to the processing of personal data. In this respect, Article 32 of the GDPR requires the controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Moreover, the GDPR states that in case of data breach, the controller shall, without undue delay, notify it to the competent supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If a high risk is likely to occur, the controller shall communicate the data breach also to the data subject, without undue delay.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Cybersecurity is one of the main topics in current political and legislative debate in Italy. Among the main initiatives undertaken to address the issue: (i) the Decree of the President of the Council of Ministers of 17 February 2017, a programmatic document aimed at improving the further development of cyber national architecture; (ii) the implementation of the NIS Directive by means of the NIS Decree, as defined above; and (iii) the Law Decree No. 105/2019, establishing urgent provisions regarding the perimeter of national cybersecurity. Furthermore, provisions aimed at strengthening and developing cybersecurity are included in the draft of the National Recovery and Resilience Plan, which is the investment programme that Italy must submit to the European Commission under the Next Generation EU, the tool to respond to the pandemic crisis caused by Covid-19.

Furthermore, specific provisions govern cybersecurity by businesses operating in certain sectors. For instance, providers of electronic communication services are subject to rules aimed at ensuring the security of the networks, both under the data protection legislation and the electronic communication services legislation. Namely, specific measures are provided by Article 16-*bis* of Legislative Decree No. 259/2003 and the relating implementing provisions issued by the Ministry of Economic Development, and by Article 132-*ter* of the IDP Code. For instance, providers of publicly accessible electronic communications services must implement a security policy and have notification duties in certain circumstances.

Another sector for which specific cybersecurity rules apply is the banking sector. Indeed, the Garante issued general resolutions regulating, for instance, the traceability of the processing of personal data, the retention of inquiry logs, the implementation of alerts and the periodic internal audits (see, for instance, the General Prescriptions on the Sharing of Personal Information in the Banking Context and on the Traceability of Banking Transactions, of 12 May 2011, as specified by the clarifications provided by Resolution of 18 July 2013); while the security measures for payment services in the internal market are provided by the PSD2 and the relating national implementing provisions. Moreover, specific IT requirements are provided by the competent regulatory authorities. For instance, the Bank of Italy (“BoI”) addressed the outsourcing of ICT

resources and services by banks, and reaffirmed its commitment to doing so also in light of new cyber risks arising from the accelerated digitalisation process dictated by the Covid-19 outbreak. Also, cybersecurity in the healthcare sector has been recently addressed by the ENISA, which, in February 2020, issued a set of tools and good practices to guarantee the security of personal data processed in the procurement by hospitals, and in January 2021 issued a new report to help healthcare organisations securely adopt cloud services and prepare for cybersecurity challenges.

The enforcement of the data protection provisions set by the GDPR and the national rules is in the hands of the Garante. As regards the regulatory framework, sectoral authorities are responsible for the correct enforcement of the relevant regulations, such as the BoI for the provisions on financial institutions, the Superior Institute of Communication and Information Technology for those on providers of electronic communication services, *etc.*

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In Italy, e-commerce has started to develop relatively late compared to other European countries. At the beginning of the 2000s, e-commerce concerned mainly services and the total income amounted at roughly EUR 1 million (see report of the Italian eCommerce B2c Observatory in cooperation with the University Politecnico of Milan and Netcomm, October 2020).

Only in 2010 did e-commerce start to also involve the sale of products, and in the following 10 years it has developed a lot, by registering in 2020 EUR 30.6 billion revenues, immediately after the UK, Germany and France.

Notwithstanding, in 2020, the percentage of e-commerce penetration on total retail was nearby 8%, thus most consumers still prefer to shop in store.

Although Italian consumers continue to be attached to the use of cash, it is quite clear that this habit is steadily declining. In this regard, statistics show that consumers are quite receptive towards new technologies as they are increasingly resorting to smartphones to buy online. Indeed, in 2020, the total value of purchases from smartphones accounted for 51% of total e-commerce, while in 2019 it was roughly 40%.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Although Italian consumers’ behaviours have historically been (and still are) more inclined towards a cash-friendly attitude, a new trend – more open to cashless, paperless and home banking means – has gained pace in recent years and has been emphasised by the Covid-19 pandemic, as noted by the BoI (see: Payment System in Italy, Statistical Survey at September 2020 – of 23 October 2020, available on the BoI’s website).

As to payment transactions specifically, paperless means (including debit cards) saw a significant increase between 2018 and 2019, in terms of both number of transactions and relevant amounts. While the typical paper-based means, such as banking and cashier checks, both declined correspondingly in the same period.

Consistently with the above, locally active debit, credit and pre-paid cards moved respectively from 45.7 to 57.2 million, from 13.1 to 15.4 million, and from 19.8 to 28.9 million in units, between 2013 and 2019. Debit cards seem then to have experienced the most remarkable increase, now covering almost all Italian bank account holders.

At the same time, home banking services flourished by growing their client-base (both corporate and retail) from 33.9 million to about 58 million in customers, between 2013 and 2019.

All of the BoI's data above suggest that a trend towards a cashless payment culture by Italian customers has consolidated in recent years, and it is expected to move forward in the years to come.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

According to statistics, in 2020, Italian digital exports of consumer goods reached a value of EUR 13.5 billion (+14%), thus accounting for 9% of total consumer goods exports (it was 7% in 2019) and 3% of total exports (2.5% in 2019). Therefore, almost all sales by Italian e-commerce are directed towards national consumers. In this regard, when Italian e-commerce sellers intend to target foreign consumers, they generally put their products on international e-commerce platforms which allow them to reach foreign consumers (e.g., eBay and Amazon).

Notwithstanding, among Italian e-commerce platforms, there are some outstanding and upstream examples which sell a lot in other jurisdictions. It seems that they attract foreign buyers as they are very specialised in a specific market sector (e.g., clothing design and food & grocery), and they commercialise this excellence in terms of quality of products.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Recalling our previous answer to question 4.3, Italian e-commerce firms mainly target national consumers, with relevant exceptions as mentioned before (i.e. fashion, food & grocery and in the last year furniture, the latter favoured by the pandemic emergency).

Further, 56% of companies use digital channels to sell products abroad – especially in Germany (34.7%), France (26.8%), the UK (26%), the US (25.4%), Spain (18%) and China (11.4%) – and 62% of these do so in more than one market, even if nearly 75% export products online for less than 20% of their turnover.

However, Italian e-commerce websites seem not to have overcome language barriers yet: in fact, in 2019 less than 10% of home e-commerce sellers provided their platforms with a second language, different from Italian. Equally, in less than 5% of cases it is possible to pay in a currency other than Euros.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

decided to invest in advancing and performing better user experience (e.g., by means of presentation style and graphical components) in such a way to attract more consumers and offer them a greater purchasing experience, leading them to recommend their website. In fact, surveys underline that most Italian consumers resort to online reviews in order to decide where to buy. Alongside management of reviews, Italian online traders aim at developing eco-friendly products and packages, as Italian consumers are more inclined to buy when the online brand is eco-sustainable. However, only few consumers choose to pay for the so-called "green" delivery, designed to offset the carbon emissions released during the delivery process.

Specialised websites also recommend national e-commerce traders, above all: (i) to include descriptions and photographs of quality products; (ii) to organise and structure the e-commerce pages in a rational way; (iii) to display logos; and (iv) to enhance ease of navigation. Furthermore, Italian e-consumers are used to approach e-commerce sellers through social media platforms (above all, Facebook and Instagram). Thus, e-commerce traders appear especially keen on improving their business profile on social networks.

Lastly, in relation to the implementation of AI software on e-commerce websites, e-commerce traders are getting more and more interested in exploiting this new technology.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The Covid-19 pandemic and the related lockdown measures have generated an unprecedented digital evolution in the lifestyle of Italians, thus modifying their purchasing behaviour. Indeed, the frequency of e-commerce purchases has increased (+79%), home delivery has remained the preferred method of receiving products by over 93% of users and cash is increasingly losing ground in favour of digital payments (see report of the Italian eCommerce B2c Observatory in cooperation with the University Politecnico di Milan and Netcomm, October 2020).

As a matter of fact, opposed to the most significant growth ever in online purchases of products (+ EUR 5.5 billion in 12 months), services halve their value (-47%) due to the crisis that hits, first of all, the tourism and the transportation sector.

As for products, in absolute value, there are three sectors that contributed most to the growth. To be more specific, of the EUR 5.5 billion total increase, EUR 1.1 billion comes from food & grocery, EUR 1 billion from computers and electronics and EUR 700 million from clothing.

As for services, the tourism and transportation sector suffered a major setback. Indeed, the spread of Covid-19 and the related lockdown measures have severely damaged these sectors, which met a decrease of 56% and plunged to a value of EUR 4.8 billion. The situation in ticketing is particularly critical too: government regulations have in fact banned live events (concerts, exhibitions, etc.) for months and to date there are still significant limitations. Instead, online purchases in insurance are bucking the trend, registering a growth of 6%, amounting now to EUR 1.6 billion.

Further, during the lockdown, the usage of smartphones for e-commerce purchases has greatly increased. In absolute value, B2C e-commerce from smartphones is close to EUR 15.7 billion, +22% compared to 2019. In short, 51% of B2C e-commerce purchases is made through such devices.

Since 2019, more and more national e-commerce traders have

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Within the Italian jurisdiction, there are different processes for online brand enforcement, depending on the type of infringement.

A first example is the sale of counterfeit products and the unauthorised use of a brand and distinctive signs on online marketplaces (e.g. Amazon). These marketplaces allow rightsholders to enforce online brand protection through specific procedures (such as reporting and notice and take down tools). By filing online forms, rightsholders may submit to the relevant marketplace requests to remove counterfeit products from the marketplace itself. Also, the same conduct even on third-party websites may amount to unfair commercial practices when they mislead users as to the origin of the products and/or qualification of the seller. In this case, rightsholders may report the online brand infringement to the AGCM, asking for a takedown order against the infringing website.

Online infringement can also occur when a brand is unlawfully used in an identical or similar third-party domain name. In this case, rightsholders may start: (i) a challenge procedure before the Italian Domain Names Registry (which manages ccTLD .it domain names); and subsequently (ii) a re-assignment procedure before a provider of services of dispute resolution, specifically aimed to re-allocate the challenged domain name.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Within the Italian jurisdiction, online brand enforcement processes described in the answer to question 5.1 may be restricted.

In relation to notice and take down procedures, brand owners have to provide evidence that they are the rightsholders of the infringed brand in order to obtain takedown. Moreover, they have to provide online marketplaces with a number of details concerning their claim (e.g. specifying the nature of the infringement).

In relation to the challenge procedure before the Italian Domain Names Registry, applicants have to prove (*inter alia*) that they are the rightsholders of the infringed brand. Also, applicants have to provide a description of the harm caused by the infringement (e.g. the likeliness of confusion between the challenged domain name and applicants' trademarks or other distinctive signs). In addition, to obtain re-assignment of the challenged domain name, applicants have to prove that the registrant of the challenged domain name does not hold title to it, and that it has registered and maintained the challenged domain name in bad faith.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The security standards are a main issue when contracting with third party-owned data centres or cloud providers. The latter should guarantee the implementation of technical and organisational measures aimed at ensuring, for example, encryption,

regular backups and recovery and restoration procedures. Along with the security measures, it is important to evaluate the allocation of responsibilities between the third-party providers and the service users. Further remarks concern the potential intermingling of personal data of different service users stored in the same third-party provider's – physical or cloud – premises (to be avoided especially if sensitive data are involved in the processing). In addition, the procedures put in place by the third party must ensure the complete deletion of the personal data in case of erasure.

Other concerns heightened by the significant increase in the use of cloud service providers (both by businesses and by consumers) regard the risk that such providers might (illegally) process the service user's personal data for further purposes other than those established by the service user himself/herself (generally speaking, the user is the controller and the provider is the processor) and that the service user's personal data might be associated to other personal data already processed by the providers. In light of the above, it is crucial to appoint the service provider as a processor (save in cases where the actual processing of the personal data requires a different qualification) and to properly evaluate the content of the related data processing agreement, even if, when considering dominant cloud service providers, the asymmetry of bargaining power is a difficult obstacle to overcome.

Regarding specific areas such as finance and the public sector, there are *ad hoc* requirements to be met when using a cloud service. When the processing via cloud services concerns activities that are critical or important to a financial institution's operations, prior approval by the regulator and specific risk management and audit requirements apply. By way of example, banks must perform additional checks on cloud providers, which include identifying where relevant data centres are located; in addition, the European Securities and Markets Authority ("ESMA") published guidelines on outsourcing cloud services in banking and insurance industry. With respect to cloud service providers who wish to provide their services to public administrations, they must undergo a qualification process set forth by AgID, must disclose the location of their own relevant data centres and/or cloud infrastructures, and must also comply with additional requirements set out by specific regulation to be adopted by AgID.

Furthermore, guidelines and recommendations on the use of third-party cloud services in the e-health sector have been published by local authorities (including the Garante) and ENISA, notably regarding the Electronic Health Record.

As a final remark, special powers attributed to the Government to veto or impose conditions on certain resolutions or transactions made by foreign investors relating to Italian companies have been extended to also encompass data centres.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

The location of the servers is not specifically addressed by Italian law. In principle, under Articles 44 *et seq.* of the GDPR, transfers of personal data to non-EEA countries are subject to restrictions (while the transfer of personal data is generally permitted within the EEA). In particular, a transfer of data shall be allowed in the following circumstances: (i) the recipient country's legal system has been subject to an adequacy decision of the EU Commission; (ii) the data controller adopted appropriate safeguards (e.g. standard contractual clauses or binding corporate rules), provided that enforceable data subject rights and effective legal remedies for data subjects are available; or (iii)

other specific situations occur, such as: the explicit consent of the data subject or the transfer is necessary to perform a contract between the data subject and the controller or to perform pre-contractual measures taken at the data subject's request.

Further, additional suggestions are included in the Garante's practical guidelines for controllers using the cloud. Such guidelines point out that controllers must take into consideration whether data is stored abroad and must ensure that data is kept accessible and confidential by the cloud service provider. In addition, to ensure security of data, controllers shall not only focus on how data is stored, but also on how it is transmitted, for instance by using encryption techniques.

As to the public sector, a "national cloud" intended for all public administrations will be implemented with the aim to develop a highly reliable infrastructure located in the Italian territory for the rationalisation and consolidation of the Information Processing Centres. Furthermore, central and local public administrations shall migrate their Information Processing Centres and relating IT services towards national cloud (or other infrastructures provided by law), where these IT services do not meet the minimum security and reliability requirements as set out by a specific AgID regulation (yet to be approved).

Finally, the emergency legislation has temporarily introduced simplified procedures for public administrations to acquire IT goods and services preferably based on SaaS cloud model from providers who must necessarily retain, process and manage data within the Italian territory. This possibility is available only where such localisation measures are justified on grounds of public security.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

In Italy, both private and governmental actors are increasing their efforts towards digitalisation. On the one hand, larger private companies are investing in digital solutions in relation to a huge variety of situations: among others, to automate trade processes. On the other hand, public administrations (e.g. the MISE) have started to provide financial grants to projects specifically addressed to SMEs, in support of their digitalisation.

All public sectors have been involved in a process of digitalisation since the 90s, when they started to modernise their infrastructures and processes, with the purpose of enhancing efficiency and reducing costs and bureaucratic hurdles. In 2012, a considerable incentive in this direction has come alongside the "E-government Plan", specifically directed to digitalise public administration.

In this context, during the last years, the Italian Customs Agency started a project aimed at digitalising procedures concerning cross-border trade. Just to quote a few examples, we can mention the "fast corridor" procedure, using new digital technologies to allow the immediate forwarding of goods and customs clearance, replacing the "document monitoring" with a telematic dialogue between all actors of the logistics chain. Another example is the "interoperability model for the digitisation of customs procedures in ports", addressing technical aspects for the development of interoperability services between the AIDA customs information system and the port information systems (Port Community System), with the aim of making the operational procedures more homogeneous in ports and optimising the port logistics cycle. Moreover, it is planned to

resort to IoT technologies to monitor goods entering or leaving the national customs territory and to send and receive electronically the documentation needed in order to import and/or export specific goods (e.g. dual use goods).

In addition, the Italian Customs Agency has set up Permanent Working Groups composed of representatives of public institutions and relevant private stakeholders to share strategies, development plans in relation to the evolution of the EU and national regulatory trade framework.

Italy is therefore committed towards digitalisation and relevant stakeholders and public authorities are leading Italy towards a 4.0 national customs system.

In addition, in March 2021, the Customs and Monopoly Agency organised the "EUR 1 - full digital" open hearing dedicated to the new procedures for requesting and issuing EUR 1, A.TR and EURMED certificates. During the hearing, the Customs Agency confirmed the availability of the request and issue functions of the first full digital EUR 1 certificate for goods destined, for now, for the Swiss Confederation and illustrated the benefits deriving from the complete dematerialisation of the document.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Notwithstanding Italian trade and customs are firmly moving towards digitalisation, there are unquestionable barriers hindering this process to some extent. On the one hand, certain obstacles depend on the nature of goods involved in trade and customs processes since they are tangible goods, which need to be materially inspected by "physical" operators. Thus, what can be digitalised are mainly the customs logistic and administrative procedures (e.g. port tracking), but for the time being, it is difficult to envisage some digitalisation of material inspections.

On the other hand, there are obstacles that can be overcome, but they require relevant efforts to succeed. Leaving aside the undeniable significant financial burden that these projects entail, public authorities need to engage staff with a special expertise relevant to these specific activities.

Additionally, there are differences and peculiarities amongst customs that need to be taken into account. In this respect, a standardised approach could not be suitable for every situation, while a more tailored approach would be necessary in order to reach full digitalisation.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Italian tax law foresees different tax incentives for digital business companies.

The Patent Box regime is a tax bonus introduced in order to improve the development of intellectual property, granting tax benefits to resident and non-resident taxpayers carrying out research and development activities. Under this regime, taxpayers shall be entitled to exclude up to 50% of their income, for purposes of the corporate taxes (IRES and IRAP), deriving from the direct exploitation of intangibles or from licensing of the IP, such as royalties earned by the taxpayer, net of all IP-related costs.

Tax credits for R&D investment and technology investment. The Italian Government recognises a tax credit amount of 20% of the eligible expenses, up to a maximum of EUR 4 million. For technological innovation activities, the tax credit is recognised separately at a 10% rate of the relevant basis of calculation, up to a maximum of EUR 2 million. For the achievement of an ecological transition or digital innovation 4.0 objective, the credit measure increases to 15%.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The most relevant disputes between digital businesses and tax authorities in Italy concern the permanent establishment (“PE”) issue and the potential application of a withholding tax on certain types of digital cross-border transactions.

The constant increase in the potential of digital technologies, and the reduced need in many cases for extensive physical presence in order to carry on business in a jurisdiction, raise questions about the qualification of a PE in a country. Over the last year, the Revenue Office has challenged, under such circumstances, the presence in Italy of a permanent establishment of a number of firms carrying out business transactions over the Internet.

The development of new digital products or means of delivering services creates uncertainties in relation to the proper qualification of payments made by Italian residents for the digital service/intangibles provided by a foreign provider. In some cases, the Italian Revenue Agency challenges the application of withholding tax on certain payments made (including royalties).

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

Both from a legal and practical perspective, businesses which decide to recruit people in Italy should be focused on the way in which the working activities shall be carried out to match the business needs.

Companies should enter into employment agreements if the hired workers are part of the company’s organisation, carrying out their duties with continuity in the workplace, during specific working time and following specific instructions.

The standard model of employment relationship is the permanent employment agreement, usually governed by Italian law and by the applicable national collective bargaining agreement, whereas fixed-term employment agreements are permitted only within certain law restrictions (*i.e.* maximum duration, certain percentage of fixed-term employees, existence of specific reasons).

If business needs allow people to carry out services in autonomy and with maximum flexibility (*i.e.* no working time, no workplace and no specific instructions), companies may execute consultancy agreements.

In conclusion, indeed any model of relationship has specific advantages and disadvantages; however, when deciding on the best way of resourcing work in Italy, in order to avoid possible risk of claims, businesses must execute the model of contract

that better matches the way to perform activities/services with the effective business needs.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation’s physical premises?

Italian law provides two different models to work away from a company’s physical premises.

The first one is the so-called “smart working” (*i.e.* flexible working modality based on which, even in presence of company physical premises, employees spend part of their working time out of the office, working from home or from different places). The other is the so-called “telework” (*i.e.* working activities entirely carried out from a home working station without company physical premises). Specific provisions – within the employment agreement, in case of telework, or in a separate agreement, in case of smart working – must be provided by the parties to regulate these modalities to work away from the company’s physical premises.

Generally speaking, smartworkers and teleworkers are subject to the same treatment as other employees, but employers must consider key topics to manage the above-mentioned models of work: (i) health and safety (ensuring that employees work in compliance with the relevant law measures and provisions); and (ii) data protection (avoiding remote monitoring of employees’ working activity).

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Smart working has now become part of everyday working life and it is destined to remain so: at the end of the emergency, it is estimated that Italian agile workers, who will work at least in part remotely, will be around a total of 5.35 million. To adapt to this “new normal” of work, 70% of large companies will increase the days of remote work, bringing them on average from one to 2.7 days per week, one in two will change the physical spaces. Furthermore, article 90, paragraph 4, of Decree Law 34/2020 provides that until April 30, 2021, smart working can be applied by private employers to any employment relationship even in the absence of the individual agreement provided for by the regulations in force. Such provision will likely be extended and it is expected that this type of work will be adopted more frequently, becoming the new normal.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Recalling the previous answer to question 7.1, the Italian public administration (in particular, the MISE) is specifically oriented towards full digitalisation, not only of public administrations themselves but also of private enterprises. In this regard, among others, companies interested in investing in their digitalisation can benefit from public funds and financial subsidies for “going digital”.

Notwithstanding the above, all legal processes or administrative procedures are made more difficult or slowed down by a binding and excessive bureaucracy.

In addition, the digital economy is still not perceived by all economic operators as a strategic factor. Indeed, Italy still ranks

24th out of 28 EU Member States as it emerges from European Commission Digital Economy and Society Index (DESI) 2019, and although it is making progress in connectivity and digital public services and is improving its fast broadband coverage and ultrafast connectivity, as well as the assignments of 5G spectrum, three out of 10 people are not regular internet users yet and more than half of the population still lack basic digital skills. This is also reflected in low use of online services, with the consequence that only a few Italian SMEs are selling online compared to other EU countries.

Finally, full digitalisation, e.g. through iCloud technologies, implies compliance with European and national data protection regulations, which are particularly stringent in many respects.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

In addition to advantages in terms of employment law and tax regulation recalled above, from an economic standpoint, a digital business can benefit from wide cross-border or even globalised competitive markets compared to companies which have not embodied yet the “digital shift”.

This is particularly true in Italy, where digitalisation of private companies and, more specifically, online trade is still at the beginning of its development. Thus, economic operators, especially SMEs, running a digital business and/or an online trade could be able to significantly overcome national non-digital competitors (in this respect, see also the answers to questions 4.1 and 7.1 above).

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

Due to the pandemic situation, Italy’s e-commerce activity increased exponentially during the last year. Ready acceptance of emerging payment methods is helping Italy to make a dynamic and fast-growing sector.

On 25 March 2020, the European Banking Authority published its ‘Statement on consumer and payment issues in light of COVID-19’, in which it encouraged retailers to ‘facilitate consumers’ ability to make payments without the need for physical contact’. In May, the Italian National Institute for Insurance against Accidents at Work (INAIL) published a technical document stating that “*it is appropriate to privilege contactless electronic payments*”. As a consequence, many digital payments providers are launching new products and services aimed at encouraging the use of digital payments. The latter have also been encouraged by the Italian Government with several initiatives, amongst which the so-called “cashback” refund provided by the Italian State. The Government cashback initiative started on an experimental basis on December 1, 2020 and allow consumers who sign up to get a cash refund on a percentage of the transactions made using electronic money.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

From a financial supervision standpoint, the online payment sector is subject to the regulatory power of the BoI, competent for supervising both the retail and wholesale markets and takes part as a national authority to the Single Euro Payment Area (“SEPA”).

Along with monitoring compliance with rules of conducts, transparency, sound and prudent management and anti-money laundering rules by the payment service providers, the BoI is also granted power to oversee the local payment system infrastructures in order to ensure proper risk management measures (e.g. ICT, business continuity and disaster recovery) are implemented, also in relation to online transactions. Specific awareness on cyber-related risks associated with online transactions is constantly raised by the BoI (see among others the BoI’s press release on an Action Plan on Cyber Resilience Oversight Expectations on Financial Markets Infrastructures of 16 January 2020). The continuing Covid-19 pandemic has also brought to the attention of the BoI specific risks associated with the massive use of online platform, in relation to both payment infrastructures’ stress and money laundering (see the BoI’s press release on Prevention of Financial Crimes Associated with the Covid-19 Emergency of 11 February 2021).

The regulatory framework has recently been reviewed due to the PSD2 and relevant implementing regulatory and technical standards, being enacted locally starting from the end of 2017. The PSD2 brought certain new business models and third-party services particularly relevant to the online payment transactions (notably Payment Initiation and Payment Account Information Providers) into the regulatory scope of the BoI who is keen on ensuring those new players have access to clients’ interfaces held by banks and other incumbents, as set out by the EU rules.

The carrying out of online payments is mainly governed by the following acts and regulations, as amended and supplemented by the PSD2 implementing rules:

- the Italian Banking Act (Legislative Decree No. 385/1993), which sets out the overall requirements for providing banking/payment-related services, including those online;
- Legislative Decree No. 141/2010, which sets out specific rules on consumer financing and payment services tied-in with other commercial services and activities, and on distributors of payment services; and
- the BoI’s Regulation of 29 July 2009, on transparency duties to customers (the “Transparency Regulation”).

EU payment providers who wish to carry out business in Italy are granted passporting rights under the Italian Financial Act, under both establishment and freedom of services, and are enrolled with the relevant BoI’s registers for EU payment institutions, pursuant to the Home Member State Authorisation principle.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The payment sector is highly regulated in Italy and local competent authorities, including courts and the BoI, normally take a consumer-friendly approach.

As to compliance issues, consistent with the above, the Transparency Regulation is key when it comes to ensuring that information on online services, and related costs, are clearly disclosed and clients are being treated fairly. In that vein, specific attention is generally drawn by the BoI to the following: (i) signing on payment services contracts by both the provider and client (also via recognised e-signatures) and handing over of all contract documentation to the latter; (ii) proper and timely complaints handling; and (iii) avoiding the bundling of unrelated services. Data protection is also at the core of any compliance governance set by online service providers.

Also, the BoI is increasingly looking at the online payment sectors in order to monitor and detect consumer frauds, money laundering and terrorism financing risks.



Irene Picciano joined Portolano Cavallo in 2019 and has 20 years of experience in EU and competition law and in regulatory and compliance. She has assisted and represented multinational clients in cartel and abuse of dominance cases before national and EU authorities and courts, dawn-raid investigations, merger control, competition compliance and restrictive agreements. Over the years she also accrued an extensive experience on complex product, trade and corporate compliance issues in many industry sectors amongst which are fashion/luxury, life sciences, automotive, food & beverage and consumer goods.

Portolano Cavallo
Piazza Borromeo, 12
Milan 20123
Italy

Tel: +39 02 722341
Email: ipicciano@portolano.it
URL: www.portolano.it



Fabiana Bisceglia joined Portolano Cavallo in 2015, upon being awarded a *cum laude* law degree by LUISS Guido Carli University, first as a trainee and then as attorney-at-law. Her areas of expertise are media, audiovisual regulatory, advertising law, as well as prize promotional activities, consumer protection, unfair commercial practices, e-commerce, privacy and data protection. Fabiana counsels Italian and foreign clients operating in a variety of business sectors. Since 2018, Fabiana has been Professor of Information and Digital Communication Law at the Academy of Arts and New Technologies in Rome.

Portolano Cavallo
Via Rasella 155
00187 Roma
Italy

Tel: +39 06 696661
Email: fbisceglia@portolano.it
URL: www.portolano.it



Donata Cordone joined Portolano Cavallo in 2017. She assists Italian and foreign clients both in court proceedings and extrajudicial settings, in particular in matters of e-commerce, Internet and new technologies, exploitation of digital content, consumer protection, advertising, unfair commercial practices, prize contests, copyright, cinema and audiovisual, intellectual property rights and unfair competition. She is a member of the Global Advertising Lawyers Alliance (GALA).

Portolano Cavallo
Piazza Borromeo, 12
Milan 20123
Italy

Tel: +39 02 722341
Email: dcordone@portolano.it
URL: www.portolano.it



Livia Petrucci began working with the firm in 2018 as an intern, starting her traineeship at Portolano Cavallo in January 2020. She earned her *cum laude* law degree from the University of Trento with a thesis on the safeguarding of personal data that was published as a part of the LawTech Student Paper Series. Livia is a member of the firm's French Desk. Her main areas include privacy, media law, consumer protection, Internet & e-commerce, and new technologies. She is also involved with legal issues related to the Life Sciences industry.

Portolano Cavallo
Piazza Borromeo, 12
Milan 20123
Italy

Tel: +39 02 722341
Email: lpetrucci@portolano.it
URL: www.portolano.it

Portolano Cavallo was founded in 2001 by partners Manuela Cavallo and Francesco Portolano.

Portolano Cavallo provides legal advice to companies operating in complex and evolving sectors; it is a leader in the Digital, Media and Technology, and Life Sciences sectors, in addition to being recognised in the Fashion/Luxury field.

The firm's practice areas range from litigation to M&A and venture capital, from emerging companies to the exploitation and protection of all forms of intellectual property, from employment to data protection, privacy and cyber-security issues, from technology transactions to antitrust and regulatory issues and white-collar crime/investigations.

In all these areas, Portolano Cavallo is recognised by multiple legal Italian and international rankings and awards.

www.portolano.it

P O R T O L A N O
C A V A L L O

Japan

Anderson Mōri & Tomotsune



Ken Kawai



Takashi Nakazaki

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

There are no legal requirements that apply specifically to B2B e-commerce in Japan.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The main legislative instruments relating to e-commerce are the Act on Special Provisions to the Civil Code Concerning Electronic Consumer Contracts and Electronic Acceptance Notice (Act on Special Provisions), the Act on Specified Commercial Transactions (ASCT) and the Act on Regulation of Transmission of Specified Electronic Mail (ARTSEM). The ASCT requires an e-commerce business operator to notify consumers of certain items, such as the cancellation policy, and prohibits an e-commerce business operator from sending junk emails. The ARTSEM also prohibits an e-commerce business operator from sending junk emails. Also, the Consumer Contract Act prohibits an e-commerce business operator from including excessively disadvantageous conditions in its terms of service. Further, some intellectual property laws may be applied to internet-related issues.

The Ministry of Economy, Trade and Industry (METI) has published the Interpretative Guidelines on Electronic Commerce and Information Property Trading on its website. These guidelines have been updated every year or every few years and their coverage has been expanded. The guidelines contain methods for applying provisions of the Civil Code, the Consumer Contract Act, the Act on Special Provisions and the ASCT to e-commerce business circumstances, including instructions for amendment of the terms of service, protection of minors, various issues related to internet auction services and AI speakers. Also, the guidelines cover application of intellectual property laws, including the Copyright Act, the Trademark Act, the Premiums and Representations Act governing advertisement issues, and other internet-related laws, to e-commerce businesses.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The Act on the Protection of Personal Information (APPI) is the main legislative instrument for data protection in Japan. The APPI was amended in 2020. The Amendment, except for certain provisions, will take effect on April 1, 2022. This amendment is a follow-up on the Japanese government's policy to review the legal system every three years, as stipulated by the 2015 amendment to the Act which came into full force on May 30, 2017. The 2020 amendment makes reforms to the Act to strengthen the protection of the rights of principals who may be identified by personal information, as well as the supervisory and enforcement powers of the Personal Information Protection Commission of Japan (PPC). The amendment also aims to promote the utilisation of data in society.

The contents of the Amendment are as follows:

- (1) Reinforces the general obligations of personal information handling business operators to properly handle personal information
 - Expressly stipulates the prohibitions on improper use of personal information.
 - Creates an obligation to report certain personal data leakages to the PPC and notify the affected principals of the same.
- (2) Reinforces the principal's rights concerning retained personal data
 - Grants a principal the right to designate the method of disclosing retained personal data.
 - Creates a right to demand for the suspension of use of personal data when a leak has occurred or "there is a possibility for the principal's rights or just interests to be infringed".
 - Amends the definition of retained personal data.
 - Adds certain new items to the list of information that business operators must disclose concerning retained personal data.
- (3) Reinforces the protection of principals' interests concerning third party provision of personal data
 - Adds certain new items to the list of information that business operators must notify to the PPC upon the provision of personal data to third parties using the "opt-out" method (the "opt-out" method refers to a business operator's provision of a principal's personal data to a third party upon notification of certain information to the PPC and disclosure of the same, without

obtaining the consent of the principal, and on the condition that the business operator will cease such provision upon a request by the principal).

- Prohibits business operators from (i) providing improperly acquired personal data to third parties using the opt-out method, or (ii) providing personal data that has already been provided by the opt-out method to third parties via the opt-out method again;
 - Creates an obligation for business operators to provide certain information on foreign systems for personal information protection to the principal when providing personal data to a third party located in a foreign country.
 - Creates an obligation for business operators to confirm and record certain matters when providing information that is expected to become personal data only when received by the recipient.
 - Creates the principal's right to demand for disclosure of records concerning the provision of personal data to third parties.
 - Adds certain items to the list of information that business operators must disclose upon joint use ("joint use" means sharing and jointly using personal data with third parties upon disclosure or notification to the principal, without obtaining the consent of the principal).
- (4) Introduces a new concept of "pseudonymously processed information" and adds related provisions
Adds a new definition of "pseudonymously processed information", which means information that is processed in a way that prevents an individual from being identified unless the information is collated with other information. In connection with this, the Amendment also stipulates the obligations of business operators that handle such information, and exempts them from the obligation to respond to requests for disclosure or suspension of use, etc. by the principal even if such information falls under the definition of personal data.
- (5) Expands the scope of extraterritorial application
To date, the provisions in the Act subject to extraterritorial application were limited only to certain provisions. The Amendment expands the scope of the extraterritorial application to all the provisions in the Amended Act. The situations and business operators that are subject to the extraterritorial application will also be expanded to broadly cover situations where business operators handle information relating to an individual in connection with the provision of goods or services to persons located in Japan.
- (6) Strengthens the PPC's enforcement power and criminal penalties
Authorises the PPC to disclose the name of business operators that have breached an order made by the PPC. Furthermore, the maximum fine that may be imposed on a legal entity for a breach of a PPC order or the provision or theft of a personal information database, etc. for the purpose of gaining an illicit profit will be raised to JPY 100 million. The maximum limit for some other criminal punishments will also be raised.
- (7) Others
Amends certain provisions concerning accredited personal information protection organisations, and introduces provisions concerning service by the PPC of demands for reports, recommendations, or orders.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Fintech

The Financial Service Agency, the authority governing the financial industry, has issued APPI guidelines specifically for the financial industry. The guidelines contain especially strict regulations. For example, if a financial institution notifies a data subject of the purpose of personal data utilisation, such notification should be in writing. This regulation might be an obstacle to the fintech business in the e-commerce context.

Retail

The Amendment to the APPI will establish newly regulation on collecting and utilizing identifier information such as cookies, and information exchanged on DMPs (Data Management Platforms, which means platforms for the collection and analysis of user data on the internet) that contains identifier information. The Amendment would affect greatly the online marketing and advertisement business in the retail sector.

Artificial intelligence (AI)

If a business operator handling personal data intends to change the purpose of personal data utilisation, the operator must obtain prior consent of the relevant data subject. The purpose of utilisation in the AI business often changes because AI technology enables unexpected uses of personal data. In the e-commerce context, obtaining prior consent from existing customers and users requires extensive costs and time, which may be unrealistic from the commercial viewpoint of an AI business.

Digital health

Healthcare-related personal data is subject to special protection as sensitive data under the APPI. The special protection prohibits entities from obtaining sensitive data without a data subject's prior consent. Also, there are some security guidelines for healthcare-related personal data in Japan, and the requirements specified by these guidelines might be an obstacle to the digital healthcare business in Japan.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Fintech / Retail / AI

The Diet of Japan enacted a bill to create "super cities" where artificial intelligence, big data and other technologies are utilised to resolve social problems in 2020. The revision stipulates procedures to change regulations in various fields at a stroke to create such smart cities. In such cities, data-linking platforms to collect and organise various kinds of data from administrative organisations and companies in a cross-sectoral way will be established for autonomous driving, cashless payments, telemedicine and other services to be introduced there. 31 municipalities submitted applications to be selected as "super cities" and some of them will be reviewed by the government.

Digital health

The Next-Generation Medical Infrastructure Act (*Jisedai-iryo-keiban-ho*) was enacted in 2017 and has been in effect since 2019. The Act clarified that de-identified clinical records could be used for research, as far as that data is collected and processed

by a government-approved database manager and processor. Only two groups (each group consists of one manager and one processor) have so far been approved under the Act.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The Basic Act on Cybersecurity, enacted in November 2014, while not specific to e-commerce businesses, provides a basic legal framework for cybersecurity. Among other things, this Act provides a basic framework on the responsibilities and policies of the national and local governments for the enhancement of cybersecurity. Furthermore, the Act requires critical information infrastructure operators (e.g., financial institutions, railroad operators, airlines and other transportation operators, as well as utility providers) and networks operators (e.g., telecommunications network operators) to enhance cybersecurity on a voluntary and proactive basis, and to cooperate with the national and local governments in taking measures for the enhancement of cybersecurity.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

There is no legislation specific to cybersecurity other than the Basic Act on Cybersecurity.

There are, however, several laws and regulations in Japan that can be used to tackle cyber-crimes, including, among others, the Unfair Competition Prevention Act, the Unauthorised Computer Access Prevention Act, the Personal Information Protection Act and the Penal Code.

In addition, regulatory and supervisory guidelines requiring cybersecurity management have also been issued, such as in respect of the financial sector. For example, the Financial Services Agency of Japan (JFSA), the competent regulator of financial institutions and fintech companies, has issued inspection manuals and supervisory guidelines that provide points of focus in connection with cybersecurity risk management.

The JFSA refers to the “FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions” (FISC Guidelines), published by the Center for Financial Industry Information Systems (FISC), when inspecting and monitoring banks, financial instruments business operators, crypto asset exchange service providers and other types of financial institutions.

The FISC Guidelines serve as *de facto* standard guidelines for the introduction and operation of financial information systems. These guidelines address, among others, prevention of system failures in financial institutions, minimisation of the impact of system failures, and safety measures for early recovery from such failures.

In recent years, there have been several cases in Japan of large-scale unauthorised leakage of customer assets resulting from cyber-attacks on crypto asset exchange service providers. Accordingly, the JFSA has imposed strict cybersecurity management standards, particularly in respect of crypto asset exchange service providers.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In Japan, e-commerce service providers such as Rakuten, Yahoo! and Amazon began to take off in the late 1990s as a result of wider use of the internet. E-commerce services initially took the form of B2C transactions. With the proliferation of smartphones and SNS, however, various e-commerce sites were gradually established, including those offering C2C-type services, such as Mercari, a marketplace that enables the sale and purchase of used goods between individuals, and provides experiential services. Although the use of e-commerce services is common in Japan, cash is still the most common method of settlement for the purchase of goods and services in physical stores. Despite that, and as described under question 4.2 below, cashless settlement is rapidly gaining prevalence as a result of government-introduced measures in Japan.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Cash is still the most common medium of exchange in Japan. The most popular methods of payment after cash are credit cards and prepaid instruments. It has been observed that cashless payments are significantly less prevalent in Japan than in other major economies.

It is, however, noteworthy that since 2018 an increasing number of companies have entered into or have expanded their businesses into the mobile payment market. For example, many companies have launched QR code payment services (such as Pay Pay, Line Pay and the like) between 2018 and 2019. As many of these companies provide their customers with incentives to use their QR code payment services, this sector of the market has become highly competitive.

To encourage the use of cashless payments and to mitigate the adverse effects of the consumption tax hike in October 2019, the Japanese government has also introduced a 5% reward point rebate programme. Those using certain cashless payment methods at qualifying stores will be eligible for rebates under this programme from October 2019 to June 2020.

With more people avoiding physical cash amid the COVID-19 pandemic, digital payments are becoming more popular in Japan.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

In our view, the answer is unfortunately “no”.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

According to a survey published by the Japan External Trade Organization (JETRO) in February 2021, 33.3% of the

respondents use e-commerce, of which 65.0% use it for overseas sales. 45.5% of these companies have made outbound sales from Japan to other countries. The largest destination of these outbound sales is China, and most of the sales are to Asian countries other than the United States. Accordingly, language does not appear to be a major barrier.

With that said, a negligible number of Japanese e-commerce platform operators have achieved significant success overseas.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Japanese consumers seem to prefer web-interfaces that are both user-friendly and aesthetically pleasing.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Digital payments are becoming more popular in Japan, with more people avoiding physical cash amid the COVID-19 pandemic. According to a survey conducted by Dentsu Inc, the largest advertising agency in Japan, nearly half of the consumers increased use of cashless payments after declaration of COVID-19 state of emergency in March 2020.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Online piracy

Typically, enforcement would begin by obtaining the postal address of an online brand infringer and sending a cease-and-desist letter requesting that the infringer cease its infringement and pay damages caused by the infringement. If the infringer did not cease its infringement, the next step would be to file an action in court. Civil remedies designed for intellectual property do not include search orders and freezing injunctions.

Although an injunction that prevents the infringer from using the intellectual property is possible, freezing injunctions as to the infringer's assets are not provided in relation to IP infringement. Provisional attachment under the Civil Preservation Act and attachment under the Civil Execution Act are available for monetary claims, including a claim for compensation of damages based on IP infringement, both of which may be similar to freezing injunctions.

Furthermore, many infringers hide their real name and postal address in an effort to avoid receiving a cease-and-desist letter from an IP rights owner or a court. In that case, it would be necessary to obtain the infringer's name and postal address from an internet service provider. The process to obtain that information may take a few weeks to several months.

Domain names

The owner of a trademark may challenge a registered 'pirate' domain name. However, the owner will often seek dispute resolution through the Japan Intellectual Property Arbitration Centre (JIPAC), certified by the JPNIC, regarding .jp domain names under the JP-Dispute Resolution Policy (JP-DRP). In these dispute resolution proceedings, the owner of the

trademark may demand cancellation of the registered domain name or transfer of the domain name to the owner.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

There are no specific restrictions that have an impact on online brand enforcement.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Generally, there are no legal considerations or risks when contracting with third party-owned data centres or cloud providers. As to security considerations, the Ministry of Economy, Trade and Industry (METI) has published the Information Security Management Guidelines for the Use of Cloud Services. The guidelines include access control, back-up, and employee management issues.

Hospitals and clinics in Japan are required to store patients' data on a cloud server that is subject to Japanese laws, such as BCP (business continuity plan) measures.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Generally, there are no requirements for servers/data centres to be located in Japan.

This is the case even in the area of financial services, where regulations tend to be more stringent than for other industries. Moreover, financial institutions are not prohibited from using cloud services. As stated in question 3.2 above, however, financial institutions are required to meet the standards stipulated in laws and guidelines relating to cybersecurity, including the FISC Guidelines.

Please note that concerns about the risk associated with storing personal information in servers/data centres located in certain other countries are recently growing among Japanese citizens.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

No specific technology has been being adopted by private enterprises and government border agencies to digitalise international trade.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

We are of the view that barriers are insufficient use of digital technologies by smaller companies in Japan, with the solution being the offering of tax incentives to these companies to adopt digital technologies in their businesses.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

There used to be no specific tax breaks available for digital businesses. However, the 2021 tax reform bills, which were passed by the Diet on 26 March 2021, include digital transformation investment tax incentives.

Specifically, digital transformation-related investments based on a business plan, certified under the revised Industrial Competitiveness Enhancement Act, made by 31 March 2023 will either be eligible for a 3% to 5% tax credit or for 30% special depreciation. The total value of investments eligible for this relief is up to JPY 30 billion.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Following tax reforms in 2015, certain transactions in which services are received by business operators and consumers located in Japan from foreign business operators will be deemed domestic transactions and accordingly subject to Japanese consumption tax.

A brief outline of the 2015 tax reforms is as follows:

- (i) a destination principle was adopted for “provision of telecommunications services” in respect of the place-of-supply criteria applicable to provision of cross-border services;
- (ii) foreign business operators “providing consumer telecommunications services” are required to register with the relevant tax office in advance;
- (iii) domestic business operators who are recipients of the “provision of telecommunications services for businesses” from a foreign business operator are required to file a tax return (i.e., a reverse charge mechanism). However, the term “provision of telecommunications services for businesses” refers to services where recipients thereof are limited to ordinary business operators based on the nature of the services or the terms and conditions of the transactions. Simply put, this reverse charge mechanism is only applicable to certain B2B transactions; and
- (iv) business operators with a taxable sales ratio of 95% or more that engage in transactions that are otherwise subject to reverse charges will be exempt from reverse charges on such transactions for the time being.

Disputes may arise in respect of the 2015 tax reforms if the exemptions thereunder are lifted in the future. At present, however, no major dispute has arisen in respect of the 2015 tax reforms.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

The main methods of retaining human resources for an

enterprise are employment (whether permanent, fixed-term or otherwise) and outsourcing (on a contractual basis).

The advantages and disadvantages of employment for companies are as set forth below:

Advantages

- The company, as an employer, essentially has the right to instruct an employee on the method, content, place and other matters pertaining to the employee’s work.
- Employees are obligated to devote themselves to their work.

Disadvantages

- It is difficult to terminate an employment agreement even if the employee does not prove to be a good fit for the company. In Japan, as compared to the U.S. or Europe, the thresholds beyond which employment contracts may be deemed justifiably terminated are very high, rendering it considerably difficult for a company to dismiss its employees.

The advantages and disadvantages of outsourcing for companies are as set forth below:

Advantages

- It is easier to terminate an outsourcing contract, relative to the termination of an employment contract.
- No labour management is necessary under an outsourcing contract.
- Companies are not required to procure employment insurance, social insurance, and the like for the relevant personnel who perform work under an outsourcing contract.

Disadvantages

- It is difficult for a company to procure the commitment of an outsourcee unless such commitment is required under the terms of the relevant outsourcing contract.
- Outsourcing contracts can be easily terminated.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation’s physical premises?

There are no specific regulations in Japan on telecommuting. Such arrangements are essentially governed by the internal rules of individual companies.

In recent years, the Japanese government has been promoting a “work style” reform. As a result, telecommuting has come under the spotlight and efforts have been made to promote remote work arrangements. On top of that, amid the COVID-19 pandemic, the Japanese government requests that each company has 70% or more employees work from home during the period of COVID-19 state of emergency.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

It is too early to expect to what extent work-from-home would be accepted after the pandemic. It would depend on companies and types of job. Having said that, a work style would likely become more flexible than before.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Although not specific to digital businesses, certain regulations in Japan may affect foreign investments in Japanese tech

companies. A brief outline of these regulations is set forth below.

- (i) the Foreign Exchange and Foreign Trade Act (FEFTA) requires prior notification of inward direct investments by foreign investors in certain industries to be given to the regulators (the “Prior Notification Requirement”);
- (ii) the list of industries subject to the Prior Notification Requirement (“Restricted Industries”) was expanded on May 27, 2019, for purposes of enhancing cybersecurity. The new industries added under the expanded list can be broadly categorised into (i) manufacturers of information processing equipment and parts, (ii) manufacturers of information processing software, and (iii) information service providers; and
- (iii) the list of Restricted Industries could be broadly interpreted to include a wide range of start-ups, including tech companies.

Additionally, enactment of regulations applicable to digital platform operators will be forthcoming. Specifically:

- (i) on February 18, 2020, a “bill to improve transparency and fairness of certain digital platforms” was approved by the Cabinet; and
- (ii) to improve the transparency and fairness of transactions on digital platforms, the bill, when enacted, will require digital platform operators designated by a separate Cabinet Order to take the following measures:
 - (a) disclose information on the terms and conditions for usage of the digital platform;
 - (b) develop systems and procedures necessary to ensure fair provision of the digital platform; and
 - (c) report the operational status of the digital platform (in response to which the Minister of Economy, Trade and Industry will evaluate and publicise the operational status of the digital platform).

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

There are no notable advantages for a digital business operating in Japan.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The FSA focuses on regulating crypto currencies and online payment services in the financial industry and the PPC focuses on regulating human resources, healthcare and telecommunication business in the data protection area.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

We have assumed for purposes of this response that online payments include prepaid payment instruments and money transfers. Based on this assumption, the Banking Act or the Payment Services Act (the PSA) will be applicable to online payments in Japan.

Money transfer services are regulated under the Banking Act and other legislation applicable to other depository institutions,

which require those who wish to provide such services to obtain the requisite licence from the JFSA. An exception to this is that money transfer services be provided if a firm undergoes license or registration as a funds transfer service provider (FTSP) under the PSA. The revised PSA came into force on May 1, 2021. The revised PSA classifies funds transfer services (FTS) into the following: (1) funds transfer services involving remittances exceeding JPY 1 million per transaction (“Category 1 FTS”); (2) funds transfer services involving remittances up to JPY 1 million per transaction (“Category 2 FTS”); and (3) funds transfer services involving remittances up to JPY 50,000 per transaction (“Category 3 FTS”). A provider of Category 1 FTS (“Category 1 FTSP”) must be authorised to operate by the JFSA and comply with the stricter code of conduct than a provider of Category 2 FTS (“Category 2 FTSP”), while a provider of Category 3 FTS (“Category 3 FTSP”) may operate if registered with the JFSA and are subject to a more relaxed code of conduct than a Category 2 FTSP.

An issuer of prepaid payment instruments is required to comply with applicable rules under the PSA. Where a prepaid payment instrument is only usable for payments to the issuer for its goods or services, such issuer will not be required under the PSA to undergo any registration, although they would still have to comply with certain notice requirements. Specifically, if the amount of unused value in prepaid payment instruments that are only usable to pay for the issuer’s goods and services exceeds JPY 10 million as at the relevant base date (being the end of March and September of every year), the issuer of such prepaid payment instruments will be required to submit a written notice to the JFSA under the PSA. On the other hand, issuers of prepaid payment instruments that are usable not only for payments to the issuer for its goods or services but also for payments to other parties designated by the issuer (the “Third-Party Businesses”) will be required to undergo registration as an “issuer of prepaid payment instruments” under the PSA.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

FTSPs are subject to a code of conduct. Such code of conduct requires an FTSP to, among others, make security deposits of an amount equivalent to the services provided, to the official depository nearest to the service provider’s business office, take measures for customer protection, properly manage information security, and conclude contracts with designated dispute resolution organisations. FTSPs are also subject to KYC requirements under the Act on Prevention of Transfer of Criminal Proceeds which is the primary Japanese AML law.

On the other hand, those who have submitted a written notice to issue prepaid payment instruments for their own business and those who are registered to provide prepaid payment instruments usable for payments to third-party businesses are subject to a code of conduct in respect of prepaid payment instruments. Such code of conduct requires issuers of prepaid payment instruments to, among others, provide information on themselves and the prepaid payment instruments they issue, make security deposits of at least 50% of the total amount of the issued – but yet-to-be-used prepaid payment instruments – to the official depository nearest to the issuer’s business office, refrain from making refunds to holders of the prepaid payment instruments they have issued, implement complaint processing measures and manage information security.



Ken Kawai has extensive experience advising financial institutions, fintech start-ups, investors and corporate clients on complex finance and financial regulatory matters. Ken focuses primarily on the fintech industry, and regularly advises fintech companies, financial institutions, international organisations and industry organisations on legal issues surrounding fintech, including the complex legal framework governing cryptocurrencies and blockchain.

Ken's practice also involves cybersecurity for financial institutions, personal data protection, and e-commerce.

Ken has received Band 1 evaluation in the Legal Department for Chambers FinTech 2020 edition.

Anderson Mōri & Tomotsune
Otemachi Park Building
1-1-1 Otemachi, Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1205
Email: ken.kawai@amt-law.com
URL: www.amt-law.com



Takashi Nakazaki is special counsel at Anderson Mōri & Tomotsune with broad experience in the areas of data protection and privacy (including big data and IoT), information security, intellectual property, licensing, and payment services including cryptocurrency. Further, he has experience working on matters relating to cyber law issues such as cloud computing, domain names, e-commerce, social media and other technology-related areas, telecommunications, labour and general corporate law.

In the area of data protection law, he frequently advises various international and domestic online service companies including operators of online games, online gambling and SNS. In addition, he regularly assists the Japanese government in data protection and cyber law areas including "National Omote-nashi project" and "AI & Data Contracts Guidelines" and continuously leads IAPP Tokyo as a co-founder.

Mr. Nakazaki has been ranked as one of the top lawyers in the data protection and information security field for the last several years.

Anderson Mōri & Tomotsune
Otemachi Park Building
1-1-1 Otemachi, Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1086
Email: takashi.nakazaki@amt-law.com
URL: www.amt-law.com

Anderson Mōri & Tomotsune is among the largest and most diversified law firms in Japan offering full corporate services. Our flexible operational structure enables us to provide our corporate clients with effective and time-sensitive solutions to legal issues of any kind. We are pleased to serve Japanese companies as well as overseas companies doing business in Japan. In response to the increasingly complex and varied legal needs of our clients, we have grown significantly, augmenting both the breadth and depth of expertise of our practice. Our principal areas of practice consist of Corporate, M&A, Capital Market, Finance and Financial Institutions, Fintech, Real Estate, Labour and Employment, Intellectual Property/Life Sciences/TMT, Competition/Antitrust, Tax, Energy and Natural Resources, Litigation/Arbitration/Dispute Resolution, Bankruptcy and Insolvency/Restructuring, International Trade and International Practice (China, India, Asia, US, EU and others).

www.amt-law.com

**ANDERSON
MŌRI &
TOMOTSUNE**

Malaysia

Shin Associates



Joel Prashant



Foo Jia Yi

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

Malaysia does not have B2B-centric legal requirements which exclude application to B2C e-commerce. Rather, there are requirements which apply generally to both B2B and B2C e-commerce.

Legislation that applies to e-commerce includes:

- (a) Communications and Multimedia Act 1998 (“**CMA**”), which regulates the multimedia and communications industry in Malaysia, including applications service providers (i.e. providers of applications services which provide particular functions such as voice services, data services, internet access and electronic commerce which are delivered to end-users) and content applications service providers (i.e. a subset of applications service providers which provide content, such as television and radio broadcast services and the provisioning of information services).
- (b) Computer Crimes Act 1997 (“**CCA**”), which provides for offences relating to the misuse of computers, further explained in question 3.2 below.
- (c) Consumer Protection Act 1999 (“**CPA**”), which applies to all goods and services offered to consumers in trade (including any trade transaction conducted through electronic means) where goods/services are primarily purchased, used or consumed for personal, domestic or household purposes.
- (d) Digital Signature Act 1997 (“**DSA**”), which regulates the use of digital signatures, security of electronic transactions and verification of digital signatures through certificates issued by licensed certification authorities.
- (e) Direct Sales and Anti-Pyramid Scheme Act 1993, which recognises sales through electronic transactions as a form of legal direct sales.
- (f) Electronic Commerce Act 2006 (“**ECA**”), which recognises the validity of electronic contracts and signatures.
- (g) Electronic Government Activities Act 2007, which applies similar rules as the ECA to the public sector.
- (h) Financial Services Act 2013 (“**FSA**”) and Islamic Financial Services Act 2013 (“**ISFA**”), which both recognise electronic money as a payment instrument.
- (i) Malaysian Communications and Multimedia Content Code prescribed by the Malaysian Communications and

Multimedia Commission (“**MCMC**”), which sets out general principles to be complied with by content applications service providers in ensuring that content on their platforms is not indecent, obscene, false, menacing or offensive. Content must also not be discriminatory in terms of race, gender, national or ethnic origin, colour, religion, age, marital status and any physical or mental disability.

- (j) Personal Data Protection Act 2010 (“**PDPA**”), which governs the use of personal data. Under the PDPA, data users must process personal data according to the Personal Data Protection Principles, which consist of the general principle (*obtaining consent from the data subject*), notice and choice principle, disclosure principle, security principle, retention principle, data integrity principle and the access principle. Registration with the Personal Data Protection Commission (“**PDPC**”) may be required if an e-commerce business falls under specified classes of data users prescribed by the PDPC as requiring registration.
- (k) Price Control and Anti-Profiteering Act 2011, which generally deals with price display and product labelling.
- (l) Registration of Business Act 1956 (“**RBA**”), which provides that “*every form of trade, commerce, craftsmanship, calling, profession, or other activity carried on for the purposes of gain*” must be registered with the Companies Commission of Malaysia within 30 days from the date of commencement of the business.
- (m) Sale of Goods Act 1957 (“**SGA**”), which governs contracts for the sale of goods in Malaysia.
- (n) Trade Descriptions Act 2011 (“**TDA**”), which prohibits false trade descriptions and false or misleading statements, conduct and practices in relation to the supply of goods or services (including through electronic means).

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Apart from the legislation referenced in question 1.1 above, the key legal requirements for B2C e-commerce fall under the purview of the CPA, and in particular, the Consumer Protection (Electronic Trade Transactions) Regulations 2012 (“**ETT Regulations**”), which regulate business operators supplying goods or services through a website or in an online marketplace (i.e. a website where goods or services are marketed by third parties for the purpose of trade) (“**Operators**”). While the

CPA governs both B2C e-commerce and non-e-commerce businesses, the ETT Regulations are specific to B2C e-commerce businesses.

Under the ETT Regulations, Operators:

- (a) are subject to disclosure requirements, namely, information such as: the name of the Operator, business, or company; business/company registration number; contact details; full price of the goods; method of payment; description of goods or services; and applicable terms and conditions;
- (b) must also provide means to allow buyers to rectify any error prior to the confirmation of the orders made by the buyers;
- (c) must acknowledge receipt of orders from buyers without undue delay; and
- (d) must take reasonable steps to keep and maintain a record of the names, telephone numbers and the addresses of suppliers of goods or services in the online marketplace, for a period of two years.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The PDPA and its subsidiary legislation regulate the collection, use, processing and disclosure of personal data in respect of commercial transactions.

While no amendments to the PDPA have been legislated since its inception, the Malaysian Government is reviewing the PDPA to focus on alignment with other international data protection laws (particularly the European Union's General Data Protection Regulation). The PDPC had on 14 February 2020 issued a public consultation paper to garner public views on the proposed review of the PDPA. No specific timeframe has been fixed for the proposed amendments to be legislated.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Fintech

One of the key privacy challenges for fintech operators would be obtaining consent of data subjects. Digital profiling (i.e. the process of gathering and analysing information about an individual that exists online) of clients seeking fintech services may pose issues under the PDPA, where consent of a data subject is required before the data subject's personal data may be processed, unless the processing is necessary for specific exempted purposes. Although the PDPA does not define nor prescribe formalities in terms of consent, the Personal Data Protection Regulations 2013 ("PDP Regulations") provide that consent from data subjects must be recorded and maintained and may be subject to inspection by the PDPC.

Fintech companies collect copious amounts of data, particularly sensitive personal information and financial records about their customers, as well as alternative data (e.g. data on customers' online spending behaviour and social media patterns) to trace their digital footprint. This creates security concerns due to the growth in the integration of banks' systems with fintech firms' software (locally and internationally), resulting in more third-party access to customer data, notwithstanding that they may have differing security frameworks and jurisdictional compliance obligations. This collection of alternative data would also trigger consent obligations under the PDPA.

As digital profiling and customer data collection is largely automated, integration of adequate mechanisms to obtain and maintain such consents in the relevant systems is imperative for compliance with the PDPA.

Financial institutions in Malaysia are also subject to additional data protection obligations in relation to customer affairs or account information under the FSA.

Various breach reporting obligations by authorities and regulators may be triggered due to data breaches. For example, under the Management of Customer Information & Permitted Disclosure policy document published by the Central Bank of Malaysia (*Bank Negara Malaysia*) ("BNM"), financial service providers who detect data breaches in their systems are required to investigate data breaches within three months from detecting the breach and submit a detailed report on the same to BNM within one day upon tabling to the board. Further, under the Guidelines on Management of Cyber Risk published by the Securities Commission of Malaysia ("SC"), all capital market entities are required to report cyber incidents/breaches to the SC on the day of the incident/breach.

Retail

The usage of cookies to track a user's surfing and purchasing trends has recently garnered significant attention, particularly in view of the recent issue concerning WhatsApp's update to its privacy policy to enable data in business messages to be used for commercial purposes such as advertisement targeting via its parent company, Facebook. The issue has brought to light the perils of cloud data mining, and the extent to which it is effectively regulated in keeping one's privacy safe in cyberspace is still fairly vague. Under the General Principle of the PDPA, explicit and express consent must be obtained from the data subject prior to processing the data. Further, the Notice and Choice Principle requires data users to notify the data subject by written notice of the purpose for which the data is collected, the right to request access for correction, source of the personal data, to whom the personal data is being disclosed to and means for the data subject to limit the processing of the personal data. Problems arise in ensuring this benchmark in consent and notification is properly met by online retail providers which may not necessarily have comprehensive data protection policies in place to address these requirements.

Another issue of retail-related personal data protection would be direct marketing. Under the PDPA, data subjects have a right to reject processing of their personal data for the purposes of direct marketing. "Direct marketing" is defined as the communication by whatever means of any advertising or marketing material which is directed to particular individuals. A common method of marketing employed by businesses is the issuance of mass promotional and marketing emails to all their customers. In doing so, these companies risk accidental exposure of the email addresses of one customer to another. For compliance with the PDPA, companies would need to ensure that there are avenues for data subjects to opt out from direct marketing, failing which, the company could be liable to fine of RM200,000.00 or imprisonment up to two years or both.

Artificial Intelligence ("AI")

The machine learning ("ML") subset of AI has a number of privacy challenges. ML requires vast amounts of data for the AI training process and, in addition, the derived system is also granted access to larger volumes of data as part of inference processing while in operation. In many cases, personal data is involved, which triggers obligations under the PDPA in processing the same.

With the increased adoption of data analytics, big data, and Internet of Things ("IoT"), which require significant levels of

data exchange and data processing, compliance with the PDPA becomes paramount where individuals are identifiable from the data exchanged or processed. This may be particularly difficult where written consent of such data subjects is required to process such data and where automated systems employing ML fail to take such consent requirements into account prior to processing the data.

Digital Health

Various types of data, including demographics and clinical information, are collected and stored in the form of electronic medical records (“EMR”). EMR is shared among healthcare practitioners and providers to improve healthcare provisioning and medical research and to allow data utility to support medical research, decision making and personalised medicine, amongst others. As EMR contains patients’ sensitive information, a higher standard of compliance with the PDPA is required, in particular, requiring express consent from the relevant data subjects in order to process sensitive personal data.

The main challenge in the digital health field is the preservation of EMR privacy and security. It is important for healthcare providers to procure privacy guarantees from their data processors at all levels within the system. Adequate security mechanisms must be applied in order to protect the EMR when processed internally by the organisation or externally by third parties, such as insurance providers, and to ensure that patients’ personal data is not exposed to unauthorised parties.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Fintech

Regulatory and governmental initiatives have been implemented and/or proposed over the past years to facilitate the development of digital services, particularly in the fintech sector.

In 2018, the Ministry of Finance launched the National Regulatory Sandbox Initiative to enable innovators to experiment and test their technological solutions/products which either require regulatory framework, or which may potentially impact a regulatory environment in a conducive space. This allows start-ups to experiment and work with BNM on assessing the fintech “risk”, and its potential upside to the financial industry.

The SC has smoothened the introduction of Digital Asset Exchange (“DAX”) operators into Malaysia and developed requirements for entities intending to operate DAX systems in Malaysia, which in turn facilitates the regulated implementation of DAX services in the country.

Retail

The Government introduced PENJANA Shop Malaysia Online’s initiative to spur economic recovery by stimulating online consumption through high impact e-commerce promotions executed via a public-private partnership model. PENJANA Shop Malaysia Online has successfully generated sales worth RM896 million and benefited 7.8 million users as well as more than 213,000 local sellers from all over the country since its launch on 1 August 2020. The Malaysia Digital Economy Corporation (“MDEC”) also set up Go-eCommerce, an online entrepreneurial platform with the tools to help sellers develop their business.

The Government also provides grants and loans to eligible enterprises for adoption or subscription of digitalisation services under the following programmes:

The SME Technology Transformation Fund, totalling RM500 million, is part of the Government’s economic stimulus package to provide financial assistance to Small and Medium Enterprises (“SMEs”) to adopt digitalisation and/or automation in their business operations to achieve higher productivity, process efficiency, efficient cost management and greater market penetration.

The Smart Automation Grant totalling RM100 million, capped at up to RM1 million per company, is targeted towards SMEs and mid-tier companies in the services sector to kickstart their digital adoption journey and increase their digital capabilities to continue striving forward in the new normal.

Under the National Economic Recovery Plan (PENJANA), the Government also introduced the MyAssist SME One Stop Shop initiative, which is an online one-stop business advisory platform for micro-enterprises and SMEs aiming to enhance the outreach of the existing physical SME Hub. The services offered include guidance on:

- funding facility;
- trade facilitation;
- branding and promotion;
- technology support; and
- legal.

AI

MDEC is developing a national AI framework, with the aim of fuelling Malaysia’s AI ambition. Malaysia’s Minister of Communications and Multimedia had previously indicated that the Government is contemplating proposing a national data and AI policy to drive Malaysia’s push towards the fourth industrial revolution.

Some examples of AI initiatives for specific industries in Malaysia are as follows:

- (a) Malaysia has put into place the National Industry 4.0 Policy Framework (“My-i4.0”) which provides a concerted and comprehensive transformation agenda for the manufacturing sector, and takes into consideration the potential application of AI to the industry.
- (b) The Government has taken measures to facilitate the digitalisation of the court system, involving the pursuit of an array of AI-based initiatives. These include the introduction of e-bail and e-review (reducing the need for lawyers and litigants to physically appear in court, saving time and costs for all parties) and digital voice-to-text court recording transcripts and digitally-secured evidence.

Digital Health

The MCMC has conducted its Connected Healthcare Pilots project with various industry partners, seeking to accelerate the adoption of healthcare technology and next generation communication services.

Digital Health Malaysia (“DHM”), an organisation co-chaired by the Director General of Health and the Chairman of the MCMC, has established four Special Interest Groups to look at policy and regulations, knowledge dissemination and networking, research and development (“R&D”), clinical trials, certifications, go-to-market strategies, and manufacturing, all related to digital health initiatives. DHM intends to set up a sandbox for digital health start-ups to provide their services in a safe environment and provide suggestions on outdated regulations.

Collaborative Research in Engineering, Science and Technology (“CREST”) is looking at healthcare as a prime sector for technological disruption. CREST has already assisted three innovators in conducting clinical trials of their high-tech solutions in Malaysia, in collaboration with the Ministry of

Health and industry partners. CREST facilitates innovation by helping to turn ideas into products and connect inventors with regulators, investors or DHM, and also provides funding.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The National Cyber Security Policy (“**NCSP**”) was implemented by the Government with the aim to develop and establish a comprehensive programme based on a National Cyber Security Framework to ensure the effectiveness of cybersecurity controls over vital assets and various sectors comprising the Critical National Information Infrastructure (“**CNII**”). The Government has stipulated ISO/IEC 27001 Information Security Management Systems as the minimum information security standard for all CNII sectors. There are also sector-specific guidelines that deal with cybersecurity in Malaysia. These include the Data Management and Management Information System Framework and Guidelines on Internet Insurance issued by BNM.

Malaysia has established a national cybersecurity specialist agency, known as CyberSecurity Malaysia (“**CSM**”), under the purview of the Ministry of Communications and Multimedia. CSM provides specialised cybersecurity services and is tasked to continuously identify possible areas which may be detrimental to national security and public safety.

Additionally, Malaysia established the National Cyber Security Agency, an agency under the Prime Minister’s Department to act as the national leading agency for cybersecurity matters, tasked with cybersecurity policy development at the national level, amongst other functions such as protecting CNII, and undertaking strategic measures in countering cyber threats.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The Government has intimated the possibility of introducing specific legislation on cybersecurity, although no clear time-frame has been fixed for its development. Further on from question 1.1 above, the current legislation applicable to cybersecurity is:

- (a) The CCA, which provides for offences relating to: unauthorised access into computers or networks; committing or facilitating the commission of further offences; and unauthorised modification of the contents of any computer and/or wrongful communication. The Royal Malaysian Police (“**RMP**”) is empowered to enforce such offences under the CCA and depending on the offence, upon conviction, applicable fines and/or imprisonment can be imposed.
- (b) The CMA, which prohibits, *inter alia*: the fraudulent or improper use of network facilities or network services; the use and possession of counterfeit access devices; the use of equipment or devices to obtain unauthorised access to any network services; and interception of any communications except with lawful authority. The MCMC enforces offences under the CMA, and depending on the offence, applicable fines and/or imprisonment can be imposed upon conviction.
- (c) The Copyright Act 1987 (“**CA**”), which prohibits circumvention of any technological protection measure which is applied to a copy of copyright work. The CA also

expressly prohibits anyone from: (i) designing, producing, adapting or performing for the purpose of enabling or facilitating the circumvention of technological protection measures; and (ii) manufacturing, importing or selling any technology or device for the purpose of circumventing any technological protection measure. The Ministry of Domestic Trade and Consumer Affairs (“**MDTCA**”) enforces offences under the CA by imposing fines and/or imprisonment upon conviction.

- (d) The PDPA and the PDP Regulations, which provide that a data user shall, when processing personal data, take practical steps to: (i) protect the personal data from any loss, misuse, modification, unauthorised or accidental access of disclosure, alteration or destruction; and (ii) develop security policies to ensure such protection. The PDPC is tasked with the enforcement of offences under the PDPA and the PDP Regulations. The PDPC may enforce such offences by imposing fines and/or imprisonment.
- (e) The Penal Code (“**PC**”), which codifies most criminal offences and procedures in Malaysia, may be relied on to prosecute specific cybersecurity-related offences which are not captured under the CCA, CMA, CA, or PDPA. Offences relating to threats to national security, fraud and identity theft are set out under the PC and are enforced by the RMP.
- (f) The Strategic Trade Act 2010 (“**STA**”), which prohibits the export, transshipment, transit and brokering of strategic items and technology, including arms and related materials, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction, without obtaining the relevant permits. The Ministry of International Trade and Industry (“**MITI**”) is tasked with enforcement of offences under the STA and any breach of the provisions contained within the STA can result in the death penalty (where death is the result of the act), imprisonment or a fine.
- (g) Other applicable guidelines or regulations: the SC has published its Guidelines on Management of Cyber Risk, making it mandatory for entities to have clear and comprehensive cyber policies and procedures which are commensurate with their risk profiles. Non-compliance may attract applicable fines and/or imprisonment upon conviction, or civil liability for damage suffered by third parties due to such non-compliance.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Consumers in Malaysia are growing towards embracing e-commerce alongside the conventional methods of purchasing goods and services. According to the “*E-Commerce Consumers Survey 2018*” (“**Survey**”), carried out by the MCMC, the percentage of e-commerce consumers in 2018 was at 51.2%.

Some of the reasons why consumers are growing towards accepting and using e-commerce are:

- (a) convenience of being able to purchase products locally and internationally and accessibility thereto;
- (b) the pricing of products in which discount vouchers or cash rebates are awarded, particularly during festive sales periods; and
- (c) availability of a wider selection of products compared to physical stores.

Electronic payments (“e-payments”) have seen widespread adoption in Malaysia in recent times. In view of this, BNM has identified the various benefits of e-payments and has focused on increasing the efficiency of the nation’s payment systems utilising e-payments. BNM released its Financial Sector Blueprint 2011-2020, focusing on e-payments for greater economic efficiency to drive Malaysia’s transition to a high value-added, high-income economy with adequate safeguards to preserve financial stability. Measures to accelerate the migration towards e-payments include providing the right price signals to encourage the switch from paper-based payments to e-payments, and facilitating wider outreach of e-payments infrastructure, such as point-of-sale terminals and mobile phone banking.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

There are no particular payment methods which offer cultural challenges in Malaysia. Rather, certain payment methods are preferred over others. According to the Survey, online banking prevailed as the preferred payment method in Malaysia, followed by credit card payment, debit card payment, and cash on delivery, amongst others.

E-wallet adoption, however, has faced rapid expansion in recent years and has been gaining traction as a preferred payment method in the country for most businesses.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Pursuant to a survey conducted by the Department of Statistics Malaysia in 2017 titled “Usage of ICT and E-Commerce by Establishment (ICTEC)”, income from e-commerce transactions in Malaysia was dominated by the domestic market of RM399.8 billion with a share of 89.3% compared to the international market of RM48.0 billion with a share of 10.7%. This appears to suggest that domestic e-commerce platforms fare better locally as compared to other jurisdictions.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Yes, e-commerce firms in Malaysia typically overcome language barriers for selling products/services in other jurisdictions by having language selection options available on their websites/platforms. The most common language selection options are English, Malay, and Chinese. An estimated 40% of all Malaysian e-commerce sales are cross-border, where the primary target markets are most ASEAN countries, Australia, China, Hong Kong, India, Japan and the USA.

4.5 Are there any particular web-interface design concepts that impact on consumers’ interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Web-interface design concepts in Malaysia are varied and constantly developing. Some of the most pertinent factors for

web-interface design concepts are the manner in which the goods and services are presented, and representations of security of information and payments contained on the website. Most e-commerce platforms in Malaysia increase accessibility to customers by having user-friendly mobile applications integrated with the online aspect of the platforms. These platforms commonly include features such as order history, order tracking, social media sharing features, and the ability to chat online with customer service representatives, which have been seen to positively impact on consumers’ interactivity.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The COVID-19 pandemic has given a huge boost to the e-commerce market growth in Malaysia. According to GlobalData’s E-Commerce Analytics, Malaysia’s e-commerce market is expected to reach MYR51.6 billion (US\$12.6 billion) by 2024, increasing at a compounded annual growth rate (“CAGR”) of 14.3% between 2020 and 2024. This is due to the unprecedented increase of digitalisation following the various lockdowns put in force to curb the spread of COVID-19. There were also initiatives put forth by the Government such as the National eCommerce Strategic Roadmap, which helped nearly 80,000 SMEs adopt e-commerce and assisted nearly 8,000 companies adopt e-commerce for exports from January to June 2020. The Government has also recognised the need to protect gig workers and has indicated that it is planning to incorporate social protection measures in the 12th Malaysia Plan (2021-2025).

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Online brand infringement may surface in various manners, ranging from the unauthorised registration of domain names featuring brand names, to selling counterfeit or infringing goods, amongst others. Online brands are principally protected under trademark laws in Malaysia, mainly by way of trademark registration with the Intellectual Property Corporation of Malaysia.

Protection of a trademark may be enforced where a person uses an identical or similar sign to a trademark that is registered without the consent of the registered proprietor, which results in the likelihood of confusion on the part of the public. Where trademark infringement arises, pursuant to the Trademarks Act 2019 (“TA”), remedies available to the registered proprietor would include:

- (a) an injunction (subject to conditions);
- (b) damages;
- (c) account of profits; or
- (d) the award of additional damages which the court considers appropriate (in cases involving the use of a counterfeit trademark).

The TA criminalises the counterfeiting of products where a similar or identical mark is used with the intent to deceive, or where a genuine registered trademark is falsified without the consent of the registered proprietor. The registered proprietor can lodge a complaint with the MDTCA, pursuant to which the enforcement division thereof may undertake raids and seize counterfeit products and/or request that such links promoting infringing products be removed. Upon conviction, a fine and/or imprisonment may be imposed.

Apart from the above, specific e-commerce platforms in Malaysia such as Lazada and Shopee provide take-down procedures where brand owners may submit requests for infringing links to be taken down.

Domain name infringement may also be enforced by referring the dispute to the Asian Domain Name Dispute Resolution Centre (“ADRC”) at the Asian International Arbitration Centre (“AIAC”) as an alternative to court proceedings.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Despite the various avenues for enforcement as listed in question 5.1, while there are no specific restrictions, such measures may be challenging to undertake. Initiating take-down requests to remove infringing materials would depend on: the cooperation of the infringer; evidence of trademark registration; and proof of trademark infringement or domain name infringement. Certain online platforms require brand owners to have registered their trademarks in the country in which the notice of infringement is filed in order to accede to take-down requests.

An online brand owner may also consider issuing take-down requests to the infringer directly; however, this may be difficult where the identity of the infringer is not readily accessible. This may also affect the ability of an owner to initiate court proceedings as the infringer’s identity would be required, and identifying the same may be difficult due to local and international privacy laws. Filing police reports does not guarantee that authorities will be able to identify and disclose such information.

For domain name infringement, dispute resolution may also be challenging as an owner will have to establish that the domain name was registered in bad faith. This may be difficult to prove where the online brand owner has unregistered rights to a trademark instead of formal registration. Local country-code top level domain name disputes are generally filed at the AIAC in accordance with the Malaysian Network Information Centre’s (“MYNIC”) Domain Name Dispute Resolution Policy (“MYDRP”) and Rules of the MYDRP. However, enforcement by way of arbitration under the MYDRP is restricted to domains ending with the country code “.my” which have been registered with the MYNIC. Dispute resolution for local and international generic top-level domain names may be referred to the ADRC. Enforcement may also be sought via civil proceedings, although this may prove to be costly and time-consuming due to the technical nature of the evidence required.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Data centres and cloud computing providers fall within the definition of “data processors” under the PDPA and would require compliance therewith. Data users that engage data processors are required to contractually ensure that the data processors provide sufficient guarantees on technical and organisational security measures governing personal data processing and to take reasonable steps to ensure the data processors’ compliance with those measures.

Additionally, the MCMC via the Technical Standards Forum designated under the CMA prepared a Technical Code on Information and Network Security – Cloud Service Provider Selection (“Code”) in reference to International Standards such

as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27036-4 and other best practices on information security, cloud deployment and strategy. Under the Code, cloud service customers (i.e. organisations or parties engaging in business relationships for the purpose of using cloud services) (“CSCs”) are required to collaborate with cloud service providers (“CSPs”) to recognise and ensure the safety and security of cloud engagement and services.

Formal agreements between CSCs and CSPs are essential to formalise the responsibilities of the relevant parties when a security incident occurs. CSCs must ensure that: (a) they have agreements with CSPs; (b) the contents in the agreements are understandable and do not harm or inflict huge losses to the organisation; and (c) the agreements include specific contractual provisions set forth in the Code, touching on service delivery, service accessibility and availability, indemnification obligations and protection of intellectual property rights, amongst others.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

There are no specific requirements for servers/data centres to be located in Malaysia. However, where businesses use equipment (including servers and data centres) in Malaysia for the processing of personal data other than for mere transit of the personal data through Malaysia, compliance with the PDPA is required.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Various initiatives have been undertaken by private enterprises to adopt Industry 4.0 technologies, particularly mobile payments, automation software and big data/analytics. A recent FedEx-commissioned study titled “*Global is the New Local: The Changing International Trade Patterns of Small Business in Asia Pacific*” revealed that Malaysia has an overall higher adoption rate of e-commerce (90%), mobile-commerce (87%) and social-commerce (86%) compared to other markets in Asia Pacific. 61% of Malaysian small and medium-sized enterprises (“SMEs”) expressed confidence that the digital economy will help reduce barriers to source global customers beyond APAC. 78% of respondents agreed that Industry 4.0 technologies have enhanced efficiencies in the supply chain and distribution channels while helping reduce challenges brought by cross-border payments.

Most industry sectors have adopted digital technologies and provide e-services to varying degrees, including: online advertising (viewed from abroad); digital Information Technology Business Processing Outsourcing (“IT-BPO”) services; exporting data processing and online software consultancy services; and direct e-services, such as online tourism booking and electronic banking.

The Government has implemented a number of long-term initiatives with favourable implications for information communications technology (“ICT”) products and services, including investment in high-speed broadband infrastructure, and encourages international companies to consider Malaysia as a test bed for the global ICT industry. In 1996, the Government developed the Multimedia Super Corridor Malaysia (“MSC”) in order to attract foreign and domestic investment in the ICT industry. The MSC is Malaysia’s initiative for the global ICT industry

and is designed to be an R&D centre for industries based on ICT. The MSC is also an ICT hub equipped with high-capacity global telecommunications and logistics networks and serves as the country's ICT backbone which enables a high-speed ICT link connecting Malaysia to Japan, ASEAN countries, USA and Europe to promote greater trade.

MDEC has engaged international partners as part of its cross-border e-commerce initiatives to help drive Malaysia's National eCommerce Strategic Roadmap, aiming to help Malaysian SMEs grow abroad by providing cross-border logistics solutions to deliver their products throughout Southeast Asia.

Among MDEC's initiatives is the onboarding of more merchants onto the Digital Free Trade Zone ("DFTZ"), which is an electronic world trade platform designed to facilitate seamless cross-border trade and to enable Malaysian SMEs to export goods with a priority for e-commerce by providing platforms, e-fulfilment activities and enhanced trade facilitation measures, such as financing, last mile fulfilment, insurance and cargo clearance, amongst others.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Examples of significant barriers include: economic implementation costs; reluctance in acceptance of technology; higher requirements for equipment and processes; lack of knowledge/education; and individual hesitance. Industry 4.0 technology implementation includes high costs of owning and using the technologies on-site, and in keeping up with the advances in technology. Some industries may not be willing to invest into what they may consider to be high-risk and expensive technology. Furthermore, costs will also be expended for training as well as external consultancy fees.

Fears of technology replacement may result in employees being resistant and reluctant to accept new technologies. Uncertainty and scepticism about the applicability, efficiency and benefits of such technologies are also barriers to the introduction and development of innovative technologies. Furthermore, certain industries strongly resist adopting new and advanced technologies, which leads to conservatism and affects employees' adaptability with these technologies.

Due to the need for employee training and development, together with the increasing need for integration skills, there are challenges to create and develop new competencies to ensure that project organisation is optimised as well as to attract new talents to the workforce, such as employees with shared technical knowledge.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Pioneer Status ("PS") and Investment Tax Allowance ("ITA")
Companies in specified sectors, including the commercial sector, which participate in promoted activities or produce promoted products, may be eligible for PS or ITA.

Various types of projects such as projects of national and strategic importance which involve large capital investment and

high-technology, as well as high-technology companies engaged in new and emerging technologies, may be granted enhanced PS and ITA incentives. PS exempts Corporate Tax ("CT") on 70% of statutory income for five years, where the remaining 30% is taxed at prevailing CT rates. ITA applies to 60% of qualifying capital expenditure ("QCE") incurred for a five-year period, to be utilised against 70% of statutory income, where the remaining 30% is taxed at prevailing CT rates.

Principal hub

A principal hub is a locally incorporated company that uses Malaysia as a base for conducting its regional and global businesses and operations through management, control, and support of key functions, such as risk management, strategic decisions, finance, and human resources. The principal hub provides CT at rates of 0% or 5% for a period of 5 + 5 years for new companies or a rate of 10% on statutory income for five years for existing companies subject to conditions for applications from 1 January 2019 to 31 December 2020.

Other incentives include:

- (a) no equity/ownership conditions;
- (b) flexibility on foreign exchange administration and expatriate positions; and
- (c) customs duty exemption for raw materials, components, or finished products brought into free zones, licensed and bonded warehouses for production or repackaging, cargo consolidation, and integration before distribution to its final customers for goods-based companies.

Under Budget 2021, it has been proposed that the application period for this incentive be extended for another two years from 1 January 2021 to 31 December 2022. Further, minimum conditions of the number of high value jobs, annual operating expenditure and the number of key posts for renewal of the tax incentive for the second five-year period will be relaxed.

Global Trading Centre

Under Budget 2021, a new incentive scheme was proposed to be introduced for entities to be designated as a Global Trading Centre and be given a 10% income tax rate for a period of five years, renewable for a further five years as a measure to enhance and simplify tax incentives for trading activities previously covered under the principal hub incentives which were subjected to higher eligibility criteria.

MSC Malaysia

MSC Malaysia status is awarded to both local and foreign companies that carry out one or more of the MSC Malaysia promoted activities. Companies recognised as a MSC Malaysia status company may apply for a services incentive which allows up to 100% income tax exemption on statutory income derived from approved MSC Malaysia promoted activities, for a period of five years, renewable for a further period of five years. List of promoted activities include:

- (a) big data analytics;
- (b) artificial intelligence;
- (c) financial technology;
- (d) internet of things;
- (e) cybersecurity (technology/software/design and support);
- (f) data centre and cloud (technology/software/design and support);
- (g) blockchain;
- (h) creative media technology;
- (i) sharing economy platform;
- (j) user interface and user experience;
- (k) integrated circuit design and embedded software;
- (l) 3D printing (technology/software/design and support);

- (m) robotics (technology/software/design);
- (n) autonomous (technology/software/design and support);
- (o) systems/network architecture design and support; or
- (p) global business services or knowledge process outsourcing excluding nontechnical and/or low value call centre, data entry, and recruitment process outsourcing.

The Government has also granted sales tax exemption for the importation of multimedia equipment by MSC Malaysia status companies subject to exemption criteria set and approval by Ministry of Finance effective from 21 February 2020.

MSC Malaysia status companies are eligible for incentives, which include:

- (a) income tax benefits of up to 10 years;
- (b) flexibility in employment of local and foreign knowledge workers;
- (c) freedom to source capital globally for investments;
- (d) protection of intellectual property and cyber laws;
- (e) no censorship of the internet; and
- (f) globally competitive telecommunication tariffs.

Incentives for R&D

- (a) Contract R&D company
Companies providing R&D services to third parties are eligible for:
 - (i) PS with income tax exemption of 100% of statutory income for five years; or
 - (ii) ITA of 100% of QCE incurred within a period of 10 years and the ITA can be utilised against 70% of statutory income for each year of assessment. Unutilised allowances can be carried forward until fully absorbed.
- (b) R&D company
An R&D company can apply for ITA of 100% of QCE for a period of 10 years. The ITA can be utilised against 70% of statutory income for each year of assessment.
- (c) In-house R&D
Companies conducting in-house R&D are eligible to apply for ITA at 50% of QCE incurred within a period of 10 years. The ITA can be utilised against 70% of statutory income for each year of assessment.
- (d) Reinvestment in R&D
R&D companies/activities mentioned in categories (a) – (c) above are eligible for an additional round of PS for another five years or ITA for a further 10 years, where applicable.
- (e) Commercialisation of Public Sector R&D
A company investing in a subsidiary involved in the commercialisation of resource-based R&D findings is allowed a deduction equivalent to the amount of such investment, while a subsidiary undertaking such commercialisation is granted PS with 100% income tax exemption of statutory income for 10 years.

Under Budget 2021, it was proposed that (i) the tax incentive for the commercialisation of non-resource-based R&D findings be reintroduced, and (ii) tax incentives for the commercialisation of R&D findings by public research institutions, including public higher learning institutions, be expanded to private higher learning institutions. The objective is to create a competitive R&D ecosystem and to encourage new R&D activities by public research institutions including public higher education institutions as well as to enhance the role of private higher education institutions in producing high quality researchers and quality R&D. The tax incentives are as follows:

- investor companies may apply for a tax deduction equivalent to the amount of investment made in a subsidiary company that commercialises the R&D findings of public research institutions including public and private higher learning institutions; and

- income tax exemption of 100% of statutory income for 10 years will be granted to subsidiary companies that commercialise R&D findings of public research institutions including public and private higher learning institutions.

In light of the COVID-19 pandemic, the Malaysian Government in March 2019 imposed a Movement Control Order (“MCO”) to restrict the movement of persons in Malaysia to combat the pandemic and subsequently introduced various initiatives to assist individuals and organisations during the imposition of the MCO, under the Economic Stimulus Package 2020.

A sum of RM300 million has been allocated towards the automation and digitalisation facility available to SMEs to encourage the automation and digitalisation of operations to increase productivity and efficiency. This facility, administered by BNM, allows eligible SMEs to obtain financing of up to RM3 million for a tenure of up to 10 years at a rate of 4.00% per annum was available from 6 March 2020 to 31 December 2020. In March 2021, BNM announced that it will allocate an additional RM700 million for the automation and digitalisation facility, which will be available until 31 December 2021 or full utilisation, whichever is earlier.

Companies relocating their operations to Malaysia and undertaking new investments

In the Budget 2021, the Government proposed to review the tax incentives for companies relocating their operations to Malaysia and making new investments as follows:

- application period for the tax incentives be extended for a further year (previously only available until 31 December 2021); and
- the scope of tax incentives be expanded to companies in selected services sector including companies adopting Industrial Revolution 4.0 and digitalisation technology with investments that contribute to significant multiplier effect in the following services:
 - provision of technology solutions, or more typically technology companies which develop technology and provide technology solutions based on substantial scientific or engineering challenges;
 - provision of infrastructure and technology for cloud computing;
 - R&D/design and development activities;
 - medical device testing laboratory and clinical trials; and
 - any services or manufacturing related services as determined by the Minister of Finance.

An income tax rate of 0% to 10% and an income tax rate of 10% will be given to new companies and existing companies with a ‘new services’ segment respectively for a period of up to 10 years.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Under the Service Tax (Amendment) Act 2019, the Malaysian Government has imposed a service tax of 6% on digital services (“DST”) provided by registered foreign service providers (“FSP”) which are imported by consumers in Malaysia under a B2C regime effective from 1 January 2020, to level the playing field between local and foreign digital service suppliers and to facilitate taxation of the digital economy.

The scope of “digital services” covers any service that is delivered or subscribed over the internet or other electronic network, which cannot be obtained without the use of information technology, and where the delivery of the service is essentially automated.

The implementation of the DST may potentially lead to disputes between digital businesses and the Malaysian tax authorities, particularly in relation to the requirement to register with the tax authorities and whether the value of digital services rendered by the FSP to Malaysian customers falls within the threshold imposed by the tax authorities for registration.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In resourcing work in Malaysia, businesses would need to consider various factors including: (a) the extent of control to be exercised over individuals carrying out such work; and (b) the specific types of workers required for the operation of the business, and in particular, the various skill sets employed by such workers.

In addressing (a) above, businesses have relative flexibility to engage individuals under various employment status models, e.g. permanent employment, part-time employment, or fixed-term employment, where significant control is exercised over the work carried out by the individuals. Where employment is concerned, compliance with the Employment Act 1955 (“EA”) is strictly required for employees earning under RM2,000 a month, amongst other specific groups of employees. Employees earning in excess of the said sum are not governed by the EA and have their rights and entitlements solely addressed by their contracts of employment. Advantages of employment models include: more control by employers over undertaken work; long-term retention of valuable skillsets; exclusivity of services; and automatic ownership of work products. Disadvantages include stringent compliance with employment laws and procedures as well as higher long-term costs.

Individuals may also be engaged on an independent contractor basis. However, there is a fine line between employment and independent contractor relationships, and there is no single objective test which distinguishes the same. Rather, the facts and circumstances surrounding the engagement are considered in determining the nature of the relationship. These include: the nature, degree and extent of control exercised over the engaged party; exclusivity of services; whether the work done is integral to the business or ancillary thereto; whether contractual provisions for overtime, working hours, holidays and other benefits are provided; whether statutory deductions have been made; and how the contract may be terminated. Should an employment relationship subsist, compliance with employment laws would be required. Independent contractors do not have specific legislation governing their engagement. Advantages of engaging independent contractors include less regulatory compliance, lower long-term costs, and short-term engagement for specific tasks. Disadvantages include less control over undertaken work, lack of exclusivity, and lack of fixed rates for services.

In addressing (b) above, both local and foreign workers may be resourced in Malaysia, with foreign workers only able to work in Malaysia upon obtaining the appropriate immigration

passes. It should be noted that the various immigration passes in Malaysia have differing rules as to their requirements and permitted scope of activities which may be undertaken by the employees, as follows:

Immigration Pass	Details
Short-term social visit pass	Issued at the entry point to foreign citizens for social and business visits for up to thirty days.
Professional visit pass	Issued to foreign citizens holding acceptable professional qualifications to take up professional work in Malaysia for a Malaysian entity for up to twelve months.
Employment pass	Issued to foreign citizens (expatriates) entering Malaysia to take up paid employment under a contract of service with an employer. The pass may be issued for up to five years. Employers must comply with certain requirements, including: ■ minimum paid-up capital ranging between RM250,000 and RM1 million; ■ obtaining recommendations from and registration with relevant monitoring agencies; ■ providing a minimum monthly salary of at least RM3,000; ■ the skill, qualification and experience required for the expatriate position must be such that it cannot be fulfilled by local candidates; and ■ the expatriate’s role must be relevant to the activities of the employer.
Residence pass – talent	Restricted to Peninsular Malaysia, and is issued to foreign citizens considered to be high-achieving individuals with the capacity to contribute towards the national key economic areas and the country’s economic transformation. The applicant must: ■ have worked in Malaysia for at least three continuous years; ■ hold a valid employment pass with more than three months’ validity at the time of the application;

Immigration Pass	Details
	■ hold a Ph.D., Master's degree, Bachelor's degree or diploma in any discipline from a recognised university, or a professional or competency certificate from a recognised professional institute; ■ hold a Malaysian income tax file number and must have paid income tax for at least two years; ■ possess five years of total work experience; and ■ earn a basic salary of RM15,000 per month.
Visit pass (temporary employment)	Issued for the employment of foreign nationals as semi-skilled or unskilled workers, or domestic helpers, from specific source countries in certain sectors of the economy, such as agriculture; construction; manufacturing; plantation; and various types of services.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no broad and overarching governmental regulations in Malaysia which govern nor restrict carrying out work away from an organisation's physical premises. However, organisations may internally implement rules and requirements in relation to the conduct of work outside of that organisation's physical premises, for confidentiality and practical reasons. General statutory health and safety obligations of employers would continue to apply in respect of such work, so far as it would be practicable to do so.

Pursuant to the MCO implemented on 18 March 2020, the Government ordered the closure of private and public premises save for several essential service sectors. Following this, the Work From Home ("WFH") Directive was announced which required certain employees to work from home. Clarification and directions were also provided by MITI which addressed questions such as the number of employees allowed in the office at the same time, whether it is mandatory for employees to conduct COVID-19 screening prior to returning to office, as well as whether employees are entitled to full salary while they are working from home.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Flexible and remote working options: With the implementation of the MCO, most companies which do not fall within the essential services sectors were forced to leave their standard office premises behind and rely fully on technology. Companies such as Facebook, Shopify and Microsoft have decided to allow a certain number of employees to work from home permanently.

The pandemic brought the realisation that in this age of digitalisation, most of the work can be done from home, saving time, money, and resources, while promoting safety.

Faster internet speed: Following the report from MCMC which reported an increase in the internet traffic from the beginning of the MCO due to the WFH Directive, the telecommunications industry is working on improving network performance following an additional investment of RM400 million for infrastructure and network upgrades as announced in the Pakej Rangsangan Ekonomi Prihatin Rakyat.

Accelerating digitalisation: The need to maintain physical distancing led to many businesses having no option but to adopt digitalisation. The government introduced a few stimulus packages to aid local SMEs to adapt to these changes. Amongst which is the RM1.2 billion PENJANA package which aims to aid the digitalisation of local businesses.

Changes in the job market: The inability of certain business to keep up with digitalisation following the pandemic resulted in the increase of unemployment. This saw the shift from traditional 9-to-5 jobs to gig jobs. This has been further accelerated by the support given by the Government such as incentives involving the welfare of gig workers in PENJANA, with a package of RM75 million. This measure incorporates a coordinating award of up to RM50 million for Gig Economy stages that add to the employees through SOCSO and EPF's I-Saraan, and RM25 million for MDEC Global Online Workforce (GLOW) programmes.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Various regulatory requirements to conduct business in Malaysia often act as barriers to the operation of digital businesses in Malaysia. The stringent licensing regime in Malaysia would be a barrier to digital business operation as entities engaging in commerce which intend to establish corporate presence in Malaysia would have to apply for licences and registrations with various authorities in order to conduct business. Conditions or restrictions connected to the issuance of such licences and registration requirements may also be imposed by the relevant authorities. Such licences and registrations are often interconnected with time-consuming application processes and the requirement for stringent compliance with directorship and equity stipulations by the relevant authorities.

Another barrier would be the slowness of regulatory clock speeds. Too often, technology advances faster than the regulators themselves can develop regulations to deal with the advancements. This leads to a backlog in legislature and stifling of technological development as regulators would need to take time to assess the risk associated with the developments and address the same accordingly in drawing up regulations. This may hinder novel digital business operations where no governing regulatory frameworks are in place.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

The Malaysian Government has strongly advocated the development and utilisation of digital services. Specific agencies and incentives have been instituted to facilitate the development of the digital economy, such as MDEC, which has set up

a Digital Hub with a view to attracting investments in technology, support the innovation of local technology and to form a sustainable digital ecosystem in the country.

The Government has revealed various initiatives to accelerate the adoption of digital technology in Malaysia and to boost the digital economy. One initiative is the “Cloud-First” strategy, introducing a method of faster delivery of information technology services such as data sharing and online transactions in which resources are retrieved from the internet through web-based tools and applications, as opposed to direct connections to servers. Led by MDEC, the Government is also developing a National AI Framework, an expansion of the National Big Data Analytics Framework.

The implementation of the Interoperable Credit Transfer Framework (“**ICTF**”), a policy document issued by BNM under the FSA, has resulted in a boom of ‘e-money’ and ‘e-wallet’ systems in Malaysia, paving the way for the expansion of cashless transactions in the Malaysian economy and interconnectivity of such systems with other digital services in Malaysia. Venturing into the ‘e-money’ and ‘e-wallet’ business will necessitate going through significant regulatory red tape as multiple approvals and/or licences from various bodies may be required for the same.

Following the COVID-19 outbreak, traditional brick and mortar businesses have suffered tremendous losses in operations, with many forced to shut. Opting for digital alternatives such as e-commerce appears to be a more effective way for businesses to mitigate economic losses and to operate in light of the pandemic. Initiatives to facilitate and promote a shift towards e-commerce and the digitalisation of the Malaysian economy are expected to be rolled out in the coming months and years to assist physical businesses to shift towards more e-commerce-based operation models.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The Government officially launched the MyDIGITAL initiative on 19 February 2021, which reflects the aspirations of the Government to successfully transform Malaysia into a digitally-driven, high income nation and a regional leader in digital economy.

The efforts and initiatives required to be taken in order to deliver on the aspirations of the MyDIGITAL initiatives are spelled out in The Malaysia Digital Economy Blueprint (“**Blueprint**”). The Blueprint charts the trajectory of the digital economy’s contribution to the Malaysian economy and builds the foundation to drive digitalisation across Malaysia including bridging the digital divide and the growth of the digital economy.

The Blueprint envisions Malaysia becoming the regional leader in digital economy and aims to achieve inclusive, responsible and sustainable socioeconomic development. The three objectives of the Blueprint are to: (i) encourage industry players to become creators, users and adopters of innovative business models; (ii) harness human capital to thrive in the digital economy; and (iii) nurture an integrated ecosystem that allows society to embrace digital economy.

There are six strategic thrusts under the Blueprint, namely: (i) drive digital transformation in the public sector; (ii) boost economic competitiveness through digitalisation; (iii) build enabling digital infrastructure; (iv) build agile and competent digital talent; (v) create an inclusive digital society; (vi) build trusted, secure and ethical digital environment. These strategic thrusts are supported by 22 strategies, 48 national initiatives and

28 sectoral initiatives. The implementation of this Blueprint will be in three phases. Phase 1 (2021 to 2022) aims to accelerate adoption towards strengthening the digital foundation. Phase 2 (2023 to 2025) focuses on driving digital transformation and inclusion across the digital economy, and Phase 3 (2026 to 2030) will chart the pathway and positioning Malaysia to become a regional market producer for digital products and digital solutions provider.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Apart from the PDPA referenced in question 1.1 above, payment systems in Malaysia are governed by the FSA and the IFSA. The ICTF would also have to be complied with by online payment providers, failing which, enforcement action may be taken by BNM.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Any person who intends to provide merchant acquiring services, such as an online payment provider, is required to register with BNM.

Pursuant to the ICTF, registered merchant acquirers (“**RMAs**”) must ensure that any inter-bank credit transfer transactions are processed in Malaysia through an operator of a shared payment infrastructure. This is to facilitate BNM’s effective oversight of such an operator to maintain the safety and integrity of credit transfer systems and ensure the integrity and stability of the financial system. The ICTF also prescribes certain steps to be taken by RMAs in relation to credit transfer services offered to its customers.

An RMA must obtain BNM’s written approval before entering into an arrangement with a third-party service provider to perform an activity related to the retention and storage of customer data on behalf of the RMA for credit transfer services.

Under the FSA, RMAs are prohibited from, among others: engaging in misleading or deceptive conduct; exerting undue pressure, influence or threatening to use harassment, coercion or physical force in the provision merchant acquiring services; demanding payments from a financial consumer for unsolicited services or products; and colluding with any other person to fix or control the features or terms of payment system services to the detriment of the financial consumer, save where such terms have been approved by BNM.

It should also be noted that under the Foreign Exchange Administration rules issued by BNM, all payments made between Malaysian residents and non-residents must be paid in Malaysian Ringgit for the settlement of trade in goods, subject to limited exceptions.

In addition, electronic transactions are often subject to threat of fraud as customers have to provide credit card and payment account details and other personal information online. As such, it is important for businesses to maintain a secure network and systems and develop security solutions to prevent exposure of the customer’s personal data to potentially malicious third parties to comply with the relevant provisions of the PDPA, amongst other legislation referenced in question 3.2 above.



Joel Prashant graduated with a Bachelor in Law (Hons) from the University of Wales, Aberystwyth and obtained his Certificate in Legal Practice prior to commencing practice as an advocate and solicitor of the High Court of Malaya. He has significant experience in civil litigation, intellectual property, corporate, commercial, TMT, employment, and data protection law, amongst others. Joel's expertise lies in the field of TMT and data protection laws where, throughout his practice, he has advised clients on TMT regulations, implementation of data protection measures, and preparation of a wide variety of documentation for multifarious clients in various sectors, including data protection policies, end-user licensing agreements, terms and conditions and policies for e-commerce platforms, and licensing and distribution agreements. Joel has also been involved in various corporate exercises for foreign and local companies and advised on a myriad of legal issues for clients from various industries.

Shin Associates
Suite B-11-6, Level 11
Wisma Pantai, Plaza Pantai
No. 5, Jalan 4/83A, Off Jalan Pantai Baru
59200, Kuala Lumpur
Malaysia

Tel: +603 2201 5584
Email: joel@shinassociates.com.my
URL: www.shinassociates.com.my



Foo Jia Yi graduated with a Bachelor in Law (Hons) from the University of Hull, UK and obtained her Certificate in Legal Practice prior to commencing practice as an advocate and solicitor of the High Court of Malaya. Jia Yi has experience in a wide range of legal matters including corporate, commercial, banking and finance, technology, conveyancing law, among others. Throughout her practice, she has been involved in various due diligence exercises for both foreign and local companies and advised and drafted contracts for clients from various industries.

Shin Associates
Suite B-11-6, Level 11
Wisma Pantai, Plaza Pantai
No. 5, Jalan 4/83A, Off Jalan Pantai Baru
59200, Kuala Lumpur
Malaysia

Tel: +603 2201 5584
Email: jiayi@shinassociates.com.my
URL: www.shinassociates.com.my

Shin Associates is passionately driven to provide comprehensive legal advisory services across national boundaries and on international platforms. The firm takes fierce pride in its lawyers' abilities to recognise unique traits of each client and to create bespoke solutions for each client. The firm has been ranked as a leading law firm for technology, media, and telecommunications ("TMT") matters in Malaysia by The Legal 500 and awarded the Media & Entertainment Law Firm of the Year in Malaysia for 2017 by Global Law Experts and is also ranked on Media Law International's publication. Since 2016, it has been consistently nominated for various categories for the Asian Legal Business ("ALB") Malaysia Law Awards and ALB South East Asia Law Awards, including Best Boutique Firm of the year, TMT Law Firm of the year, and Transactional Boutique Law Firm of the year. In 2020, the firm was nominated as the Transactional Boutique Law Firm of the year, West Malaysia Law Firm of the year and TMT Law Firm of the year for the ALB Malaysia Law Awards 2020. The firm has also been ranked by Chambers and Partners as a recognised practitioner, and ranked by Asialaw as a notable firm in the Technology and Telecommunications and Intellectual Property practice areas.

www.shinassociates.com.my



Nigeria

Greychapel Legal



Eniola Elegushi



Maryann Ntamere

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

We have provided below some of the key legal requirements applicable (although not exclusively) to B2B ecommerce services, which are contained in different legislations and vary with the nature of ecommerce business/service:

Fintech

Fintech players are required to comply with the regulations applicable to their service offerings. For example, payment solutions and infrastructure providers are required to comply with the Central Bank of Nigeria (CBN) regulations on payment services, as applicable; investment and asset management fintech service providers are required to comply with the Securities and Exchange Commission (SEC) Rules and the Investment and Securities Act; data security and monetisation service providers are required to comply with the applicable National Information Technology Development Agency regulations.

Information Technology

Indigenous information technology (IT) service providers/contractors, including consulting firms, software development companies, and business process operating firms, are required to register with National Information Technology Development Agency (NITDA) in order to deliver information technology services to Ministries, Departments and Agencies of Government in Nigeria. To be considered as an indigenous IT service provider by NITDA:

- a. the company must be registered with the Corporate Affairs Commission (CAC), in accordance with the provisions of the Companies and Allied Matters Act (CAMA); and
- b. Nigerians must hold above 51% of the total issued shares of the company.

Furthermore, cyber companies, internet providers and other specified companies who generate an annual turnover of ₦100 million (One-Hundred Million Naira) and above are liable to pay Information Technology Tax. The tax is governed by the National Information Technology Development Act (NITDA) 2007 and, when paid, is deductible for company income tax purposes.

Data Processors/Controllers

Parties to a data processing contract (other than individual data subjects) are required by the Nigerian Data Protection Regulations issued by NITDA to exercise reasonable measures to ensure that the counter party does not have a record of violating the rights of data subjects and is accountable to NITDA or a regulatory authority for data protection within or outside Nigeria.

Information and Communications Technology Providers

Private information and communications technology companies are required to comply with the National Cybersecurity Strategy Implementation Guidelines 2019 issued by NITDA to safeguard themselves and associated infrastructure for an aggregate national resiliency.

Manufacturers, Importers, Distributors and Suppliers of Goods and Services

These players have a duty under the Federal Competition and Consumer Protection Act 2019 to label goods properly so they can be easily traceable. They also have a duty to withdraw hazardous goods and notify the public in the event of risk.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The key legal requirements applicable (although not exclusively) to B2C ecommerce in Nigeria are drawn from different legislations and vary with the nature of the ecommerce business/service rendered.

The Federal Competition and Consumer Protection Act (FCCPA) 2019, for instance, which scope of application includes the protection and promotion of the interests and welfare of consumers, provides that entities aimed at making profit and geared towards the satisfaction of demand from the public are required to comply with the provisions of the FCCPA 2019. Some of the obligations of an undertaking under the FCCPA include:

- to adequately display the price of goods or services displayed for sale;
- not to knowingly apply to any goods a trade description that is likely to mislead consumers;
- not to enter into a transaction with prices or terms that are unfair, unreasonable or unjust; and

- to ensure that goods delivered correspond to that description or sample agreed with a consumer.

Ecommerce businesses providing payment/financial services are required to comply with the CBN's Consumer Protection Framework 2016. Ecommerce businesses whose service offerings include mobile communications are required to adhere to the minimum set of requirements and standards for the provision of telecommunications services as set out in the Nigerian Communications Commission (NCC) Consumer Code of Practice Regulations 2007.

There are also industry-specific obligations, some of which have been detailed in question 1.1 above.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

With the advancement of technology, the digitalisation of processes around the globe and the consequent increasing value attributed to data, the importance of data protection cannot be overemphasised.

In acknowledgment of the need to develop a comprehensive data protection regime in Nigeria to, amongst other things, foster the integrity of commerce and industry in the volatile data economy, the National Information Technology Development Agency (NITDA), which is the primary regulatory authority responsible for the administration of electronic governance and monitoring the use of electronic data and other forms of electronic communication transactions, issued the Nigerian Data Protection Regulation in January 2019.

The Nigerian Data Protection Regulation 2019 is currently the most comprehensive data protection regulation in Nigeria.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

As with all technological and digital innovations, the greatest privacy challenges faced by fintech, retail, AI and digital health are cybersecurity and data security challenges.

Fintech, retail, AI and digital health solutions are data generators and continue to gain access to and leverage heavily on a vast amount of personal and sensitive data of their customers/data subjects. With the increased digitalisation of processes come the attendant data breaches and cyber-attack challenges. Unfortunately, the inadequacy of some organisations' cybersecurity and compliance programmes make them more attractive targets. Over the past year, there have been numerous incidents revealing the security vulnerabilities of some organisations.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The Government and regulators have, through the formulation of enabling policies and engagements/collaborations with industry stakeholders, facilitated the testing and development of fintech, retail, AI and digital health in Nigeria.

Some of the policies and initiatives are detailed below:

Retail

- a. The Finance Act 2020 which was recently enacted exempts companies with an annual turnover of ₦25

million (Twenty-Five Million Naira) or less from paying Companies Income Tax. Most online retail platforms fall under this category, and will benefit from this provision.

- b. The Companies and Allied Matters Act 2020, in promoting the ease of doing business, now allows for a private company to be set up with a single member.
- c. The Federal Competition and Consumer Protection Act 2019 seeks among others to combat monopoly and unfair market practices thus giving retailers the opportunity to grow and develop their brand.
- d. The Central Bank of Nigeria is constantly rolling out schemes, funds, and special loan packages that are favourable to retailers; particularly in the aftermath of the COVID-19 pandemic.

Fintech

- a. The introduction of various regulations and policies by the Central Bank of Nigeria to facilitate, regulate and/or enhance the adoption of fintech solutions in Nigeria including:
 - the cashless policy aimed at reducing the amount of physical cash circulated in the economy and, accordingly, encouraging electronic-based transactions;
 - the guidelines for the licensing and regulation of payment service banks, which introduced a new category of financial service providers, i.e. payment service banks which leverage technology to, *inter alia*, promote financial inclusion and improve access to financial services in unbanked areas;
 - the guidelines for the operation of treasury single account by state governments which led to the exponential growth of fintech firms like Remita; and
 - the unique biometric identification system for the banking industry – the Bank Verification Number (BVN) – to facilitate the easy identification of customers in the financial system.
- b. The collaboration amongst the Nigeria Inter-Bank Settlement System, the Central Bank of Nigeria and the Financial Services Innovators (FSI), a non-profit organisation, to launch the first fintech industry innovation sandbox – an initiative aimed to support fintech entrants by providing vital information and resources required to commence and scale their businesses in Nigeria.

Artificial Intelligence (AI)

- a. The proposed inclusion of robotics and artificial intelligence in post-basic and secondary education curricula in Nigeria by the Federal Ministry of Education, in order to bring students up to par with 21st century technology and education standards.
- b. The proposed creation of an agency by the Ministry of Science & Technology for artificial intelligence and robotics in a bid to, *inter alia*, increase the level and quality of research in the country and boost the country's GDP.
- c. The partnerships between the Federal Ministry of Communications and Digital Economy and institutions including IBM Digital Nations Africa to enable Nigerians to acquire cutting-edge digital skills on key emerging technologies like blockchain, artificial intelligence, big data and cloud computing within the comfort of their homes.

Digital Health

- a. The organisation of digital health summits by health agencies to encourage collaborations and facilitate connections between stakeholders to transform digital health in Nigeria.

- b. The issuance of the National Health Act 2014 which permits, subject to meeting stipulating requirements, the disclosure by healthcare providers of patient healthcare records to other healthcare providers and third parties.
- c. Contributions by the Nigerian Government to the growing healthcare start-up ecosystem through programmes such as Start-up Nigeria, a three-month incubation programme designed to help Nigerians with great innovative ideas create viable products and gain traction including in the digital health space.
- d. The issuance of the National Office for Technology Acquisition and Promotions policies to strengthen local software development and acquisition of technology that has facilitated the development of digital health.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Cybercrimes Act)

This is the most comprehensive legal framework in Nigeria for the prohibition, prevention, detection, prosecution, and punishment of all forms of cybercrimes. It also promotes cybersecurity and affords protection for computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights. The Cybercrimes Act, to a large extent, addresses the gaps which had hitherto rendered the Nigerian cyberspace unsafe for transacting business and contributes to the expansion of the scope of ecommerce transactions.

With regard to its enforcement, the Cybercrimes Act empowers the Attorney-General of the Federation to make regulations for the general enforcement of the provisions of the Act, including the prosecution of cybercrime cases at the Federal High Court.

Nigeria National Cybersecurity Framework 2019

This Framework was issued by the National Information Technology Development Agency in 2019 to guide public and private sector organisations in instituting measures for enshrining cybersecurity culture and enthrone cyber-resilience in Nigeria.

The Framework outlines the essential security base practices required of, *inter alia*, organisations in both the private and public sectors, and every person that interacts and transacts in the digital domains and boundaries of Nigerian cyberspace.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

a. The Risk Based Cyber Security Framework and Guidelines 2018 for Deposit Money Banks and Payment Service Providers

This Guideline was issued by the Central Bank of Nigeria in response to the increase and sophistication of cybersecurity threats against deposit money banks and payment service providers. The Guidelines stipulate, *inter alia*, the minimum requirements for enhancing cybersecurity and provide guidance on cybersecurity governance, risk management and compliance requirements.

b. The Criminal Laws of the Various States

The criminal laws of the various states in Nigeria also contain provisions on cybersecurity. For instance, the Criminal Law of Lagos State 2015 specifically provides against the unauthorised access to computer material (with or without intent to commit/facilitate the commission of further offences), and the unauthorised modification of computer material (with or without intent to commit/facilitate the commission of further offences).

Upon the receipt of a complaint from a member of the public, the officers of the Nigeria Police Force will conduct their investigations, following which they would cause the person suspected of the offence to be charged to court.

c. The Advance Fee Fraud Act 2006

The Advance Fee Fraud Act specifically provides for electronic communication offences and is enforced by the officers of the Nigeria Police Force, in accordance with the general criminal procedure laws in Nigeria.

d. The Money Laundering (Prohibition) Act 2011

This Act contains provisions empowering the Economic and Financial Crimes Commission (EFCC), Central Bank of Nigeria (CBN), Nigerian Drug Law Enforcement Agency and Securities and Exchange Commission (SEC) to, pursuant to an order of the Federal High Court, obtain access to a suspected computer used in perpetuating money laundering by electronic means. The Act can be enforced by any one of the above-mentioned agencies following the general criminal procedure in Nigeria.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Generally, consumers' attitude towards e-commerce in Nigeria has been positive over time. According to the US Government—Nigeria Country Commercial Guide, ecommerce spending in Nigeria in 2018 was estimated at US\$12 billion and was projected to increase to US\$75 billion in revenues by 2025. It has been reported that Nigeria's growing middle class accounts for approximately 23% of the population and is estimated to have a combined buying power in excess of US\$28 billion. It is further estimated that approximately 63% of the population subscribes to mobile telephones and approximately 48% have internet access, primarily via mobile devices.

These statistics point to the fact that Nigeria has a vast market of consumers who are willing, and financially able, to make purchases online. However, despite these figures, there are certain determinants which have affected attitude to e-commerce over time. For example, e-commerce is more popular amongst the younger generation than the older generation and is widely adopted by the urban demography than its rural counterparts who prefer cash/physical transactions.

However, there has been a lot of sensitisation on the subject, and the implementation of policies, including the Cashless Policy and the Payments Systems Vision 2020 in 2007 by the Central Bank of Nigeria (CBN), to encourage the use of modern technologies and discourage a cash-friendly policy.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The Nigerian Payment Gateways typically support debit card and direct debit payment methods and on limited occasions, the cash on delivery payment method.

The debit card culture is prevalent in e-commerce transactions in Nigeria and indeed has encouraged the entrance of payment service dominant players such as Visa and MasterCard.

Direct debit and cash on delivery methods are classified as alternative payment methods and are usually adopted, where available, by consumers as safer and more secure options than the debit card method. Based on the 2019 report of the World Bank Group's Nigeria Digital Economy Diagnostic Report, 67% of Nigerian shoppers opt for cash on delivery, whilst about 23% use credit cards, with another 10% using mobile payments.

Direct debits are mostly utilised with subscription plans/models. Cash on delivery methods are adopted by vendors to build the trust of consumers in the brand and assure efficient delivery. This payment method, although widely accepted by consumers, has however posed unique challenges for vendors.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

The success of e-commerce platforms in other jurisdictions would depend on a varying number of factors, such as consumer behaviours, enabling laws, etc.

For instance, Jumia, which is arguably one of the largest e-commerce platforms in Africa, initially expanded its operations to about 14 African countries, but Nigeria remains its biggest and core market. Whilst it has had to close its operations in three other countries, its operations in the Nigerian market still thrive.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

The primary language used by ecommerce firms is English. However, most ecommerce platforms adopt the official language of the jurisdictions within which they operate.

For instance, Jumia operates in African countries, spanning both francophone and anglophone countries. The Jumia platforms support the official language of the country in which it operates. Where, however, the official language is other than English, there is the option to translate same from English.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

There are varying evidences to support the fact that the various elements of an online environment impact on consumers' interactivity.

It is, however, established that web interface designs with elements that are predictable, easy to use, access and understand are pleasurable for consumers and may positively impact on their purchasing behaviour.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Yes, the COVID-19 pandemic has had a long-term effect on the cultural norms. For example, following the pandemic, businesses have had to:

- develop and execute holistic digital engagement frameworks to migrate from strictly brick and mortar to digitally enabled platforms;
- create incentives to encourage customer utilisation of these platforms;
- diversify payment options for customers across multiple online platforms; and
- implement cybersecurity frameworks to protect customers.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

The process for online brand enforcement varies with the nature of infringement and includes application to court seeking injunctive reliefs and/or damages.

The Cybercrimes Act establishes a unified framework for the investigation and prosecution of crimes relating to online brand infringement, such as cybersquatting. Actions under the Cybercrimes Act are instituted at the Federal High Court.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

We are not aware of any restrictions on online brand enforcement in Nigeria.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The Nigeria Data Protection Regulations 2019 provides that:

- a. any person (identified as the data controller) engaging a third party to process (and store) data shall enter into a written contract with the said third party; and
- b. the data controller shall also ensure the strict adherence by the third party with the provisions of the regulation.

The risk relating to this is that the data controller may not be in a position to control the third party's actions, which may lead to a breach of the regulations, for which the data controller is ultimately liable.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

The "Guidelines for Nigerian Content Development in Information & Communication Technology 2019", issued by

the NITDA, states that all Government data must be hosted in Nigeria.

The Nigeria Data Protection Regulation 2019 also provides that transfer of personal data to a foreign country or an international organisation shall be subject to the approval of the NITDA and supervised by the Attorney-General of the Federation, save where:

- a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers;
- b. the transfer is necessary for the performance of a contract between the data subject and the controller;
- c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- d. the transfer is necessary for important reasons of public interest;
- e. the transfer is necessary for the establishment, exercise or defence of legal claims; and
- f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

- a. The Oracle Blockchain Cloud Service – which was adopted by the Nigeria Customs Service sometime in 2018 to build an efficient platform for the automation of customs excise processes.
- b. Nigeria Integrated Customs Information System II (NCIS 2) is an enhanced platform of the Nigerian Customs Service aimed at automating clearing processes and enhancing trade facilitation.
- c. The Nigeria Single Window Trade Portal is a cross-government website that creates a single portal for domestic and international trade actors to access a full range of resources and standardised services from different Nigerian government agencies.
- d. Addition by Jumia Nigeria of the “Jumia Global” feature on its website, which enables customers to purchase goods with ease from vendors in other countries.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

- a. Inadequate/unfavourable legal framework to support the adoption of digital technologies.
- b. Lack of requisite technical skill and expertise of stakeholders.
- c. Quality and cost of internet access.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Generally, the tax incentives that apply to businesses in Nigeria are of relevance to digital businesses. These tax incentives include the following:

- i. Exemption from Companies Income Tax: The Finance Act 2020 provides that companies with annual gross turnover of less than ₦25 million are completely exempted from paying companies income tax; companies whose annual turnover is more than ₦25 million but less than ₦100 million are subject to income tax of 20%; and companies whose annual turnover exceeds ₦100 million are subject to income tax of 30%.
- ii. Pioneer Status Incentive: The Industrial Development (Income Tax Relief) Act 1971 provides for Pioneer Status Incentives. A Pioneer Status Incentive is a tax holiday which grants qualifying industries and products relief from payment of corporate income tax for an initial period of three years extendable for one or two additional years. To qualify for Pioneer Status Incentive, the products and services of an applicant must be amongst the list of pioneer industries in Nigeria as provided by the National Investment Promotion Commission, which includes technology companies providing software and ecommerce services.
- iii. Tax Incentives for research and development: The Companies Income Tax Act, Chapter C21 LFN 2004 provides that profit reserved by a company for research and development is tax deductible and such deduction shall not exceed 10% of the total profits of the company for the year as ascertained before any deduction is made. Also, the Act provides that companies and organisations engaged in research and development activities for commercialisation are allowed to enjoy 20% investment tax credit on their qualifying expenditure for the said purpose.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The potential areas of disputes between digital businesses and tax authorities in our view are as detailed below:

- a. **Determining significant economic presence**
The recently enacted Finance Act 2020 provides that the profits of a non-resident company will be subject to tax in Nigeria where it transmits, emits or receives signals, sounds, messages, images or data of any kind by cable, radio, electromagnetic systems or any other electronic or wireless apparatus to Nigeria in respect of any activity, including electronic commerce, to the extent that the company has significant economic presence in Nigeria and profit can be attributable to such activity. Accordingly, dispute may arise in the determination of what constitutes significant economic presence in Nigeria.

b. Enforcement

Digital businesses are technology driven rather than location driven. This reality may make the enforcement of taxation of digital businesses an arduous task in Nigeria, which may ultimately result in disputes between digital businesses and the tax authorities.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

The legal and practical considerations include the following:

- a. The selection process – which should not in any way portray discrimination on the basis of gender, ethnic group, place of origin or religion or other protected category as provided in the Constitution of the Federal Republic of Nigeria 1999 (as amended).
- b. Whether it should be a contract of service or a contract for service – key determinant being the level of control a business may want to exercise over the worker.
- c. The entitlements of a worker, having regard to the applicable laws in force including the Labour Act Chapter L1 LFN, 2004, Pension Reform Act, 2014 and Employee Compensation Act, 2010.

Employment Status Models

From a legal point of view, the status of an employee may be classified into two main categories: the first being employees engaged under a contract of manual labour or clerical work in the private / public sector; and the second being employees who undertake administrative, executive, technical or professional roles. Whilst the Labour Act prescribes the minimum requirements applicable to employments of employees who fall within the first category, the employment of the latter is primarily regulated in the manner as agreed in a contract of employment.

Accordingly, whilst an employee may have a permanent or a fixed status of employment, the minimum requirements of the Labour Act would remain applicable where the employee is engaged under a contract of manual labour or clerical work in the private/public sector.

Furthermore, Nigerian laws relating to employment make no distinction between part-time and full-time employment in its application. Thus, both categories of employees would have similar rights and entitlements under the relevant laws governing the relationship between the employer and employee.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no specific laws regulating remote working in Nigeria. However, in carrying out work away from an organisation's physical premises, the applicable regulations regarding the security and privacy of data must be complied with.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

The COVID-19 pandemic has led to a high maximisation of

technology as employees have had to work from home, and attend meetings and conferences virtually. Thus, the use of tools such as private virtual networks, teleconferencing, instant messaging, business applications and social media has become desirable for sustainability of businesses.

The advantages of working remotely cannot be overemphasised. However, there are certain long-term effects of working remotely, which include the following:

- employees are likely to be more pressured to work over-time without compensation; and
- onboarding of new employees may be a challenge especially in imbibing the organisation's core values.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The key legal barriers faced by digital businesses, as like any other business operating in Nigeria, include the following:

- a. Business registration/incorporation – in order to take advantage of some of the benefits and incentives available to businesses operating in Nigeria, a business must be registered or incorporated in accordance with the provisions of the Companies and Allied Matters Act.
- b. Registration with applicable tax authorities – which is a requirement for every business carrying on business in Nigeria.
- c. Obtaining regulatory approvals/permits – which may be required by the business before it can commence operations in Nigeria, and will depend on factors such as the service/product offering of the business, the composition of its shareholders (i.e. whether the entity has foreign shareholding), whether technology transfer would be made, etc.
- d. Compliance with applicable laws – including data protection and consumer protection laws/regulations.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

The general advantages of operating a digital business in this era of technological revolution are applicable to digital businesses operating in Nigeria; the most notable being that the ecommerce industry in Nigeria shows tremendous potential for growth having regard to its demography, including the high ratio of young adults. According to the World Bank Group's Digital Economy Diagnostic 2019 Report, Nigeria accounts for about 47% of West Africa's population and has one of the largest populations of youth in the world.

Indeed, the opportunities in the digital sector have been widely recognised, considering the significant foreign investments that the Nigerian e-commerce sector has attracted in recent years.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The key areas of focus by regulators in respect of those operating digital business in Nigeria spans across:

- Cybersecurity – organisations operating digital business by their set up have access to private and confidential

information of clients and the loss of control over such information could lead to information theft. To curtail the perpetration of a cyberattack on digital business, the Cybercrimes (Prohibition, Prevention) Act 2015 (Cybercrimes Act) was enacted to punish cybercrime offenders.

- Money laundering – the use of advanced technology in digital business and exposure to private and confidential information of people puts data subjects at the risk of money launderers. As a check on money laundering, the Money Laundering (Prohibition) Act 2011 (as amended) and the Advance Fee Fraud and other Fraud Related Offences Act, 2006 were promulgated.
- Right to Privacy – The right to privacy is a fundamental right enshrined in the Constitution of the Federal Republic of Nigeria, 1999 (as amended). Hence, the protection of the information of clients by digital business organisations is key to regulators. Further to the above, and in an attempt to protect the information of data subjects, the Nigeria Data Protection Regulation 2019 was enacted to ensure the protection of information of data subjects.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The following regulations/guidelines have been issued by the Central Bank of Nigeria (CBN) in relation to online payments in Nigeria:

- a. Regulatory Guideline on Reduction of Chargeback period on transactions using electronic payment channels in Nigeria 2020.

- b. Guidelines on Electronic Payment in Nigeria 2020.
- c. Guideline on Nigerian Payments System Risk and Information Security Management Framework in 2020.
- d. Regulation on Electronic Payments and Collections for Public and Private Sectors in Nigeria 2019.
- e. Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services in Nigeria 2018.
- f. Regulatory Framework for the use of Unstructured Supplementary Service Data (USSD) Financial Services in Nigeria 2018.
- g. Regulation for Direct Debit Scheme in Nigeria 2018.
- h. Guidelines for Licensing & Regulation of Payment Service Banks in Nigeria 2018.
- i. Guidelines on the Operation of Electronic Payment Channels in Nigeria 2016.
- j. Guidelines on the use of Mobile Money Services in Nigeria 2015.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The key legal issues for online payment providers to consider include the following:

- a. licensing by the applicable regulatory bodies including the Central Bank of Nigeria;
- b. compliance with applicable regulation, some of which are detailed in question 11.1 above;
- c. adoption of comprehensive cybersecurity programmes; and
- d. ensuring compliance with applicable data protection laws/regulations.



Eniola Elegushi is a Senior Associate with Greychapel Legal. She holds a Master of Laws Degree in International Commercial Law from University College London and is an alumnus of the prestigious University of Lagos, Nigeria, where she graduated with a Second-Class Upper Degree.

She is an enthusiastic and focused individual who enjoys being part of a successful and productive team. She has a wealth of experience in corporate and commercial law and banking and finance garnered over a number of years and has a good poise under pressure. She is fluent in the English language and has a good command of the French language. She was awarded a diploma certificate in French language by the French Ministry of Education.

She was recently awarded a certificate of recognition by the World Bank in acknowledgment of her contribution to the Ease of Doing Business Initiative in Nigeria. She is a registered capital market consultant with the Securities and Exchange Commission of Nigeria.

Greychapel Legal
17b, Emmanuel Abimbola Cole Street
Lekki Phase 1, Lagos
Nigeria

Tel: +234 80626 55121
Email: e.elegushi@greychapellegal.com
URL: www.greychapellegal.com



Maryann Ntamere obtained her LL.B. Degree from Madonna University, Nigeria, where she finished with a Second-Class Upper Degree. She is a commercially savvy lawyer and a team player with excellent written and communication skills. Maryann is innovative and practical in her approach to dealing with legal issues.

She is a core member of the Business and Regulatory Advisory Practice. She was part of a team that advised a local company on the provision of consultancy and management services to the Government of Edo State of Nigeria.

She routinely provides general legal support to corporate bodies and individuals seeking to achieve compliance with relevant legislation and regulations. She is part of the team currently advising a Nigerian company on a ₦15 Billion Private Sukuk Issuance.

Greychapel Legal
17b, Emmanuel Abimbola Cole Street
Lekki Phase 1, Lagos
Nigeria

Tel: +234 90968 93111
Email: m.ntamere@greychapellegal.com
URL: www.greychapellegal.com

Greychapel Legal is a full-service Nigerian commercial law firm engaged in the delivery of bespoke legal advisory services driven by integrity and excellence. The firm has, over the years, acquired cognate expertise in providing pragmatic advice to various clients in diverse sectors including the corporate, commercial and finance sectors; thereby influencing our recognition and ranking in legal directories including the IFLR1000 in the years 2019 and 2020.

We currently act for some of the major players in the e-commerce sector including the fintech and digital health spaces. We pro-actively develop and adopt pragmatic legal strategies to match our clients' innovative minds in managing their legal risks.

We have consistently maintained good working relationships with regulatory agencies such as the Corporate Affairs Commission, the Securities and Exchange Commission, the Central Bank of Nigeria, the Nigerian Investment Promotion Commission, amongst others. We are also licensed by the Securities and Exchange Commission to advise on capital market transactions.

www.greychapellegal.com



GREYCHAPEL
LEGAL

Romania



Alexandru
Stanescu



Andrei Pelinari



Stelian Mic



Tudor Velea

Mic, Ilie & Asociații / Pelinari & Pelinari / SLV Legal

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

Romania transposed within its national legislation all the EU e-commerce directives, regulations and guidelines which apply to B2B e-commerce.

The Romanian market is quite new when talking of e-commerce mechanics, both in terms of standardised agreements and lay-outs and presentation. Thus, most Romanian websites are purely for presentation only, rather than structured as online shops or for commercial purposes. However, lately, marketplace retailers and the food delivery industry have experienced a rapid and massive development.

As a way of background, e-commerce services are not subject to any prior authorisation and are carried out in accordance with the principles of free and fair competition and free provision of services.

A game-changer in e-commerce B2B relationships is the Regulation (EU) 2019/1150 (“**P2B Regulation**”), which regulates the commercial relationship between providers of online intermediation services and business users listed on the marketplace. In terms of fairness and commercial transparency, a business that provides online intermediation services has the obligation to provide business users with clear, unequivocal and easily accessible information on: (i) grounds for decisions to suspend, terminate or impose any other kind of restriction upon business users; (ii) the effects over the ownership and control of the business users’ IP rights; (iii) any proposed changes of the terms and conditions – this shall also be notified to each business user within at least 15 days prior to the entry into force of such amendments; (iv) ranking mechanics and the possibility to influence ranking; (v) any ancillary services offered to the consumer immediately prior to the completion of a transaction initiated on online intermediation services to complement the primary good being offered by the business user; (vi) information on treatment and ranking of goods or services offered by themselves or by business users they control compared to third-party business users; (vii) access to data; (viii) restrictions to offer different conditions through other means; (ix) internal complaint-handling system in relation to business users; and (x) mediation as a settlement method in relation with business users. It is to be noted, however, that most of the information duties in B2B e-commerce can be waived or differently agreed between the parties as long as none of them is a consumer.

In order to ensure the application and observance of the P2B Regulation at national level, the Romanian Government has adopted GEO 23/2021 on measures to implement P2B Regulation. For ease of reference, non-compliance by providers of online intermediation services with the provisions relating to: (i) procedures and deadlines for amending the terms and conditions; (ii) the procedures, deadlines and justification for restricting, suspending or terminating the provision of services; (iii) ensuring transparency on ranking; (iv) ensuring transparency on differential treatment; (v) making retroactive changes to terms and conditions; (vi) ensuring transparency on data access; and (vii) ensuring transparency on data restrictions on the provision of different conditions by other means, represent administrative offence and are sanctioned with a fine between 0.1% to 1% of the turnover achieved by the provider within the previous financial year.

Supplementary, PSD2 is also directly applicable in Romania; therefore, all merchants need to analyse if their business model involves a requalification risk as a payment services provider, scenario when a specific licence for payment services will be necessary. Therefore, when the payment is done via a credit/debit card through the e-commerce platform/marketplace, it should be analysed if the funds are collected by the platform/marketplace and then distributed to the vendors listed on the platform, or such distribution of funds is done directly by the payment services provider. Supplementary, it should be noted that according to the provisions of PSD2 and article 4 of Law 209/2019, the commercial agent exemption applies only if the platform operator has only a “one side mandate” either from the seller or from the purchaser, not from both of them (the latter being the scenario applicable to most marketplaces).

In recent years, and further pushed by the advent of the COVID-19 pandemic, the Romanian business environment tried to determine law-compliant ways to conclude and execute B2B agreements in electronic form. In Romania, e-contracts produce all the effects recognised by law for standard hard copy contracts, only if such agreements are signed with an extended electronic signature having attached a qualified certificate (the sole equivalent in Romania of a handwritten signature). Several businesses have tried to implement a mechanism that allows the simple use of a service by “ticking” a box on a web page that refers to that specific service, to constitute valid consent of concluding an agreement. However, the local legal system did not evolve in the direction, where the simple use of a service does give rise to a valid contract between the parties regarding such service, as the buyer, via its legal representative, must unequivocally express his acceptance of the use of the service, mainly due to the fact there is no clear mechanics to ensure that the person “ticking” the box or using the service is the actual

legal representative of the business, with authority to bind it contractually. Such system of acceptance can be implemented only in B2C e-commerce, as there are specific legal provisions regulating this approach.

When referring to specific areas of e-commerce, Romania has greatly benefitted first from the EU Directive 633/2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain which is expected to be transposed nationally May 1, 2021. This came as a response to the significant imbalances in bargaining power between suppliers and buyers of agricultural and food products, aiming to impose an EU standard of protection against unfair trading practices and hence to reduce behaviours that grossly deviate from good commercial conduct, break good faith and fair dealing practices or attempt to impose unilaterally terms and conditions to the party in the weakest position.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Similarly to B2B, Romania transposed within its national legislation all the EU e-commerce directives, regulations and guidelines which apply also to B2C e-commerce.

The national entity that ensures the observance of consumers rights is the National Authority for Consumer Protection (“ANPC”) and under certain conditions, the authority has, in the exercise of its duties, an active procedural capacity for triggering legal action in matters related to consumer protection.

Regarding the requirement to inform the consumer, article 6 of the G.E.O. no. 34/2014 provides that before an e-contract produces binding effects on the consumer, the business must provide the consumer with the following information in a clear and intelligible manner: (i) main characteristics of the products/services; (ii) address to which the consumer may send any complaints; (iii) total price of the goods and services with all taxes included or, if they cannot be reasonably calculated in advance, a statement that these additional costs could be borne by the consumer, including the period of validity of the offer or prices; (iv) the methods of payment, delivery, execution, the date until which the professional undertakes to deliver the products or to provide the services and, as the case may be, the procedure of the professional for solving the complaints; (v) in case there is a right of withdrawal, the conditions, terms and procedures for exercising the respective right; and (vi) a statement regarding the existence of a legal guarantee regarding the conformity of the products, etc.

The consumer also benefits from a period of 14 days to withdraw from an e-contract, without having to justify the withdrawal decision. If the business did not transmit to the consumer the information regarding the right of withdrawal, the withdrawal period expires 12 months from the end of the initial withdrawal period of 14 days. However, the G.E.O. no. 34/2014 provides the consumers do not benefit from the right of withdrawal for: (i) products that are likely to deteriorate or expire rapidly; (ii) sealed products that cannot be returned due to health protection or which have been unsealed by the consumer; and (iii) products which, after delivery, are by their nature inseparably mixed with other elements, etc.

The general rule is that the seller is liable to the consumer for any lack of conformity existing at the time the products were delivered. In case of non-conformity, the consumer has the

right to request the seller to bring the product to conformity, free of charge, by repair or replacement, to benefit from the corresponding price reduction or termination of the contract for such product.

In respect of reimbursements, the seller will reimburse the value of the products and delivery costs using the same payment methods as those used by the consumer for the initial transaction, unless the consumer has agreed to another payment method. The seller may defer the refund until the date of receipt of the products or until the time of receipt of proof from the consumer that products were returned, considering the nearest date.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Regarding the legislation applicable at local level, in Romania there has been no changes in the last year. The internal law, which establishes some specific provisions in the field of data protection, respectively Law no. 190/2018 on measures to implement the EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, has not changed since 2019.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

In the areas of fintech, as well as artificial intelligence and digital health, implementing and enforcing regulatory norms is often difficult due to the time disparity between the issuance and update of laws and the speed of tech advancements and increasing needs of their beneficiaries.

Besides legislative voids, one of the most important challenges that organisations are facing is human error, resulting both in financial losses and leakage of personal data.

In the field of fintech, the matter of payment services providers, e-commerce platforms and the access of the often poorly informed public to these instruments, are being supervised by the National Authority for the Supervision of Personal Data Processing resulting in more and more sanctions applied for security incidents (either caused by the mismanagement of IT systems or by employees/representatives of operators).

For AI, the private companies working in the market are often a support for the national authorities, rather than the opposite, due to unclear, untimely or voids of the law protecting personal data. The National Agency for Payments and Social Inspection (“ANPIS”) had recently received the help of a software robot that helped process the increasing e-payments request during the state of emergency generated by the COVID-19 crisis.

Regarding health, the core issues revolve around the right to digitally access medical data and to decide if and when to communicate this data, as well as the issue of health literacy disparity in a digital context.

Currently, most procedures require the beneficiary to submit their requests personally. Digital tools that use and process personal data are protected by GDPR, which allows patients to have control over the use of their medical data. As for how digitalisation could look from a data protection standpoint, the European Economic and Social Committee issued in 2018 a point of view on the matter, establishing the importance of distinguishing between data types, namely, raw data, and data

generated by algorithms or artificial intelligence services. Under GDPR, the rights of use, access and distribution of digital medical data would remain a patient prerogative, as long as that data is introduced by the patient itself. The questions still to be answered concern the rights over and management of such data, when entered, altered, or supplemented by an algorithm or AI tool.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Since 2015, the national authorities have issued a National Strategy on the Digital Agenda, to be implemented until 2020, covering four main areas: (i) e-Government, interoperability, cyber security, cloud computing and social media, with the purpose to increase efficiency and reduce costs in the public sector through digitalisation of the administration; (ii) IT&C in education, health, and culture; (iii) e-commerce, research-development and innovation in IT&C, more oriented towards the private sector; and (iv) broadband and digital infrastructure services – an area aimed at ensuring the conditions of access to IT&C equipment, to increase digital literacy and improve digital skills. An update of the agenda for 2021 is expected to be issued.

For fintech, the Financial Supervisory Authority has created the FinTech Hub, available on its website, to work as an institutional framework for dialogue with companies developing in the financial market. In addition, Law 209/2019 on payment services covers the areas of PSPs, e-wallet providers, e-money and licences, under the scrutiny of the National Bank of Romania, who issues regulations and guidelines on the applicability of the law and has monitoring and supervision authority. It is currently possible for businesses to request an opinion from both ASF and NBR regarding the applicability of exemptions or the authorisation requirements for fintech entities.

The national authorities have shown increased interest in recent years, regarding the topic of digital health, although the EU laws and regulations are still one step ahead of the local ones. Through the National Strategy on the Digital Agenda, so far, Romania has implemented the following IT systems specific to the medical sector: (i) Single Integrated System (SUI); (ii) Classification System by diagnostic groups (Related Diagnostic Groups – GDI); (iii) Electronic Prescription System (RE); (iv) Health Insurance Card System (SCAS); (v) Electronic Patient Record Management System; (vi) SMURD – ambulance requests; and (vii) telemedicine for rural areas.

Although a wholesome instrument allowing the collection and access to the patient's own medical history, digital/remote health prevention, evaluation and treatment of the patient has yet to be implemented nationally, one of the most important steps made in this direction was taken in the context of the global pandemic. The creation of a national digital platform for booking a vaccination against COVID-19 currently allows the users to make a vaccine appointment online.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

Any key digital service provider, be it an online marketplace, a search engine or a cloud computing service, is subject to strict requirements meant to secure their informatic systems and the data involved. Such requirements have been introduced

by Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the “NIS Directive”), which is the first horizontal legislation addressing cybersecurity challenges and a true game changer for cybersecurity resilience and cooperation in Europe. At local level, requirements have been implemented by underlying transposing laws of the Member States. In Romania, the NIS Directive was transposed through Law no. 362/2018 for ensuring a high common level of security of networks and information systems, further updated and supplemented (the “NIS Law”); for more information on national improvements, see below at question 3.2.

E-commerce business is referred to under the NIS Directive as “online marketplace”, meaning a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders, either on the online marketplace's website or on a trader's website, which uses computing services provided by the online marketplace. Online marketplaces are a type of digital service (i.e. expressly included in Annex III to the NIS Directive), and the professionals carrying out e-commerce businesses are digital service providers bound to implement appropriate technical and organisational measures, as well as notification procedures, in order to manage the risk posed to the security of network and information systems used in running their businesses. E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach.

Although seen as separate from the vital sectors where security measures are paramount for worldwide economy and society (briefly, the essential services are health, energy, water, financial market infrastructure, banking, transport, digital infrastructure), some digital services have fallen under the spotlight due to the large number of users relying on them, the dependency of other sectors on them, the impact that incidents could have in terms of degree and duration, and the geographic spread with regard to the area that could be affected by an incident. A disruption of a digital service could prevent the provision of other services which depend on it and could thus have an impact on the participation of such businesses in the internal market and cross-border trade across the EU.

In this context of increased digitisation of the internal market in recent years and the evolving cybersecurity threat landscape, the proposal of a second NIS directive which builds on the current NIS Directive was presented in December 2020.

While, in what concerns the operators of essential services, Member States are expected to identify and report the relevant operators, and even impose stricter requirements than those laid down in the NIS Directive, they are not expected to identify digital service providers, as the NIS Directive applies to all digital service providers within its scope, respectively all providers except small and medium enterprises within which implementing the security measures would prove disproportionate by reference to the risks presented by the network and information systems concerned. The qualification as a digital service provider is made through self-assessment.

The two main requirements for e-commerce businesses envisage (i) ensuring the security of the network and information systems which they use, given that these are primarily private networks and the information systems are managed by their internal IT staff or are outsourced (e.g. the use of HTTPS protocols and SSL certificates, the monitoring of transactions and periodic back-ups, firewalls, public key infrastructure, encryption software, digital certificates, etc.), and (ii) compliance with the notification obligation in case of a cyber-incident, with a view to establish the continuity of those services. Regardless of whether the maintenance of the network and

information systems is managed internally or is outsourced, the above requirements apply.

A detail worth mentioning is related to the impact of a cyber-incident on the end users: after notification of the competent authority by the digital service provider concerned (or by a competent authority from another Member State), they consult each other on whether to inform the public about individual incidents in those cases when it is necessary to prevent an incident or to deal with an ongoing one, or simply when disclosure is of public interest. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the digital service providers reporting incidents.

As anticipated in the paragraph above, the security of information in e-commerce businesses is deeply linked to the protection of personal data, given that computing services provided by an online marketplace may include processing of transactions, aggregations of data or profiling of users. Personal data are, in many cases, compromised as a result of cyber-incidents. In this context, competent authorities in both cybersecurity and data protection are expected to cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The NIS Law (defined at question 3.1 above) has recently been heavily supplemented by methodological norms and secondary laws, *inter alia*, the Government Decision no. 963/2020 on the approval of the list of essential services in Romania, the Government Decision no. 976/2020 on the approval of threshold values for establishing the significant disruptive effect of incidents on the networks and computer systems of essential service operators, and the Decision of the National Cyber Security Incident Response Center no. 88/2020 on the approval of the list of European and international standards and specifications.

These newly enacted provisions are a consequence of Romanian authorities' attempt to avoid sanctions applied by the European Commission for Romania's failure to notify in due time the national measures taken for the implementation of the NIS Directive. In October 2020, the European Commission issued an opinion regarding Romania's progress in applying and reporting the developments on the matter, which proved quite inadequate, triggering a two-month deadline for remedy.

The NIS Directive provides that Member States must adopt a strategy on the security of networks and information systems whereby strategic objectives and appropriate policy and regulatory measures are outlined in order to achieve and then maintain a high level of security. In Romania, forecasts and efforts to enhance national cybersecurity were adopted through the Government Resolution no. 271/2013 for the approval of the Cyber Security Strategy of Romania and of the Action Plan at National Level.

In terms of implementation and enforcement of the NIS Law and the strategy on cybersecurity, the competent authority in Romania in matters of cybersecurity is the National Authority for Security of Networks and Information Systems ("ANSRSI"). This institution is in close cooperation with the national law enforcement authorities and the National Supervisory Authority for Personal Data Processing, the data protection competent authority. As required under the NIS Directive, Romania has

also designated the computer security incident response team ("CSIRT"): CERT-RO (abbreviation from *Centrul National de Raspuns la Incidente de Securitate Cibernetica*), which handles the local implementation and incident administration pursuant to the NIS Directive.

In addition to sanctions imposed by the supervising authorities for breaches of security requirements, court decisions issued in civil cases based on tort and decisions in criminal cases related to cybersecurity can intervene following actions filed against the person who committed a cybersecurity offence and/or against the entity responsible for the security system that was breached and is deemed liable.

Digital service providers are subject to *ex post* supervisory activities performed by ANSRSI – usually after an incident occurs. When there are suspicions of failure to meet any of the security requirements, the implementation of the NIS Directive is made through requests addressed to the digital service providers to make available information needed to assess the security of the network and information systems, while in case of evidence that a certain requirement is not complied with, the supervising authority takes action directly by requesting the remedy of that requirement.

Companies in Romania have started to put in place insurance policies against security breaches, given that the insurance market promotes products dedicated to such incidents and no legal provisions prohibit or limit insurance coverage against types of loss from business interruption, system failures or digital assets restoration.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In Romania, e-commerce has started to develop relatively late compared to other European countries due to the late adoption of electronic payment instruments. Romania has less than one bank card per capita, one of the lowest values in the European Union, due to the preference for cash payments. Romanian consumers continue to prefer the use of cash, but this habit is steadily declining especially with the necessity to avoid cash payments during the COVID-19 pandemic; the National Bank of Romania registered a significant increase in the total number of credit cards in 2020. Statistics show that there is an increasing number of consumers using new payment technologies, contactless payments and increasingly using smartphones to purchase online.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The number of credit card transactions increased by 9.6% compared to the same period last year. The value of transactions increased by 9.3% at the end of the second quarter of 2020, compared to the similar period last year. The transition to cashless and contactless is a trend that has intensified in recent years amid the digitalisation of banking services, but has been accelerated during the pandemic. As an additional measure to ensure health, banks have recommended that people make

cashless payments through modern means of payment provided by them, such as cards or online payments. Credit institutions in Romania are actively contributing to the acceleration of the introduction of digital solutions in banking financial services and are concerned with redefining business models through new innovative services.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Home state retailer websites perform well in Romania. The most sold products and services on e-commerce websites in Romania are technology products and, increasingly, second-hand products (thanks to the increasing number of second-hand sale apps and websites). Indeed, such products and services target a huge number of potential consumers, and not only a particular sector of the Romanian population.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Very few e-commerce websites are available in both Romanian and English, as they have not overcome the language barriers yet. The survey of Romania's most popular and largest online stores shows that most do not provide for the option to change the language. Usually, online stores in Romania target local customers with very few exceptions.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

E-commerce websites constantly try to improve the users' experience through intuitive use, nice and clean graphics and faster browsing. Surveys show that Romanian consumers take into account online reviews in order to decide where to buy. Most online retailers use tracking tools to analyse consumer behaviour so as to provide convenient services for consumers. Online retailers strive to give accurate information on the product with pictures and reviews. The Romanian consumer is discerning and prefers solid brands and e-commerce websites to typically display the brand logo for the consumer to notice it. The delivery policy is equally important, and an increasing number of websites offer free delivery with the option to pay for the items once they are delivered. Customer service experience is also important with the possibility to return unsatisfactory products without hassle.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The 2020 pandemic has had an important role in attracting more consumers to acquire their goods online. Successive lockdowns and health measures have forced consumers to resort to online purchasing of staple products and services. The trend will most likely continue. According to a survey by ARMO (the Romanian Association of Online Stores), online commerce in

Romania reached the threshold of EUR 5.6 billion at the end of 2020, representing an increase of 30% compared to 2019. The increase was approximately EUR 500 million over initial forecasts, amid the COVID-19 pandemic that has accelerated the pace of online shopping, as well as the percentage of online card payments.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Generally, violations of exclusive rights and trademarks are solved by the courts. According to law 84/1998, as amended in 2010, it is a crime punishable by imprisonment from three months to three years or by a fine from EUR 10,000 to EUR 30,000 to counterfeit a trademark or to sell counterfeit goods. In addition, according to law 11/1991, it constitutes a crime and is punishable by imprisonment from three months to two years or a fine where a trademark or a packaging is likely to cause confusion with the products legitimately used by another trader. In reality there are very few enforcement cases and some counterfeit products are sold in Romania but on a small scale and usually through secondary sale websites such as OLX or eBay. In addition, decree number 21/1992 allows for tougher sanctions in the event that counterfeit products affect the public health or endangers the consumers in any way.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

There are no preventative measures to directly impede online sales of counterfeit products. Article 84(1) of law 84/1998 allows the authorities to seize counterfeit products on the spot and apply a sanction whether pecuniary, penal or both (typically the sanction is just a fine).

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Cloud computing technology is one of the most advanced internet-based technologies nowadays, as it became a fact of everyday life for many businesses; however, everyone needs to know that it creates many legal issues that can lead to problems if not handled proactively. Nearly every business that uses computers, in industries including social media, financial services, healthcare and software, is itself a consumer of cloud-based solutions which creates unprecedented risks.

Cloud computing services span a wide range of activities that can be delivered according to different models. The term 'cloud computing services' covers services that allow access to a scalable and elastic pool of shareable computing resources which include networks, servers or other infrastructure, storage, applications and services.

When entering into negotiations with a cloud service provider, one of the first steps to consider is the due diligence of the provider of cloud services, a process which can be important for both customers and business partners in light of the potential inability to significantly influence the contract terms. Such process should serve to clarify the operational history and reliability of the supplier, data location, portability and back-up

of information, as well as compliance with technical security standards. Companies know very well that the provider's client can hold personal data relating to its customers on the cloud, and therefore, the client will be likely to require a higher privacy standard and guarantees before entering into any transaction.

The legal risks that can arise "in the cloud" include, briefly: (i) liability for copyright infringement; (ii) data loss and data management; (iii) data breaches and portability of data; (iv) privacy and HIPAA violations; (v) hacking and cybersecurity; and (vi) shared resources and multi-tenancy, as well as many other similar complex issues that can lead to regulatory debates and litigation in matters of civil law that lay itself open to strategic choices as for the *forum* choice or for the choice of alternative dispute resolution mechanisms. This is made even more complex by geographical issues, since cloud services usually involve extra-territorial entities; this would make any form of transnational litigation prohibitively costly with the consequent likelihood for the client to be somehow forced to withdraw his claims.

Out of the above, we would discuss for the purpose of this material, the matters related to data privacy, the applicability of the European General Data Protection Regulation 2016/679 (GDPR) being one of the most important issues to be borne in mind when thinking about cloud computing. In fact, if the data processed by the cloud provider is "personal data" in the sense of the GDPR, and it is related to EU citizens, the provider would need to be compliant with the EU privacy regulation even if its servers or its headquarters are located abroad – which actually is the case of most famous cloud providers located in the US (e.g., Microsoft, Amazon, IBM).

There are opinions that argue that "data encrypted and secured to recognized standards should not be considered 'personal data' in the hands of those without access to the decryption key" since they only grant the "utility infrastructure services". Pursuant to this theory, all the European privacy implications such as data anonymisation, sharing of fragmentation data and encryption will not apply to cloud providers that do not have access to decryption keys. On the other hand, excluding the applicability of the GDPR without sufficient grounds, the above could turn into a delicate and possibly dangerous decision, not only due to possible fines that may go up to €20 million or 4% of the worldwide annual revenue (whichever is higher), but also for the reputation of the company. In addition to this, another risk is related to the costs that a company might suffer as a consequence of data breach within the cloud. In fact, not only the company would have to declare the breach to the supervisory authority, but also to the data subject.

A second very important issue concerns security. Due to its distributed nature, the cloud results in weak security systems that are easy to break into. In simpler words, the security of the system is only as strong as the weakest user's set-up, given that any breach of security spreads across all participants. In cloud computing, a company's data is locked-in and the third party in control.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Companies are concerned about the physical location of their data that are stored in the public cloud. The laws of the host country of the equipment apply to the data on the machines. In 2020, only around 15% of the Romanian companies outsourced cloud services to professional providers, which places Romania below the European average on this matter.

Besides the relevant provisions in the Romanian Law no. 190/2018 on measures for the implementation of Regulation

(EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (briefly referred to at question 6.1 above), the Romanian Supervising Financial Authority ("ASF") issued Norm no. 33/2020 regarding the outsourcing to cloud service providers (the "Norm").

In terms of authorisation and outsourcing of servers/data centres in Romania, the Norm is expressly supplemented by some of the provisions of Law no. 237/2015 on the authorisation and supervision of the insurance and reinsurance activity, provisions which become applicable in the context of outsourcing to cloud service providers and collaboration between supervising authorities.

Cloud storage is often deemed a critical or significant function or activity or a development in the functions or activities of a company, thus its outsourcing should be made so as to avoid: (i) significant deterioration in the quality of the governance system; (ii) significant increase in operational risk; (iii) the inability of the ASF to monitor how companies comply with their obligations; or (iv) discontinuities in the provision of quality services to contractors. When outsourcing activities or functions, companies remain responsible for compliance with legal provisions.

No express provisions on the authorisation of cloud service providers; however, requirements can be extracted from the provisions imposing certain standards of outsourcing under an outsourcing agreement. A company must assess the risk profile of a service provider, particularly taking into consideration the following: the ICT risk; the risk regarding the continuity of the activity; the legal risk; the compliance risk; the risk of concentration; the operational risk; and the risk associated with the data migration phase and/or the implementation phase, as the case may be. In order to be able to prove compliance to the above, the company may use certifications based on international standards, audit reports of recognised third parties or internal audit reports, as well as other documents that can demonstrate the performance of a complex assessment.

The notification obligation provided by Law no. 237/2015 on the authorisation and supervision of the insurance and reinsurance activity is applicable on the companies when outsourcing cloud services as well. The written notification must include at least the following information: a short description of the outsourced activity; why such activity is deemed critical or significant; the start date; the renewal date of the outsourcing agreement; the termination date and notice periods; the applicable law to the outsourcing agreement; the name, registration number, fiscal code, address, other contact detail of the service provider; the name of the mother-company of the service provider (if the case); and, in case the service provider is part of a group of companies, the name of the group and main establishment. In addition, the notification must comprise the services and the models that will be used (e.g., public cloud, private, hybrid, community), as well as the data that is intended to be stored and their locations.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Beforehand, in the context that Romania has been an EU Member State since 2007, the Romanian government border agencies have undertaken efforts to ensure that community

customs obligations are fulfilled, including from the standpoint of digitalising international trade customs regulation.

Therefore, the Directorate-General for Customs (“**DGC**”), responsible for Romanian trade controls, has already implemented digital trans-European centralised systems, developed in accordance with the functional and technical specifications of DG TAXUD, for instance ECS – RO, ICS – RO, EORI – RO, TARIC – RO, via the E-CUSTOMS platform.

In regard to the governmental actors increasing the efforts toward digitalisation, as of April 2021, the National Agency for Tax Administration (“**ANAF**”) offers the possibility of electronic registration in the One-Stop Shop – OSS (Special VAT Regime) system, which will become fully operational starting from July 1, 2021.

The OSS system provides an opportunity for private enterprises to stop registering and reporting VAT in each of the EU Member States where they owe VAT, but to benefit from electronic services to fulfil these obligations through the Member State of Identification.

By implementing this system, Romanian authorities aim to decrease the administrative burden for business by simplifying the VAT reporting and payment procedure (B2C), facilitating cross-border trade and combatting VAT fraud.

In addition, the Authority for the Digitalization of Romania (“**ADR**”) has developed the Strategic Framework for the adoption and use of innovative technologies in public administration 2021–2027 – solutions for streamlining the activity of the public administration.

Among the objectives to be carried out within the project, there is the development of the national strategic framework in the field of artificial intelligence, and the analysis and updating of legislation in blockchain technologies, artificial intelligence, EOSC, EuroHPC and PRACE, in keeping with European standards.

This project creates the prerequisites for developing a technology of distributed blockchain registries in order to verify certificates of goods’ origins and any other relevant information, and therefore facilitate an end-to-end visibility of the international trade supply chain.

Lastly, in respect to the import side of the international trade, private enterprises from foreign states, by establishing international consortiums with Romanian enterprises, can participate in public procurement procedures of goods and services entirely through a digital platform, specifically SICAP. In order to comply with the EU Directives on e-invoices, the European standard regarding new taxation system and e-invoice has been transposed into Romanian legislation by Law No. 199/2020, nevertheless the scope of applicability of this law is restricted to public procurement and public works, in the interim.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Of course, there are a series of obstacles regarding trade facilitation via adoption of digital technologies, such as the more or less inevitable dose of scepticism about new technologies, in general, in a state where the trend of digitalisation has emerged rather recently.

However, any obstacles or scepticism can be efficiently surpassed and/or countered by the authorities through the medium of adopting predictable and comprehensible regulatory measures and policies, engaging staff with special expertise, making sure that all electronic systems operate properly and so on. Consequently, the newly adopted technology must match the specific needs and requirements of its users, to ensure that the final result represents a real and concrete benefit to international trade, such as reduced customs time and administrative costs, and at the same time minimising the risk of non-compliance from the enterprises.

Although the process of further digitalising customs administration implies a certain financial burden for the public authorities, Romanian authorities, such as ANAF and ADR, have shown great interest in following the trend of digitalisation, one of the administration’s top priorities at this time, as well as in the foreseeable future.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

There are several tax incentives in Romania that could be accessed by digital businesses.

Taxation of newly established companies and micro-enterprises
Corporate profit tax rate applicable in Romania is 16% applied to the taxable base, which is computed as the accounting profit adjusted for tax purposes (special rules apply in case of non-taxable income and non-deductible expenses).

However, newly established companies as well as existing Romanian legal entities having a turnover of up to EUR 1 million, are subject to 1% or 3% tax on income.

Incentives in case of research and development (R&D) activities
For companies subject to profit tax, for R&D activities from the applicative research and/or technological development categories, relevant to the activity of the company (that meet the definition provided in the Romanian legislation), specific incentives can be applied (i.e. supplementary deduction of 50% of the eligible expenses, accelerated depreciation for equipment used in R&D activities).

Companies that carry out exclusively innovation and R&D activities, as well as related activities, are exempt from corporate profit tax in their first 10 years of activity.

Incentives in case of reinvested profit
For companies subject to profit tax, profit reinvested under certain specific conditions is exempt from profit tax (e.g. profit reinvested in technological equipment, computers and peripheral equipment, other equipment for petty cash, control, invoicing, software, used for the purpose of the company’s economic activity).

Tax credit for sponsorship and scholarships
Tax credit is granted to companies that have incurred expenses with sponsorships and scholarships, under certain conditions and thresholds.

Personal income tax exemption for IT specialists

Employees working as IT specialists for companies deriving income from software creation, may benefit from an exemption for the 10% personal income tax applied on salary income, in certain conditions detailed under the Romanian legislation.

Personal income tax exemption for employees working in R&D and innovation

Employees part of a R&D and innovation team, working for an R&D and innovation project, may benefit from an exemption for the 10% personal income tax applied on salary income, in certain conditions detailed under the Romanian legislation.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Main disputes with tax authorities in case of tax audits could be seen in the areas of calculation of the taxable base, observance of transfer pricing rules and application of tax incentives, if the case.

Calculation of taxable base, in case of companies paying profit tax

Main disputes here refer to meeting the formal conditions for deduction of expenses. For deduction of expenses with services, companies need to have available contracts and proper back-up documentation to sustain that the services were actually provided for the benefit of the economic activity of the company.

Transfer pricing rules

Transfer pricing is a topic approached by the tax authorities regularly in case of audits on companies having transactions with both domestic and cross-border related parties. Digital businesses are even more exposed, as they deal with unique transfer pricing challenges (the allocation of functions, risks and assets involved in the intra-group transactions not being easily determined, due to the specifics of the business), which at this point in time are not settled by OECD guidelines.

However, until new international guidelines are issued, a proactive preparation of a transfer pricing policy (based on solid economic reasoning), followed by preparation and annual updates of the transfer pricing file, can mitigate potential risks of adjustments in case of tax audits.

Meeting the conditions for the application of the tax incentives

Main disputes that arise between taxpayers and tax authorities in case of digital companies refer to the application of the exemption for personal income tax for employees working on software creation. The legislation sets up special conditions, including formal conditions, that need to be observed by the companies in order to be able to apply the exemption.

Anti-abuse rules

Under the general anti-abuse rule provided under the Romanian legislation, in determining the amount of a tax, duty or mandatory social security contribution, the tax authorities may disregard a transaction that has no economic substance, adjusting its tax effects, or may reclassify the form of a transaction/activity to reflect the economic content of the transaction/activity.

In case of digital business, the business model can include extended collaboration with freelancers or micro companies. Main disputes that can arise here between taxpayers and tax authorities refer to risk of reclassification of such contracts to employment contracts (this leading to significant additional taxation).

Companies need to make sure that the independence of the collaborators is clear and unlikely to be contested in case of a tax audit. Guidance is provided here in the tax legislation, i.e. contractors are deemed as independent if specific criteria mentioned in the legislation are met. However, even if the criteria are met, tax authorities can apply the general anti-abuse rules if they have evidence that the economical substance of the contract is that of an employment contract and not of a collaboration contract.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In the case of employment contracts, the Romanian legislation can be characterised as one that ensures a fair balance between the interests of the employer and those of the employee.

The current Romanian regulations provide employees with relatively increased job security and working conditions, respectively (i) notice period for dismissal of minimum 20 working days, (ii) in the case of dismissals, the employer does not have absolute freedom and must comply with certain conditions provided by the law (for example, there must be a well-justified reason for dismissals), and (iii) daily/weekly/annual rest breaks are expressly regulated representing rights of the employee that must be strictly observed by the employer.

At the same time, in Romania, employers also have (i) a great deal of flexibility in determining and transferring the tasks of employees or in the case of business restructuring, (ii) a reasonable time lapse of probation period until the end of which the employer may at any time order the termination of the contract, and (iii) provisional transfer to another employer, etc.

For employers who work globally, Romanian regulations offer useful legal tools, such as teleworking, night work, weekend work or the possibility of exceeding regular weekly working time (overtime), as well as other facilities, provisions that should be carefully regulated by the employment contract.

In terms of disadvantages, it can be mentioned that some regulations require, in practice, a higher level of bureaucracy in the conduct of employment.

In case of contracts concluded with freelancers in Romania, the local legislation offers a wide freedom in terms of the conditions and the concrete way of carrying out the collaboration. This type of collaboration is especially convenient for smaller businesses that outsource certain services (such as monitoring certain applications). The disadvantage of this type of contract stems from the fact that both parties are on an equal footing, without a relationship of subordination, which may sometimes not meet the expectations of the parties.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

In the field of labour relations in Romania, more and more digitisation and simplification initiatives are being felt: from already implemented measures (telework, regulation and recognition of electronic signatures, etc.) to initiatives that will be adopted in the near future (complete digitisation of the employment contract, etc.).

As already mentioned, telework has been expressly regulated in Romania since 2018, Law no. 81/2018, and can be provided both exclusively from the employee's premises and also in a mixed system (hybrid) (partly at the employee's premises/partly at the employer's headquarters). There are a few specific elements that need to be included in this type of labour contract, such as the express specification that the employee works in telework regime, the address where the work is performed, the way to achieve control over the employee's activity, the timing of working hours, etc.

Remote employment is facilitated in Romania and due to other regulations, for example (i) regulation and recognition of electronic signatures, both in relation to private individuals and to public institutions, or (ii) rules governing and facilitating conducting trade by electronic means. Also, from a legal point of view, employees who work remotely (telework) enjoy exactly the same rights as employees who work at the employer's premises.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

In Romania, just like all over the world, the pandemic has generated a series of legislative initiatives based on which more and more operations will go exclusively online. With relevance in labour law, legislative changes are currently being discussed so that a full digitisation of the individual employment may be possible. The online work contract and the development of the exclusively electronic employment relationship represent a need issued especially in the last year, when more and more legal collaborations are carried out exclusively online.

Most probably, the long-term effect that the pandemic has generated is that an important part of the job will be carried out remotely even if things will return to normal; more importantly, from a practical perspective, a lot of employers have seen the advantages of teleworking (either exclusively from the employee's home or in a hybrid system), reason enough for the labour law to adapt. Seeing the legislation already adopted so far, as well as the digitalisation trend present in Romania nowadays, we must adapt to an increasing wave of jobs and work-related legal issues, in the context of telework.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Investments in digital infrastructure in Romania have evolved in recent years and substantially more attention has been paid to this component since the emergence of the SARS-COV2 (COVID 19) pandemic. At the moment, three legislative projects are being discussed, all with high potential in improving and boosting online commerce; yet, no effective date has been made public.

E-commerce in Romania stands for around 10% of the retail market, despite the monopoly of the giant e-traders the other 25,000 online businesses compete with.

One surmountable barrier would be compliance with legal requirements for digital content and data protection; although the legislation allows the standard "by continuing 'I agree to the terms and conditions'" stipulation as consent, the same being applicable in the area of consumer protection, the trader will have to deal with.

Setting up an online business in Romania does not require prior authorisation, yet authorisation might be required depending on the offered goods/services (for example, food products, beverages, pharmaceutical products, and insurance services).

Although obtaining a domain name with the Romanian authorities takes at least six months, the procedure is simple and it can be registered as both a domain name and a trademark, by the applicant at the same time.

Online advertising is permitted with some restrictions and prohibitions of certain goods, such as tobacco, alcoholic beverages and non-medical prescribed drugs.

All in all, there are no notable barriers in operating in Romania as a digital business.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Romanian consumers have proven to switch to digital commerce more and more every year, increasing e-commerce businesses revenues by 30% yearly since 2017, and even more in the current year, given the pandemic restrictions and digital alternatives.

Being a country where most of its young and middle-aged population are bilingual, with a widespread knowledge of English, French and other European languages, it facilitates foreign online businesses as well.

One administrative advantage for new B2C businesses operating in Romania, besides the low registration costs (around EUR30), is the predictability of legal regulations, which are applicable in the entire country, lacking regional rules. In terms of costs, online sales in Romania are subject to the standard 19% VAT rate and income taxation for micro-enterprises is also very low, at 1% until the annual revenues surpass EUR1 million.

Another advantage would be the flexibility in labour law, such as the possibility to conclude labour contracts solely online starting with 2021, establishing working hours is not mandatory, especially for collaboration-type agreements, flexible hours are viable, also nightwork or temporary work.

In 2020, Romania implemented in all administrative authorities the legal obligation/possibility to submit and/or receive all digitally signed documents, eliminating the burden of physically filing them, although the administrative act describing the conditions of digital signatures is yet to come.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The opportunity of going digital created by the pandemic pushed the regulatory bodies in Romania to reconsider the benefits arising from it.

At the moment, focus is on proposals to reform the infrastructure and legal framework of business law on cybersecurity, discussing a proposal for safeguarding the citizens' fundamental rights and freedoms in cyberspace.

Also, the Government has drafted and launched for public debate a bill of law on electronic identification and trustworthy services for electronic transactions. The bill regulates aspects regarding electronic signatures and related problems.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The Law no. 209/2019 on payment services and for the amendment of some normative acts mainly reflects the provisions of the Directive 2015/2366 of the European Parliament and of the Council on payment services in the internal market (PSD 2) and creates an environment for open payment services in Romania.

Below are some of the relevant changes to the former national payments framework: (i) the so-called one-leg transactions, where only one of the payment service providers is located within a Member State, for those parts of the transaction which are conducted in a Member State; (ii) requirements on strong customer authentication; and (iii) newly introduced types of third-party service providers: PISP – a payment service provider that initiates a payment order at the request of a payment service user with respect to a payment account held at another payment service provider; AISP – a payment service provider that provides consolidated information about one or more payment accounts held by a payment service user with either another payment service provider or with more than one payment service provider; and CBPII – a payment service provider issuing card-based payment instruments.

In addition, the National Bank of Romania had issued secondary regulations which, together with the transposing Law no. 209/2019, manage to outline a fully-functionable framework: the NBR Regulation No. 4/2019 on payment institutions and specialised providers of account information services, the NBR Regulation No. 5/2012 regarding the classification of

loans and the constitution, regularisation and use of the specific provisions of credit risk applicable to the entities supervised by the National Bank of Romania, other than the credit institutions, and NBR Regulation No. 4/2012 regarding the reporting of the situation regarding the classification of exposures from credits/credits related to payment services and the need for specific provisions of credit risk related to them, applicable to entities supervised by the National Bank of Romania, other than credit institutions.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The risks which may arise are rather operational, related to the implementation of the PSD2 requirements and of the ancillary Romanian legislation. Briefly, the main issues are related to security challenges, cyberattacks and attack detection, identity theft, fraud and account takeover, as well as concerns regarding the payment processors. The result of a constantly developing sector is a cascade of cybercrime attacks across the payments industry worldwide with losses expected to reach \$200 billion by 2024, financial consultants say.

The National Bank of Romania also published a material concerning the risks associated with online payments, more from a regulatory perspective. *Inter alia*, the supervising authority evidences the credit risk, the concentration risk, the custody risk, the general business risk, the investment risk, the liquidity risk, the operational risk, and the systemic risk. These are explained in detail at <https://www.bnr.ro/Oversight-3310.aspx>, available in both English and Romanian.



Alexandru Stanescu is a lawyer focusing on investments, commercial & corporate aspects of tech, and competition, as well as alternative dispute resolution. He is President of the Spanish Club of Arbitration – Romania, a board Member of ThinkBlockTank – European lawyers Blockchain Association based in Luxembourg, and Kleros.io, fellowship for decentralised justice. He is also active in the field of international arbitration & technology.

Alexandru has worked with the World Bank, covering competition, institutional change management, insolvency and ease of doing business policies. While at the World Bank, Alexandru was involved in the change management projects of the Competition Council of Romania, the Ministry of Justice of Romania, General Secretariat of the Government.

He was co-founder and CLO of Ginplatform.io – the first masternode automatic setup solution for more than 100 blockchains.

SLV Legal

2nd district, 17 Mantuleasa street
Bucharest 023961
Romania

Tel: +40 7457 72762
Email: alexandru.stanescu@slvlegal.com
URL: www.slvlegal.com



Andrei Pelinari is a member of the Bucharest Bar and is specialised in new technologies law, as well as in commercial and investment arbitration. He is a Fellow of the Chartered Institute of Arbitrators, UK, of the Arbitrator's Mediator's Institute of New Zealand and the Malaysian Institute of Arbitrators. His experience spans over 20 years, during which he has advised clients in complex infrastructure projects financed from EU funds and/or investment banks, in several economic sectors and industries, i.e civil, industrial, historic urban areas, rehabilitation of water supply and sewerage pipenetworks, pharma industry, banking, cosmetics, automotive industry, IT, new technologies. Andrei has represented clients private and public entities in state courts and in commercial and investment arbitration.

Pelinari & Pelinari

2nd district, 17 Mantuleasa street
Bucharest 023961
Romania

Tel: +40 7232 45795
Email: andreipelinari@pelinari.ro
URL: www.pelinari.ro



Stelian Mic is a Romanian and English law qualified lawyer, being a member of the Bucharest Bar Association since 2008, a member of the Law Society of England and Wales since 2011 and a member of the Global Blockchain Consortium since 2018.

Lately Stelian tends to be more and more involved in restructuring work as well as online commerce and digital assets regulatory matters, being significantly involved in a series of projects from the technology, blockchain and fintech area, both as a direct partner and a consulting attorney.

Mic, Ilie & Asociații

33 Aviatorilor Blvd., Floor 4, District 1
Bucharest 011853
Romania

Tel: +40 74005 3445
Email: stelian.mic@mialegal.ro
URL: www.mialegal.ro



Tudor Velea acts as counsel to financial institutions, sponsors and corporate clients in a variety of private equity and venture capital investments. He specialises in advising financial institutions on legal and financial regulatory aspects of their businesses and transactions and has a particular interest in AI, smart contracts and DLT uses in financial markets.

Tudor co-heads the firm's FinTech and the digital currency & blockchain technology practice, with a particular emphasis on private equity and complex transactions in the technology sector. He regularly advises on digital asset transactions, blockchain technology matters and corporate and securities law. Tudor advises companies through every stage of the corporate life cycle. Prior to co-founding the firm, Tudor began his career in the Investment Management Group at Debevoise & Plimpton in New York, and was a senior associate at White & Case in Miami and Dentons in Bucharest.

SLV Legal

2nd district, 17 Mantuleasa street
Bucharest 023961
Romania

Tel: +40 73334 8043
Email: tudor.velea@slvlegal.com
URL: www.slvlegal.com

A consortium formed of **Mic, Ilie & Asociații**, **Pelinari & Pelinari SCA** and **SLV Legal**, three law firms of young tech-savvy partners with extensive expertise in local and international law matters pertaining to all key business sectors, with a focus on the emerging industries, such as new information technologies, deep tech, digital assets, online trading platforms, cryptocurrency exchanges, and online marketplaces.

We advise and work on ground-breaking matters for and together with a wide range of clients, from start-up companies to multinational large companies and unicorns, wherever they do business, from major financial centres to emerging and growth markets.

We help CEE innovators to expand internationally, especially in the EU and

the US by bringing to the table the network and professional alliances that we have built along the years. We are qualified to provide advice in various jurisdictions including the UK and the US.

www.mialegal.ro | www.pelinari.ro | www.slvlegal.com



Saudi Arabia

Hammad & Al-Mehdar Law Firm



Suhaib Hammad

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

The Saudi E-Commerce Law issued under Royal Decree number M/126 dated 10/07/2019G, and its implementing regulations, governs e-commerce activities in the kingdom of Saudi Arabia (the “Kingdom”). The law does not distinguish between B2B or B2C and defines the consumer as any natural person or legal entity.

See question 1.2 for further details.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

As explained under question 1.1, the law does not distinguish between B2B or B2C and defines the consumer as any natural person or legal entity. The provisions of the e-commerce law govern the relationship between retailers/service providers and consumers, and it requires having an agreement on the terms and conditions of sale in place between the service provider and the consumer. The service provider must provide a statement to the consumer clarifying the terms and conditions of the transaction, which should include certain key provisions setting out the procedure and steps that must be followed to conclude the transaction, contact information of the service provider, total price including the delivery costs and any other charges and taxes, product warranty information, and manner of data collection and usage. The terms and conditions must be expressly agreed in the form of an electronic agreement. Any e-advertisement of the products shall be considered among the contractual documents supplementing the agreed terms and conditions of the transaction. The law further requires retailers/service providers to register the e-commerce activity in the Articles of Association and in the Commercial Registration Certificate of the service provider's entity at the Ministry of Commerce (MOC), and to disclose any special licence obtained by the service provider from another relevant authority to conduct its activity. Failing to register the activity before commencing the e-commerce activity will impose penalties on the service provider by the MOC.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Data protection in the Kingdom is still in the process of being regulated to accommodate the recent trends in electronic transactions. There are a few statutes and regulations in place which govern limited aspects of data protection, but the Kingdom does not have a specific comprehensive guidance on data protection overall. Among the limited protections available, the e-commerce law has additional implementing regulations which were issued in January 2020 and they reflect certain data protection obligations on the service provider when handling consumer data. Another example is in relation to patient data that is electronically collected and stored by a healthcare provider, which is currently regulated by the Ministry of Health under their telehealth licensing and operational requirements, and it requires obtaining a clear consent from the patient to share their data.

In an effort to further regulate data collection and usage, the Saudi Authority for Data and Artificial Intelligence was established in August 2019. It is responsible for regulating and overseeing data collection and processing in the Kingdom, and to implement the necessary data protection and consumer privacy regulations across all sectors. The authority is currently in the process of preparing the draft regulations, and we can reasonably anticipate that the initial draft will embody similar protections as those adopted by the Abu Dhabi Global Market Authority and the General Data Protection Regulation (EU GDPR).

It is important to note that generally in the Kingdom Shariah and Islamic principles protect the individual's right to privacy and prohibit any action that may invade such privacy. These principles prohibit disclosure of personal information without the consent of the individual, unless public interest requires such disclosure.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

The major challenge facing organisations in fintech, AI and digital health is the absence of clear explicit guidance which addresses current and anticipated practices and developments in these industries. The service provider in this case, while adhering to the limited existing regulations which may apply, may generally set privacy policies as they deem fit and suitable at the risk of having to revise them later once the specific data privacy regulation comes into force. For this reason, such organisations in the Kingdom are attempting to overcome this

by adopting best market practices used by their peers overseas in well-regulated jurisdictions, such as the EU and the UAE, in an effort to establish an internal process of handling data which may not require a complete revision of the process by the service provider.

Another challenge is whether such organisations are able to store their users’ data with a third-party provider or within their organisation, and whether such storage will be overseas, on cloud servers, or in a physical location in the Kingdom. Service providers which are collecting and processing data from a government entity in the Kingdom must store the data within the premises of the relevant government entity, unless they obtain a clear consent from the authorised person at the relevant authority to store it elsewhere. See question 6.2 for further information.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Saudi Arabia is aiming to become the new tech hub in the region. This is in line with the Kingdom’s 2030 Vision which was announced in 2018. The relevant authorities overseeing fintech, AI and digital health are in the process of introducing programmes and initiatives to support testing and development.

AI is fairly new, and we expect to see developments soon, following the establishment of the Saudi Authority for Data and Artificial Intelligence. Digital health has developed without requiring much governmental support on testing. The Ministry of Health has issued its regulations on licensing and operating remote healthcare services using online platforms and applications and there are multiple licensed entities already operating in the field.

Fintech has seen the most in terms of governmental support through the Saudi Arabian Monetary Agency (SAMA) and the Capital Markets Authority (CMA). Both the CMA and SAMA have allowed organisations and start-ups to test and develop their offerings within the experimental sandbox programmes of each regulator. Applicants would be granted initial permits allowing them to conduct limited operations in the Kingdom under strict oversight by the regulators. This allowed the regulators to examine the conduct of the applicants, and based on that, the regulators have issued suitable regulations and guidance on licensing and operation.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The cybersecurity framework is limited to the information and telecommunications (ICT) sector. The CITC decided to establish a comprehensive Cybersecurity Regulatory Framework (CRF) to increase the cybersecurity maturity of the ICT sector. The purpose of this framework is to safeguard the public interest and user interest, as well as maintaining the security of telecommunications information.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The current published cybersecurity legislation is limited to the telecoms sector and it is enforced by the CITC; however,

we anticipate that the data authority will potentially contribute further to this when they issue their set of regulations.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

The Saudi Arabian economy has experienced unprecedented growth over the past several years. The National Transformation Program (NTP) and Vision 2030 together envisage a multifaceted development of the economy, with both laying out significant plans to help make this happen. Enabling economic diversification, driving growth of the small and medium-sized enterprise (SME) segment, and fostering innovation and entrepreneurship are at the core of these objectives; developing the e-commerce sector as part of the NTP will add further fuel to these economic development plans. It is notable that the rapidly growing e-commerce markets such as Middle East, North Africa, Central Europe and India, though accounting for only 2.5% of the worldwide e-commerce spending, represent a tremendous potential for e-commerce growth. Investments in the e-commerce industry by international companies have also significantly contributed to the unprecedented growth of emerging e-commerce markets. A rapidly growing community of venture capital (VC) funds and domestic entrepreneurs has further complemented the growth of e-commerce within these emerging e-commerce markets. In line with other emerging economies, the Saudi e-commerce market has been experiencing significant growth and development over the past few years.

B2C e-commerce spending surpassed SAR 29.7 billion in 2016. Saudi Arabia’s young population, increasing broadband and smartphone penetration rates, and the government’s growing focus on e-commerce are key factors that are driving this shift toward online buying in the country. In addition to local online sellers, start-ups, and home-based businesses, a lot of larger regional and international players are also investing and expanding their physical presence in Saudi Arabia. Furthermore, traditional businesses ranging from FMCG companies to banks are increasingly seeing e-commerce as a rapidly growing complementary channel for their products and services. See ICT report, E-Commerce in Saudi Arabia.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Pre-2020, there was a cultural issue with credit cards generally as they are viewed, especially by the older generations, as non-Shariah compliant. This was because there was a fatwa issued over 30 years ago which stated that interest charged on credit card holders for late payments is considered usury and therefore contradicts Shariah which prohibits such transactions. This has led retailers/service providers to use “cash on delivery” which became the preferred payment method. Souq.com was one of the first to use this, and quite successfully managed to penetrate the Saudi market easily and ahead of other international retailers/service providers like Amazon. Amazon subsequently had to acquire Souq.com to increase its market share in the Kingdom and the region.

The religious prohibition around credit cards has led banks to issue prepaid credit cards, which can be topped up for any amount. This was considered Shariah compliant since it only carries an annual fee without charging interest. The religious prohibition has also created a debit card culture, and while retailers/service providers would like to accept that form of payment, the SAMA requires retailers/service providers to have a local bank account in the Kingdom in order to accept payments from Saudi debit cards. In order to have a local bank account, a retailer must set-up a local entity. This poses a challenge for retailers/service providers who operate through a single hub location in the region.

The current Saudi culture has, however, changed significantly since the Covid-19 pandemic. See question 4.6 for further details.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

While we are not aware of such situations, it is not necessarily the case, because there is still high demand for e-commerce services locally and most local retailers/service providers are still limited in the territories they cover.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

All e-commerce platforms in the Kingdom offer dual language options, Arabic and English at a minimum. The local population of citizens and expatriates would speak either one of those two languages, if not both for working professionals.

When local firms wish to expand globally, they mainly do so by using an English platform. As far as we are aware, most local e-commerce firms are expanding regionally within the Middle East which are all Arabic speaking countries. Therefore, they would not need to consider additional language support besides Arabic and English.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

A study was conducted with the main objective of exploring whether navigation or e-interactivity on an online store play an important role in converting online window shoppers into e-customers. The findings identify the preferred areas of e-customers. The study was based on primary data collected from the respondents in Jeddah city of Saudi Arabia through a structured close-ended questionnaire. The questionnaire was developed in English language and translated into Arabic language as the respondents were mainly Arabic speakers. The results were obtained through analysis of data on SPSS using statistical tools such as frequencies, mean, and factor analysis. The results suggest that navigation aspects were more preferred by the e-customers on the e-retail store while shopping online. To convert the prospective visitors into customers, the e-retailers/service providers should emphasise more on navigation factors such as clarity of the website, detailed information on

the website, speed of the website, organisation of the website, effectiveness of the website, overall structure of the website, easy navigation of website, and ease of use of the website (see Navigation versus E-Interactivity in Online Store: An empirical study in Saudi Arabia, Dr. Zaid Ahmad Ansari). Saudis in general prefer to rely on images and graphical concepts in their online shopping.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Yes, the Covid-19 pandemic has had a major impact on making payments. With the introduction of e-wallets and electronic payments through Apple Pay or STC Pay, and the requirement to add a debit card or credit card in the e-wallet, the Ministry of Health directed retailers/service providers not to take cash payments and to rely mostly on electronic payments to avoid spreading the virus. This has led more consumers to obtain debit and credit cards, and set-up their e-wallets accordingly. In addition, the mandated lockdowns led to a change in retailers/service providers behaviours forcing them to make their products available online. While most retailers/service providers joined existing e-commerce platforms, some retailers/service providers such as restaurants and supermarket chains went a step further and set-up their own platforms and smartphone applications to sell directly to consumers.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

The process requires filing a complaint by the brand owner with the MOC. The protections under current applicable laws are focused on trademark infringement, and do not consider online brands overall. Still, this grants sufficient protection to brand owners when a third party infringes their rights.

The MOC is reactive rather than proactive when it comes to online brands. However, in limited cases, they have acted without being prompted by a brand owner when they were made aware of a violation. The Saudi authorities together with consumers and social influencers combined their efforts to protect intellectual property and combat commercial fraud of the product owner. For example, one prominent case occurred in one of the biggest traditional markets in Riyadh. An activist using Snapchat showed his followers counterfeit products, including cosmetics, that a makeup artist was promoting at the market as genuine. Another activist, using social media channels, exposed gold shops selling counterfeit jewellery. Upon reviewing these social media posts, the Anti-Counterfeiting Department within the MOC raided these shops and closed them down. MOC did not wait for someone to file a complaint but instead took the initiative based on the social media post's information to stop the sale of these counterfeit goods in Riyadh's traditional markets.

This awareness in turn helps the authorities expand their fight to protect consumers from commercial fraud and at the same time enables them to undertake their responsibilities at reduced costs. For brand owners, this type of social media activism also provides them with well-documented evidence of counterfeiting and other fraudulent activities and can accelerate processing of their IP infringement claims before the courts (see Social Media and the Fight against Counterfeiting in Saudi Arabia, Al-Tamimi & Co.).

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

The legal protections available under applicable laws are limited to registered intellectual property. It is advisable for retailers/service providers to register their trademarks to benefit from the protection granted by law and the enforcement agencies.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The provision of the Cloud Computing Regulatory Framework by the CITC shall apply with regard to any cloud service provided to cloud customers having a residence or customer address in the Kingdom. The framework requires certain data protection requirements for cloud computing services under Articles 3.4 and 3.5. We consider the main risk as the protection of such data. The current applicable data privacy regulations require obtaining clear consent from a user before processing their data and the terms of the privacy policy must clarify the manner in which such data will be processed. Contracting parties must ensure compliance with their published privacy policy, and any regulations which may restrict the transfer of data beyond the borders of the Kingdom.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

The local authorities, mainly the Ministry of Interior, prefer that the data is stored locally in the Kingdom. Certain regulations in the healthcare, transportation, and fintech industries require retailers/service providers to store their data locally in order to obtain and maintain their operational licence.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The UAE and the Kingdom are working jointly on developing a digital currency and payment system to facilitate cross-border trade between the two countries.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Digitalisation also increases the benefits that can be drawn from regional trade agreements (RTAs). When combined with an RTA, a 10% increase in digital connectivity increases exports by an additional 2.3%. Finally, there is a statistically significant relationship between information and communication technology (ICT) goods imports, digitalisation and services exports, suggesting that, just as services have become more important for goods exports, ICT goods increasingly enable the export of digitally deliverable services.

A barrier on one of these transactions will affect the need or ability to undertake the other transactions. This means that market openness needs to be approached more holistically, taking into consideration the full range of measures that affect any particular transaction. For instance, Internet access may be a necessary but not sufficient condition for digitally enabled trade in goods to flourish. If logistics services in the receiving (or delivering) country are costly due to service trade restrictions, or if goods are held up at the border by cumbersome procedures, then the benefits of digital trade may not materialise (see Trade in the Digital Era, OECD, March, 2019).

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

There are no particular tax incentives to digital businesses in the Kingdom.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

We expect the point to be most disputed is in relation to applying the Value Added Tax on transactions initiated through e-commerce platforms, where the authorities would assert the tax immediately upon completion of payment and collect it monthly from the service provider. While the e-commerce platform might have a process of when they consider tax to be due based on their policies and terms.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

The Saudi Labor Law tries to balance the rights of both the employees and the employers. It also permits private enterprises to establish their own policies within the framework of the law as they relate to employee attendance and working remotely. The Labor Law does not restrict employers from using resources of any nationality. The Wage Protection System permits employees to receive their salaries in any currency and even if paid into an overseas bank account.

Non-Saudi employees recruited locally in the Kingdom must hold a valid work permit and obtain a residency card in order to travel to and work on the ground in the Kingdom.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

While there are no specific regulations relating to working remotely, the Saudi Ministry of Labor and Social Development has created a local and flexible work environment that keeps

pace with the developments in the global labour market adopted through the “Telework” programme, which is a national initiative supported by the Ministry. The programme is aimed at providing a flexible work atmosphere for working away from the organisation. This initiative is supervised by the Takamul Investment Holding Company; the first Saudi entity licensed by the Saudi Ministry of Labor and Social Development.

The programme offers a certification process for employers looking to resource employees online. By joining the programme, the employers would be able to reach a wide number of candidates made available through the Ministry from data provided by job seekers. The programme operates through a digital platform which connects the employers with the employee.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

The Ministry has permitted employers to develop their own remote working policies within the framework of the law, and employers have embraced reducing the work force in the main premises and have started to recruit employees remotely even after the Ministry of Health revised their directives on not attending the work place.

Currently, the Ministry requires employees to be vaccinated before they can return to the workplace, while there no such requirement for remotely recruited employees.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

While the Kingdom has been recently adopting new regulations to cater for the rapidly evolving digital and fintech businesses, the laws and regulations still need to be updated to follow international legislation and cover this new era of businesses, as well as provide much more comfort to foreign investors when doing business in the Kingdom. Ninety (90) per cent of businesses are facing significant roadblocks to their digital transformation initiatives, with data privacy and cybersecurity concerns (see “90% of UAE, Saudi firms say facing digital challenges” by Arabian Business).

While the Kingdom has recently began adopting new regulations to cater for the rapidly evolving digital and fintech businesses, the laws and regulations still need to be updated to follow international legislation and cover this new era of businesses and provide much more comfort to foreign investors when doing business in the Kingdom.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

From our exposure, we feel the most notable advantage is related to economy growth and sustainable development. The Kingdom is now leading digitalisation and AI in the entire regime. This will also positively impact SMEs, employment and foreign investment. It is notable to mention that the Kingdom has a targeted geographical location connecting Europe, Asia and the Americas, which helps with introducing innovations and exchanging business opportunities.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The regulator is focused on registering all operators of digital businesses in a comprehensive registry with accurate and up to date information which would allow the enforcement agencies to take action against violators of the E-Commerce Law and other relevant legislation. The major challenge has been in monitoring the activities of the operators and locating their legal entities when needed. This focus aims to ensure fair trade online and secure experience for consumers in line with the MOC’s consumer protection guidelines. For this reason, the MOC also requires the registration of non-Saudi based retailers/service providers. However, it is struggling with enforcing this requirement in reality. Nonetheless, foreign retailers/service providers are advised to adhere to the requirements of the applicable e-commerce law to avoid blocking their platforms from the Saudi market.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

In January 2020, SAMA introduced the Payment Service Provider Regulations (“PSP Regulations”) to regulate PSPs’ operations within the Kingdom by supervising, controlling, and issuing the guidelines relating to PSP licences, in which PSPs may obtain a PSP licence from SAMA to provide payment services in Saudi Arabia.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The main issue relates to processing debit card payments for non-Saudi retailers/service providers who do not maintain local bank accounts. SAMA restricts the use of debit card payments and limits its processing to be done between local bank accounts. An account holder may then manually transfer funds from the local bank account to an overseas bank account. This creates additional steps which requires manual processing of payments to foreign retailers/service providers, holding funds in custody, and in some cases placing the payment provider as the retailer/service provider in the transaction to receive the debit card payment, and then set-up another transaction with the actual retailer/service provider.

Furthermore, overseas payment providers must adhere to the requirements of the local Payment Service Provider Regulations to avoid being restricted from having access to local consumers.



Suhaib Hammad joined Hammad & Al-Mehdar Law Firm in 2009. He earned his LL.B. from IIU Malaysia and his LL.M. from the University of Miami, specialising in International Business Law.

As a Partner, Suhaib leads the Commercial and Intellectual Property practice, focusing on ICT, TMT and Life Sciences. In addition, Suhaib was placed on secondment with the corporate and commercial team at Simmons & Simmons in their Dubai and London offices, and has worked on leading cross-border transactions. His experience includes advising major international telecoms and healthcare companies on Saudi regulations in relation to formation and operation. Suhaib was also awarded a Client Choice Award by Lexology for the year 2019. The Firm was recognised as the best Mergers & Acquisitions law firm for the years 2017 and 2018 by the IFN Law Awards, and has been honourably mentioned as a Tier 1 Firm in The Legal 500 2017 for Banking & Finance Transactions.

Hammad & Al-Mehdar Law Firm
King Road Tower, L 12
Office 1209 King Abdulaziz Road
Jeddah
Saudi Arabia

Tel: +966 92000 4626
Email: sh@hmco.com.sa
URL: www.hmco.com.sa

Hammad & Al-Mehdar Law Firm was founded in 1983 in Jeddah, Saudi Arabia, and has grown to become a prominent private practice Saudi firm in the Kingdom and the GCC. The law firm boasts a leading local presence supported by international capabilities.

Hammad & Al-Mehdar provides a full suite of business and corporate legal services in all major areas of Saudi law, working on cutting-edge, complex and high-value transactions and disputes.

Headquartered in Jeddah, Hammad & Al-Mehdar's growth story is one of trade, innovation and technology in the Kingdom's private sector. Hammad & Al-Mehdar maintains a strong specialisation in servicing privately held businesses, with unrivalled expertise in business and transaction structuring, private construction works, commercial, intellectual property, corporate governance, and regulatory advisory services.

www.hmco.com.sa

HAMMAD & AL-MEHDAR

LAW FIRM

Switzerland



Jürg Schneider



Hugh Reeves



Maria Gentile

Walder Wyss Ltd

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

Swiss law contains very few provisions on e-commerce in a B2B context. There is no dedicated e-commerce law, as may exist in other jurisdictions.

The most relevant rules applicable to e-commerce players are included in the Federal Unfair Competition Act (UCA). Article 3 para. 1 litt. s UCA indeed requires that anyone offering goods, works or services by means of electronic commerce must: (i) indicate in a clear and complete manner its identity and contact address, including e-mail address; (ii) indicate the different technical steps leading to the conclusion of a contract; (iii) provide the appropriate technical tools allowing to detect and correct any incorrect inputs prior to despatch of an order; and (iv) confirm without delay and by e-mail the client's order. Article 3 para. 1 litt. s UCA, however, applies to B2B and B2C e-commerce alike.

From a contracts law standpoint, Swiss law is generally permissive granting a broad contractual freedom to the parties. This is particularly true in B2B relationships where, save for a few exceptions, the contracting businesses have a lot of liberty to define the contents and provisions of their agreement and are not bound by formal requirements.

Further rules apply to B2B e-commerce actors, such as requirements against certain types of advertising and marketing behaviour, though these rules are neither specific to B2B businesses nor to e-commerce activities. Therefore, these rules will not be discussed unless specifically addressed hereafter.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Similarly to the situation discussed above concerning B2B e-commerce, few rules apply specifically to B2C e-commerce.

As mentioned above, the requirements of Article 3 para. 1 litt. s UCA are of particular relevance for e-commerce businesses, both in B2B and in B2C situations. The UCA also prohibits the use of abusive general terms and conditions, which contain provisions that go against the rules of good faith and put the consumer at a disproportionate and unjustified disadvantage (being specified that there are no content requirements for general terms and conditions). Moreover, the Federal Ordinance on Price Indication (PIO) applies to whomever offers or advertises goods or services to consumers, being specified that a consumer is defined as any person who purchases goods or services for purposes not related to his commercial or professional activity. Under the PIO, sellers who sell to consumers must indicate the effective price, in Swiss francs, including VAT and any other taxes or fees (copyright fees, waste disposal costs, etc.). The seller must also state the unitary price for measurable goods (and detail price for any pre-wrapped goods), though some exceptions apply, for instance when sale is based on weight or length. In specific sectors, some additional rules apply (e.g. for package travel offers or for products that may be relevant from a product safety stand-point). Note, however, that the PIO also applies to offers and advertisements to consumers in a non-e-commerce situation.

Contrary to many foreign jurisdictions (especially the EU and the USA), Swiss law does not contain many rules to protect consumers in an e-commerce setting. Indeed, consumer protection is – arguably – not (yet) a Swiss speciality and remains in a rather embryonic stage of development, despite on-going pressure from consumer protection organisations and legal scholars, as well as a specific act on consumer information. For instance, Swiss law does not have a general withdrawal right, though it is more and more frequently found in the general terms and conditions of Swiss-based e-commerce platforms active in the European Union or in direct competition with EU-based platforms. Furthermore, Swiss law does not have any provisions on maximum delivery dates. That said, Swiss private international law and Swiss civil procedure law do contain certain provisions that strengthen the consumer's position. In contracts with consumers, both in international and purely national relationships, the contracting parties cannot contractually waive beforehand (including in any general terms and conditions) the consumer's right to bring a court claim before the courts of his place of domicile or habitual residence. Moreover,

under Swiss private international law, in international relationships, the parties cannot waive the applicability of the law of the state of the consumer's place of habitual residence if: (i) the supplier received the order in that jurisdiction; (ii) the conclusion of the contract followed an offering or advertising in that jurisdiction and the consumer performed the necessary steps towards contracting in that jurisdiction; or (iii) the consumer was enticed by the supplier to go to another country in order to put in an order. Switzerland is bound by further specific court competency rules (so-called "Lugano Convention") with EU and EFTA states; these rules are substantially the same as the general private international rules outlined above and seek to ensure that consumers retain access to their local courts.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The data protection legal landscape in Switzerland has been rather dynamic over the past years. In light of developments at the European and international levels, the Swiss legislator decided to revise the Federal Data Protection Act (FDPA). This revision has been completed and the revised law is expected to enter into force by the end of 2022. The revision aims to align with the standards under the GDPR ensuring an adequate data protection level not only within Switzerland but from an EU perspective as well.

Under the current FDPA, and somewhat unusually by international comparison, personal data of legal entities are protected to the same extent than those of individuals, which can lead to more extensive data protection compliance obligations for e-commerce businesses. However, the revised FDPA will do away with this specificity.

The current FDPA has garnered the reputation of being a "paper tiger" due to the relatively low penalties as it only provides for an amount of CHF 10,000 in certain cases of breaches; this will be expanded and increased to CHF 250,000.

Lastly, considering the international environment of digitalisation, the revised FDPA – similarly to article 3 GDPR – also has specific provisions on its (extra-)territorial scope. Foreign-based entities will be subject to the revised FDPA if and to the extent their data processing has an impact on the Swiss territory, namely when services are offered to Swiss-based customers or any related processing is taking place in Switzerland.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

As regards general data protection principles, transparency requirements are of central importance, especially if an organisation resorts to AI in the course of its activities. Transparency reflects a particular challenge in this field as data are, to a large extent, collected from various separate sources, processed on an aggregate basis and mostly based on algorithms or other technology. This often makes it difficult for organisations to provide full transparency to the data subjects.

Moreover, given that the personal data that fintech and digital health businesses process may often qualify as sensitive data or lead to personality profiles, there is a heightened potential risk for the affected data subjects. In addition, strict standards that apply to outsourcing or cross-border data transfers, as well as data security considerations, are prime concerns for digital

businesses. Indeed, they tend to be internationally active and amass significant quantities of personal data and, as the case may be, sensitive personal data. These businesses, even if they are relatively small in size, therefore need to proactively ensure that they meet the requirements of data protection legislation and provide at all times a high level of data security.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

The Swiss government as well as the Federal Data Protection and Information Commissioner (FDPIC) have a significant interest in supporting actors operating in these fields. Much of this support is currently taking place through government-backed research, which may lead to regulatory changes.

In 2018, the government published its strategy for national digital developments, the "Digital Switzerland" strategy, addressing various issues in relation to the ongoing digitalisation, such as for instance the challenges of decision-making based on machine learning and algorithm methodology. In this context, the government appointed a working group tasked with identifying upcoming issues in the field of AI and analysing the need for specific steps in data-driven sectors. Conversely, the government has drafted an eHealth strategy addressing key issues such as the handling of digital patient data as well as the use of AI and machine learning (e.g. robotic technologies).

The FDPIC has published multiple statements and non-binding guidelines on how to address data protection matters in these areas. For instance, the FDPIC published its opinion on the implementation of a proximity tracing application in relation to the COVID-19 pandemic.

Further, sector-specific regulations address particular data protection issues. The Swiss Financial Market Supervisory Authority (FINMA), for example, issued binding guidelines on outsourcing and data security for the financial and insurance sector. eHealth – a public organisation established by the federal and cantonal authorities – published several factsheets and other guidance on how to deal with electronic health data.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

Switzerland does not have a dedicated cybersecurity legislation. Rather, cybersecurity is primarily a subset of data protection legislation and is therefore governed by the rules on data protection and data security. These rules are relatively general. For instance, there is (at the time of writing) no general data breach notification requirement. As the rules are technologically neutral, the legislation avoids discussing the use of one specific technology. However, cybersecurity is a central concern of the Swiss government and is frequently discussed and analysed in governmental reports and national strategies. Because Swiss data protection legislation sets a comparatively high bar, data security and cybersecurity are generally adequately ensured; this has so far comforted the legislator in not venturing into drafting any *ad hoc* cybersecurity legislation.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Anyone who processes personal data must implement technical and organisational measures to protect this data in particular against any accidental or unauthorised destruction, accidental loss, technical faults, forgery, theft or unlawful use. These technical and organisational measures include a variety of checks or controls, such as controls over who has access to or receives personal data, storage controls, usage controls and so forth. Swiss data protection and data security regulations do, however, not require implementation of a specific technical standard, given the legislation's technological neutrality, though many actors implement international standards (e.g. ISO 27001) as a matter of good business practice.

Enforcement is essentially within the remit of the above-mentioned FDPIC. Though the FDPIC's current enforcement powers are somewhat limited, this will change with the advent of the revised data protection legislation. Moreover, other sectoral authorities and regulators may have enforcement powers in certain specific cases (for instance, the Office of Communications (OFCOM) or the Financial Markets Supervisory Authority (FINMA)).

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Consumers have an overall positive attitude towards e-commerce and online shopping. In the statistics, Switzerland systematically ranks highly in percentage of the population performing online purchases. Moreover, e-commerce has enjoyed uninterrupted growth over the past years. According to the Swiss Association of Distance Sellers (VSV ASVAD), the amount of online purchases in 2020 reached CHF 13.1 billion (being specified that different studies reach slightly different numbers and results). Consumer electronics as well as fashion and clothing items constitute the bulk of online sales to consumers. Consumers can also access foreign online sellers (albeit with some *de facto* barriers, see hereafter the answer to question 10.1) and purchases from businesses based outside of Switzerland (primarily in Germany and France) account for approximately one quarter of B2C purchases. This has resulted in a downwards pressure on B2C purchases by Swiss-based businesses, as well as a broader diversification of the online offering of goods and services.

Despite the above, e-commerce does remain a relatively new concept for Swiss-based consumers and businesses alike and is therefore expected to continue to gain traction across the board over the next years. This is particularly true for certain categories of goods, such as foodstuffs, which have not yet properly penetrated the e-commerce landscape.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Swiss buyers are in general open to cashless payment methods, though payments against invoice remain an important means

of payment. Credit cards and payment services (e.g. PayPal) are popular. In particular, the use of credit cards, which frequently came at an additional cost for the buyer, has profited from the intervention of the Swiss Competition Commission which, in recent years, took measures to progressively, yet strongly, reduce the interchange fees (fees due to credit card issuers which were frequently levied on the end customer by the merchants). In addition, mobile payment methods have been enjoying growing popularity, especially among younger age groups. Direct debit, debit card and cash on delivery are, on the other hand, not the most sought-after payment methods, and online businesses do not systematically provide those options.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Local e-commerce retailers and platforms tend to focus on the Swiss internal market. Indeed, one of the Swiss industry's concerns is the preservation and, where possible, increase of the foothold of local businesses. This is because foreign-based businesses are frequently able to offer similar or identical goods at a more competitive price-point. With some noteworthy exceptions, local sellers are currently not performing well outside of the country in comparison to many e-commerce businesses based abroad.

There have been recurring attempts to introduce online labels aimed at highlighting the Swiss origins of e-commerce platforms and their offerings. However, in many cases such e-commerce labels have proven disappointing (as shows the now-defunct "Webtrader" label or the "e-comtrust" label, which however remains in existence).

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

The use of varied languages is a strength of many Swiss e-commerce platforms. Swiss e-commerce platforms frequently use several languages, namely German, French, Italian and often English. Interestingly, though German, French and Italian are the official Swiss languages (a fourth official language being the seldom-found Rhaeto-Romance), one or several of these languages – usually Italian, eventually French – are left out or substituted by English. The use of English offers a double advantage: firstly, it allows businesses to target customers outside of Switzerland in countries which do not speak German, French or Italian; and, second, it allows these businesses to avoid the internal language barriers (and related translation costs) and allows them to also target the sizeable international community within Switzerland.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

As the Swiss market is linguistically segmented, the use of all official languages ensures that consumers across the country can fully enjoy their shopping experience. As mentioned above, the use of English is also common amongst Swiss-based

e-commerce platforms. If consumers are targeted, the seller must display its prices in Swiss francs, including VAT. Moreover, NetComm Suisse, the Swiss e-commerce association, considers that customers pay close attention not only to prices but also to quality, branding and reputation. Therefore, the leading Swiss e-commerce platforms often seek to make a strong impression in terms of product quality and forego the offering of lesser-known but cheaper brands in favour of brands with excellent reputation.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

The Covid-19 pandemic has not led to any cultural shift. This is likely due to the strong internet presence of Swiss consumers prior to the pandemic. 2020 nonetheless proved a positive year for e-commerce overall, with a strong increase in sales compared to 2019.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

A first step often involves reaching out directly to the e-commerce platform as these typically have specific brand protection practices (such as take-down action) and respond swiftly. This process also has the advantage of speed, as recourse to the local courts is more time-consuming and costly. Various e-commerce platforms such as eBay and AliExpress, which both have a dedicated Swiss e-commerce platform, have policies in place to combat brand infringement (Amazon is not (yet) present in Switzerland with a dedicated Swiss e-commerce platform, potential Swiss-based customers being redirected to foreign Amazon websites).

Alternatively, or consequently, to the above steps, brand holders can rely on a cease-and-desist and – if necessary – court injunction process against the known infringer. The legal basis for such actions is primarily trademark law but can also be founded on rights arising from unfair competition or company name regulations. This process may also be relevant in cases of domain name uses (for the “.ch” top-level domains) though in this context the WIPO’s domain name dispute resolution mechanism, set up by the WIPO’s mediation and arbitration centre, has enjoyed much success and allows the owners of trademarks, domain names or any other signs to resolve domain name complaints. In addition, domain name registrars are in practice cooperative to *prima facie* legitimate infringement claims and respond promptly to take-down and intervention requests.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

In practice, enforcement action against actors based outside of Switzerland may prove cumbersome. Moreover, Swiss law and case law is, by international comparison, still in quite early stages with respect to the notions of contributory infringement and vicarious liability of hosting providers, web access providers and platform operators and there are arguably not many clear rules in that respect. The same goes for the use of someone else’s trademarks in Google Ads (formerly AdWords) or website metatags in particular, as there is little case law in this respect and the situation may therefore evolve; as things currently stand, the use of a protected term in Google Ads is generally permissible provided

this use is not product-identifying; metatags are generally not problematic, though a case-by-case analysis is always necessary.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

By contracting with third party-owned data centres or cloud providers, organisations enter into a controller-processor set-up from a data protection perspective. Under the FDPA (see above responses in Section 2), outsourcing is generally permitted provided that (1) the processor processes such information only to the extent permitted to the controller, (2) no confidentiality obligations prohibit such outsourcing, and (3) the processor implements appropriate technical and organisational measures.

Compliance risks in this context primarily arise if data security (see above responses in Section 3) is implemented inappropriately or if personal data is transferred or disclosed abroad, in particular when recipients are located in countries outside the EU/EEA which do not provide an adequate data protection level.

The FPDIC, in its guidelines on cloud computing, recommends assessing any data security risk prior to engaging any subcontractor. For example, organisations should assess whether the specific cloud model is organised in a private or public cloud or whether the service includes infrastructure (IaaS), a platform (PaaS) or the provision of the software as a service package (SaaS). Further, organisations should in particular consider potential risks such as loss of control, service provider non-compliance (which can, however, only be assessed conclusively in advance with difficulty) and access by foreign authorities which may be subject to a criminal offence.

Despite the above concerns, in practice, reputable cloud providers frequently provide for even higher data security standards than those in place within the outsourcing organisation’s own IT infrastructure.

Moreover, it is likely that outsourcing would include a transfer of data abroad. The FDPA requires that any such transfer is based on additional safeguards – similar to those in the EU under the GDPR – which may be met by an adequacy decision by the FDPIC or contractual agreements such as the EU standard model clauses issued by the EU Commission (as the case may be, adapted to Swiss circumstances). In this respect, the case of transfers to the USA is noteworthy as the self-certification programme known as the “Swiss-US Privacy Shield” (equivalent in scope and functioning to the EU-US Privacy Shield), was repealed in September 2020, thereby bringing about a new level of complexity around Swiss-US data transfers.

Further, compliance risks in relation to cloud services may be addressed sector-specifically. For instance, the financial markets regulator, FINMA, has addressed specific risks in the financial and insurance sector in its circular on operational risks including outsourcing and data security aspects (see also above response to question 2.3).

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

There are no general requirements for data territoriality. Therefore, data storage outside of Switzerland is generally possible; though the company looking to store abroad may need to put certain safeguards in place prior to any cross-border transfer of personal data (see above response to question 6.1).

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

In 2020, Switzerland ranked six in the IMD Business School's World Digital Competitiveness Ranking (down one place from the previous year). Switzerland is praised for its ability to assimilate new technologies quickly and to exploit them to stimulate the digital transformation.

National initiatives such as "Digital Switzerland" (see above answer to question 2.3), which bring together government bodies, companies, and interest groups, are aimed at building Switzerland's digital future at the international level.

Mandated by the Confederation, Switzerland Global Enterprise (S-GE) supports Swiss companies, especially SMEs, in their export and import activities. In 2017, S-GE started Export Digital in cooperation with Google, a digital market analysis tool that helps Swiss SMEs to start exporting or to boost their export strategies.

The Swiss authorities are prioritising the challenges of digital transformation, and major IT projects are currently underway to improve efficiency and performance in this area.

Presently, the Swiss tax authorities already offer electronic platforms enabling companies to process tax transactions online.

At the level of the Federal Tax Administration, this is particularly the case for customs duties and value added tax (VAT) with platforms such as: TARES, which offers an online customs clearance procedure; CSP (customs account in the centralised settlement procedure of the Federal Customs Administration), which allows regular importers of commercial goods into Switzerland to carry out customs clearance without immediate cash payment, to request to receive tax rulings in electronic form and to receive invoices in electronic form rather than on paper; and ESTV SuisseTax (E-Government Portal), which allows companies to process tax transactions online for VAT and also for other taxes such as withholding tax.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

The digitalisation of society and the economy is a challenge for political authorities, as it requires the adaptation of the legal and administrative frameworks.

To this end, the Federal Council regularly conducts surveys aiming at analysing the "numerical compatibility" of laws with an economic impact and the need to amend them.

On 1 February, 2021, the Federal Act on the Adaptation of Federal Law to Developments in Distributed Electronic Registry Technology partially entered into force. With this law, sometimes referred to as a "DLT" legislation, *ad hoc* adaptations for several federal acts affecting both civil law and financial market law will be taking place. This law aims to provide the best possible framework conditions so that Switzerland can establish and develop itself as a leading, innovative and sustainable location for fintech and DLT companies.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

A corporate tax reform (TRAF) came into force on 1 January, 2020 in Switzerland. TRAF has induced significant changes in Swiss domestic law, amongst which the introduction of a patent box regime and the possibility to use increased R&D deductions, both aiming at promoting research and development.

The patent box offers privileged taxation for income from patents and similar intellectual property rights on the part of total R&D expenses that has been incurred in the country of residence in relation to total R&D expenses. The tax privilege consists of an exemption from cantonal tax of up to 90% of the qualifying above-mentioned income.

With the additional deduction for R&D, taxpayers incurring R&D expenses in Switzerland, directly or indirectly through third parties, can deduct from their taxable income up to 150% of their actual R&D expenses. The additional 50% deduction is calculated on R&D personnel expenses – increased by 35% – and/or R&D expenses invoiced by third parties – up to 80%.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The main issue at stake in taxing the digital economy is balancing the allocation of tax revenues between the countries of residence of multinational companies and the markets where they are active. Current international allocation rules for corporate income tax purposes are indeed based on a physical presence of companies in a State (head office or a permanent establishment) and are outdated by the evolution of the digital business model. Countries where consumers (but not companies) are based thus see a share of the profits made on their territory escape taxation. The current discussions at OECD and EU level aim at enabling these "consumer-based" countries to tax part of the profits derived from their market. In this context, it is necessary to provide efficient tools to avoid double taxation, since the share of profits taxed at the place of market should not, in addition, be taxed at the place where the company is taxed on an unlimited basis. Otherwise, the introduction of such a system could lead to major disputes between digital companies and the various tax authorities. Switzerland supports the work of the OECD for the "Taxation of the Digital Economy" for the long-term adaptation of corporate taxation to achieve a well-functioning global system of business taxation and ultimately ensuring sustainable growth. In this respect, Switzerland favours a multilateral approach, based on consensus, rather than a multitude of uncoordinated national measures.

As regards indirect taxation, Switzerland has not entered into any tax treaty for VAT purposes. Consequently, conflicts often arise when it comes to qualifying or localising a cross-border transaction for VAT purposes. A digital entrepreneur might thus suffer double VAT burden on cross-border transactions.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

Swiss employment law is generally considered liberal though it does contain rules protecting the employee (such as termination notice periods, statutory social security contributions, overtime). That being said, the choice between an employment relationship rather than an independent contractor/self-employed contractor relationship essentially depends on how much control the employer wants to have over the contracted person (e.g. with respect to work organisation, business knowledge, etc.). In this context, if an employer wants close control over the contractor's activity, it will rather opt for an employment relationship bearing in mind the protective rights in favour of employees.

The distinction between an employment relationship and an independent contractor relationship under Swiss law may prove complex, being specified that the formal designation of the relationship by the parties is irrelevant. The qualification of the relationship between the parties is therefore to be made on a case-by-case basis depending on all factual circumstances and in particular on the existence of any subordination (such as the obligation to comply with instructions, work organisation and time management). Depending on the relationship's qualification, the more protective employment law provisions may be applicable.

The qualification of the relationship between the parties remains irrelevant from a social insurance law perspective. Thus, an independent contractor/self-employed contractor may be qualified as dependant from a social insurance perspective triggering the obligation to pay social security contributions.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

Although remote work has been increasing in Switzerland over the last decade, it is far from being common practice. In this context, Swiss employment law does not provide for any specific rules with respect to remote work and the parties to an employment agreement remain free to discuss the conditions. However, even though Swiss law is silent with respect to remote work, all provisions remain applicable in particular with respect to time recording and health and safety regulations. Employers should have internal regulations and provide for specific terms in the employment agreement such as coverage of equipment cost. Lastly, implementing and monitoring remote work remains mostly permissible, though the employer is generally prohibited from monitoring employee behaviour.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

There is a general feeling that remote work, which has become commonplace during the Covid-19 pandemic, will remain a frequent practice going forward. Indeed, as the Swiss workforce includes a strong services sector, for whom remote work presents few hurdles, it is often expected that there will be a lasting effect from the pandemic on remote work habits.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Swiss-based businesses have in recent years had to ensure that their activities, from a data processing standpoint, were in line with the requirements of the EU GDPR (see above answers in Section 3). Indeed, though the GDPR is not directly applicable in Switzerland, many Swiss-based companies look to sell outside of Switzerland and logically target EU-based individuals, thus leading to the applicability of the GDPR. Though many actors already took the necessary steps, and awareness in this respect is high, there remains a sizeable amount of businesses that still need to adapt to the extent they wish to target EU/EEA-based individuals.

Moreover, Switzerland's comes in 36th position on the international "Ease of Doing Business Index", a World Bank ranking that provides an assessment of countries' regulatory landscape in terms of creating and operating a business. This indicates that local businesses face various regulatory obstacles; however, the government has been taking steps towards a business-friendly national environment (see below response to question 10.2).

Online businesses based outside of Switzerland but selling to Swiss-based buyers face the legal and practical barrier of customs clearance for goods entering Switzerland, which may make their offering less attractive to Swiss-based customers who bear any related customs clearance fees. Foreign businesses, to avoid this hurdle, need to register for VAT purposes with the Swiss tax authorities and charge Swiss VAT to their Swiss-based clients, which may be dissuasive due to the time and efforts involved.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

The Swiss government has over the years constantly looked to secure the position of local SMEs, which constitute 99% of all legal entities in Switzerland and are responsible for two-thirds of the jobs in the country (according to the Federal Statistics Office). Despite Switzerland not being first-in-class in the Ease of Doing Business Index (see above answer to question 10.1), the SMEs, and businesses in general, therefore benefit from an environment that is suitable to their needs and favourable to their growth given this environment's political, economic, legal and judicial stability and reliability. As mentioned earlier (response to question 1.2), consumer protection is not as developed in Switzerland as it may be in neighbouring jurisdictions. This does allow businesses to avoid having to implement consumer protection rights and measures. On the other hand, it may have a negative impact on customer trust as these customers are increasingly getting accustomed to the consumer-oriented practices found abroad. For this reason, many businesses have already bolstered, on a voluntary basis, the contractual rights granted to their customers.

Lastly, as mentioned (response to question 4.1), Swiss residents are particularly active online and therefore offer a thriving setting for digital businesses.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

Currently, regulatory focus frequently pertains to the technological shift. In particular, matters of cybersecurity and data

protection have received a lot of attention. The various sectoral regulators or prudential bodies usually follow a rather hands-off approach. Indeed, interactions with regulatory bodies is usually easy and not laden with formal requirements.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Payment systems, defined as systems to clear and settle claims for payment according to a unified set of rules, only require a licence (issued by the regulator, FINMA) if they are not operated by a bank and if their supervision is regarded as necessary for the functioning of the financial market or the protection of the market participants. Other online payment systems do not require a FINMA licence.

Under Swiss anti-money laundering (AML) regulations, the operation of an online payment system qualifies as financial intermediation subject to supervision and legal obligations. Swiss AML regulations only apply if the operator maintains a physical presence in Switzerland, meaning that it has a subsidiary, branch or office in Switzerland or otherwise engages persons in Switzerland on a commercial and continuous basis who represent the operator in connection with the payment process or advertising. According to FINMA's practice, a physical presence is already given if a point of sale of an electronic means of payment or a customer service centre exists in Switzerland. Specific rules apply to means of payments such as prepaid cards for which exemptions are available depending on certain thresholds.

Just like AML regulations, banking regulations apply to any activity which is not merely cross-border but involves physical presence of a service provider. If, at any time during the payment process, money is accepted and stored (so-called "deposit-taking"), such receipt of funds from the public may be regarded as regulated banking activity and require a banking licence. Electronic means of payment which cannot load more than CHF 3,000 and if no interest is paid, are notably exempt.

If electronic means of payment (such as customer cards) provide a credit function, e.g. by allowing an overdraft, the Consumer Credit Act applies, which requires a licence to extend interest-paying consumer loans and regulates the conditions for such loans. The Consumer Credit Act scope of application extends to all loans offered to customers in Switzerland, which includes loans offered from abroad.

To date, Switzerland has not planned to implement a payment services regulation similar to the European framework of PSD II.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

A provider of an online payment system which may be regarded as necessary for the functioning of the financial market or the protection of the market participants must apply to FINMA for a licence (see above response to question 11.1). However, this is not usually the case.

Furthermore, a provider of an online payment system or electronic means of payment with physical presence in Switzerland (see above response to question 11.1) is subject to the obligation to affiliate with a Swiss self-regulatory organisation (SRO) and to comply with Swiss AML rules, as well as the regulations of the SRO. Such obligations include, among other duties, the identification of the customers, assessment of certain transactions and reporting to the Laundering Reporting Office Switzerland in case of suspicion. The regulator has developed specific standards for online and video identification.

In case of a physical presence in Switzerland, a potential banking licence requirement must be assessed if money is received from customers and stored.

If the online payment system or electronic means of payment involves a credit function, e.g. by allowing an overdraft, the extension of interest-paying loans to consumers located in Switzerland, even if provided cross-border, requires a consumer credit licence and is subject to the requirements for consumer credits.



Jürg Schneider is a partner in the Information Technology, Intellectual Property and Competition team, co-heads the firm's Data Protection practice and is in charge of the Lausanne office. His practice areas include information technology, data protection and commercial contracts. He regularly advises both Swiss and international firms on comprehensive global projects and digitalisation activities. He has deep and extensive experience in the fields of data protection, information security, and e-commerce, with a particular focus on transborder and international contexts. In addition, Jürg Schneider regularly publishes and lectures on ICT topics and is a member of several professional organisations. He is a member of the board of directors of the International Technology Law Association and former co-chair of its data protection committee. Jürg Schneider is listed in Chambers Europe, The Legal 500 and Who's Who Legal TMT.

Walder Wyss Ltd
Av. du Théâtre 1
1005 Lausanne
Switzerland

Tel: +41 58 658 80 00 / +41 58 658 55 71
Email: juerg.schneider@walderwyss.com
URL: www.walderwyss.com



Hugh Reeves is a managing associate in the Information Technology, Intellectual Property and Competition team. He specialises in technology transactions, telecommunications, e-commerce, commercial contracts, as well as information technology, and advises clients of all sizes on their deployment and commercial activities in Switzerland. Hugh is also active in the areas of data protection and intellectual property and regularly publishes in his areas of practice.

Walder Wyss Ltd
Av. du Théâtre 1
1005 Lausanne
Switzerland

Tel: +41 58 658 80 00 / +41 58 658 52 73
Email: hugh.reeves@walderwyss.com
URL: www.walderwyss.com



Maria Gentile is a senior associate in the firm's Tax team. She specialises in all aspects of domestic and international tax matters, regarding both individuals and corporate entities and is particularly active in the field of value added tax (VAT). Maria regularly represents her clients in proceedings before the tax authorities and the courts and advises *inter alia* on matters of tax planning and wealth reorganisation.

Walder Wyss Ltd
Rue d'Italie 10
1204 Geneva
Switzerland

Tel: +41 58 658 30 00 / +41 58 658 30 37
Email: maria.gentile@walderwyss.com
URL: www.walderwyss.com

Walder Wyss is one of the main actors of the Swiss legal services landscape with more than 240 lawyers. Its competencies in particular include providing advice on e-commerce, commercial contracts, intellectual property, data protection and all types of local or cross-border transactions. Our lawyers possess market-leading and peer-recognised knowledge in their respective practice areas. With offices across the country and experts in virtually all areas of the law, Walder Wyss offers its clients all the legal assistance they may require.

www.walderwyss.com

walderwyss attorneys at law

Taiwan

Lee and Li, Attorneys-at-Law



Robin Chang



Eddie Hsiung

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

With respect to B2B, there are no specific e-commerce rules in Taiwan. Therefore, from the Taiwan legal perspective, generally e-commerce is not treated differently from non-e-commerce businesses and is subject to the Taiwan Civil Code (specifically provisions governing contracts) and other laws and regulations that may apply, such as the Personal Data Protection Act (PDPA) to the extent personal data is involved. Nonetheless, the chance that the Electronic Signature Act (ESA) would apply is generally higher for B2B e-commerce (so far as the “electronic signature” defined under the ESA is concerned). Except for the general registrations required for company formation (from the perspectives of corporate, tax and import/export) and for those required for regulated entities, there are no registration requirements for B2B e-commerce.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In Taiwan, the main laws governing B2C e-commerce include the Consumer Protection Act (CPA) and the Guidelines for Consumer Protection in the Context of Electronic Commerce (E-Commerce Guidelines).

According to the CPA, subject to relevant conditions, restrictions and exceptions, online consumers are entitled to a seven-day “hesitation period”. In other words, consumers can rescind the contract within seven days by returning the goods or sending a written notice, upon receipt of goods or services. Under such circumstance, consumers are not required to state any reason or be responsible for any expense or cost. Also, to protect consumers, Taiwan’s regulators have been paying attention to certain specific types of goods, services and business models, and have promulgated certain templates for standardised contracts and/or provisions that shall/shall not be included in the standardised contracts (Consumer Protection Provisions); therefore, B2C e-commerce operators should comply with such Consumer Protection Provisions to the extent applicable.

The purpose of the E-Commerce Guidelines, known as the government’s guidelines for better enforcement of the CPA, is to ensure fair trade, to protect consumers’ rights and interests, to build consumers’ trust in e-commerce mechanisms, as well as to promote the development of e-commerce. The E-Commerce Guidelines provide for the relevant rules and guidelines that e-commerce operators need to follow when conducting business activities, advertising, and marketing. For example, consumers should be given the right to decide whether to receive advertising emails. In addition, when designing an e-commerce platform or an e-payment system, the needs of the disabled should be taken into consideration.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Under Taiwan law, the PDPA is the main law governing personal data protection. Under the PDPA, unless otherwise specified, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing, or using any of said individual’s personal information, subject to certain exemptions.

It is noteworthy that in response to the implementation of the GDPR, the Taiwan government has been contemplating amending the PDPA to obtain the Adequacy Decision from the EU, although this proposal is still under discussion. Also, some fintech industry players specifically advocate that the PDPA should be amended to grant the “right to data portability” to the individuals as the same provided for under the GDPR.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

With respect to personal data protection, under the PDPA, an organisation would generally need to, for example, establish a sound practice for obtaining sufficiently informed consent from the data subject in order to properly use the collected data internally and transmit the same to others, as well as to establish appropriate and feasible internal rules, policies and mechanisms for personal data protection to meet relevant regulatory obligations. For any multinational company group with a presence, business and/or customers in other countries/jurisdictions, it should also pay attention to applicable data protection law of such jurisdictions such as the GDPR. In addition to the above, we wish to illustrate the following two topics which are being hotly discussed in Taiwan:

1. Open banking: In response to the advocacy of “open banking” from some industry experts and market players, the Financial Supervisory Commission (FSC) has demanded the Bankers Association to set out relevant self-regulatory rules to implement the concept of open banking in Taiwan. The FSC did not wish to set out mandatory disclosure rules for banks, and instead, to ask the self-regulatory organisation (i.e., the Bankers Association) and the Financial Information Service Co. to set out relevant rules and information security standards for banks to follow. The goal is to provide the third-party financial service providers (TSPs) with open access to consumer banking, transaction, and other financial data from financial institutions through the use of APIs. If any personal data is involved, making the data available by the financial institutions to the TSPs should be subject to the PDPA.
2. De-identification: According to a ruling issued by the Ministry of Justice in August 2018, personal data that has been de-identified by the use of various technologies and is presented in such a way that it is no longer possible to directly or indirectly identify particular individuals does not fall within the definition of “personal data” under the PDPA and thus the collection, processing, or use of such de-identified personal data will not be subject to the PDPA. However, it is suggested that an organisation should be aware of and hold a cautious attitude towards the practice and techniques of “de-identification”, since there are no clear rules as to whether any specific personal data should be deemed to have been “de-identified” from the PDPA perspective.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Taiwanese government bodies, as well as data protection authorities are taking an encouraging attitude toward the developments in areas such as fintech, retail, AI, and digital health. Certain authorities provide answers to the FAQs regarding personal data protection on official websites, host seminars upon regulatory changes, provide official guidance for digital businesses regarding data protection and allow businesses to seek advisory opinions on how to comply with relevant regulations.

Regarding the promotion of the digital health industry, it is noteworthy that through national health insurance, which is a compulsory social insurance programme organised by the Taiwanese government, the Ministry of Health and Welfare has accumulated a huge database of medical data. For the purposes of health promotion, disease management, etc., an entity that meets relevant requirements can apply for access to data in the National Health Insurance system after completing the de-identification process.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The Cybersecurity Act, which took effect on 1 January 2019, is the first cybersecurity-focused legislation in Taiwan; thereafter, a series of related rules and regulations have been promulgated by relevant government agencies. Pursuant to the Cybersecurity Act, companies are required to meet certain obligations (such as requirements for maintaining a specific security level, setting up

relevant internal rules for implementing plans for maintaining information security, reporting to the government in case of any cybersecurity incident, etc.) under the Cybersecurity Act if they are designated by the Taiwanese government as the “critical infrastructure provider” (CIP).

Government agencies as well as the CIPs are required by the Cybersecurity Act to adopt cybersecurity maintenance plans and report any cybersecurity incident to the superior/supervisory governmental authorities. For this purpose, a few government authorities have already issued relevant guidelines for cybersecurity plans in this regard for reference by the businesses that are subject to their supervision. It has been anticipated that the Cybersecurity Act will reshape cybersecurity in Taiwan. In addition, the Taiwanese government believes that cybersecurity is a matter that concerns national security, and the Legislative Yuan enacted certain amendments to the National Security Act in 2019, under which the protection of national security shall include the security of cyberspace as well as the physical space, in the territory of Taiwan.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

There is no general cybersecurity legislation other than the Cybersecurity Act. However, there are several laws and regulations in Taiwan that may be relevant to cybersecurity such as the PDPA, Criminal Code, etc. For example, pursuant to the PDPA and relevant regulations, any company that possesses personal data has the general obligation to adopt proper security measures to protect such data from being stolen, altered, damaged, destroyed, or disclosed.

In practice, as to how companies in the private sector deal with any concerns in relation to cybersecurity, larger enterprises in Taiwan may tend to adopt more comprehensive solutions to potential security issues and concerns, and it is not uncommon to see internal or external IT specialists or consultants engaged to design and implement relevant operating procedures for cybersecurity. However, small or medium-sized enterprises in Taiwan tend to purchase packaged software or procure other “one-stop” solutions to address potential cybersecurity issues and for compliance with relevant laws, regardless of whether cybersecurity incidents may be actually effectively monitored or prevented from a technical viewpoint.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

According to official statistic data from the Department of Statistics, the Ministry of Economic Affairs (MOEA), with the emergence and expanded use of the internet and the revolution in consumers’ spending habits, the retail businesses combining digital tools (e.g., e-commerce platform, e-payment methods, etc.) and social network sites are experiencing rapid growth. For example, the annual turnover of the online retail industry reached NT\$34.18 billion in 2020, with an annual growth rate of 18.97% (the growth rates in 2018 and 2019 were 12.26% and 14.12%, respectively). In addition, online sales accounted for 8.86% of the total turnover of the retail industry in 2020 (such percentages were 6.24%, 6.74%, and 7.46% from 2017 to 2019, respectively). It is expected that e-commerce industries allowing

consumers to shop without physical contact will continue to thrive in the future.

Although the use of e-commerce services is common, cash and credit cards are still the most common ways to pay for purchases. Take the retail industry for example, cash (including cash on delivery) accounted for 35.1% of consumers' payments, credit cards accounted for 37.9%, and payments with mobile phone (including but not limited to the "e-payment" defined under Taiwan's Electronic Payment Institutions Act) accounted for only 2.8% in 2020.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

As stated in our response to question 4.1, according to official statistics, most consumers in Taiwan still use cash or credit cards. However, it is noteworthy that the government has been actively promoting mobile payments since 2018, hoping to reach the goal of 90% mobile payment penetration by the year 2025. According to relevant official statistics, the percentage of domestic mobile usage rose to 62.2% in 2019 from 50.3% in 2018 and the total number of users of e-payment (i.e., the e-payment defined under Taiwan's Electronic Payment Institutions Act) has reached 12.49 million (more than half of Taiwan's population) as of the end of February 2021.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

In our view, the answer is no.

Also, although we noted from relevant news reports that some Taiwan retailer websites or e-commerce platforms tried to expand overseas, based on the fact that the Taiwanese market still has room for growth and due to other commercial or legal considerations (including but not limited to logistics, marketing, tax issues), it appears that these companies are still focusing on local markets.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Please see our response to question 4.3. Please note that, in our view, language is not the major barrier for Taiwanese e-commerce firms doing business in other jurisdictions. Taiwanese e-commerce firms doing business in other jurisdictions usually need to use local languages for the targeted customers in such foreign markets by leveraging the employees and specialists in those markets.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

It is generally understood that an aesthetically pleasing web-interface design with comment functions, multiple payment methods, clear pictures, and descriptions of products will be

deemed as a consumer-friendly web-interface design and thus attracts more consumers.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Please see our response to question 4.1. The statistics show that more and more people in Taiwan tend to purchase goods and services through retailer websites or e-commerce platforms. The COVID-19 pandemic encourages this development because more consumers would like to stay home and shop online or order food online through food delivery services, such as Uber Eats and Foodpanda.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Trademark

According to Taiwan's Trademark Act, trademark infringement damages may be claimed through civil procedure. As for criminal liability for infringement of trademark, the offender shall be punished with imprisonment for a period not exceeding three years or a fine not exceeding NT\$200,000, or both, if he or she: (1) uses a trademark that is identical to the registered trademark in relation to identical goods or services; (2) uses a trademark that is identical to the registered trademark in relation to similar goods or services and hence there exists the likelihood of confusion to relevant consumers; or (3) uses a trademark that is similar to the registered trademark in relation to identical or similar goods or services and there exists the likelihood of confusion for relevant consumers. While the trademark owner may take the above-mentioned civil or criminal actions depending on individual circumstances, it is also common in Taiwan that a trademark owner engages a local law firm to send the demand letter to the infringer, or even "cooperate" with local IP police (specialising in investigation of criminal violation of the Trademark Act) to "monitor" counterfeiting activities proactively.

Domain Name

In local practice, Taiwan Network Information Center (TWNIC), a foundation formed under the supervision of the government, has established the "Domain Name Dispute Resolution Rules" (DNDR Rules) for resolving disputes relating to domain names. Pursuant to the DNDR Rules, a complainant may file with the TWNIC for resolving the dispute if (1) the registered domain name is identical or confusingly similar to a trademark, symbol, name, corporate name or other emblem of the complainant, (2) the registrant has no rights or legitimate interests in the domain name, and (3) the registrant has registered or used the domain name in bad faith. An eligible dispute resolution institution shall be a neutral body recognised by TWNIC, which are currently the Science & Technology Law Institute and the Taipei Bar Association.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

The domain name dispute resolutions mentioned in our response to question 5.1 above may only deal with the cases where the dispute concerns the domain name that has Taiwan's country code top-level domain, i.e., ".tw".

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

With respect to the services rendered by third party-owned data centres or cloud providers, the PDPA will be applicable, as an organisation using the cloud/data storage service will carry out the activities of collecting data from the data subjects, which would then be passed to a service provider for processing and use. Pursuant to the PDPA, such organisation may be held liable to its customers if the service provider does not comply with the PDPA.

On the other hand, if an organisation in Taiwan intends to procure cloud/data storage services outside Taiwan, in addition to the relevant requirements for international transmission under the PDPA, such organisation should also check whether it is subject to any sector-specific regulations for outsourcing data processing or even storing data outside Taiwan. For example, financial institutions may be subject to prior approval from the financial regulator, the FSC, for their outsourcing activities involving cloud-related services. Also, for some industries, customers' data is prohibited from being transferred to China, such as telecommunications and broadcasting operators, TV channels and cable TV system operators, due to national security concern.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

With respect to data localisation, there are no general data localisation requirements in Taiwan, with certain exceptions such as the customers' data of a bank should be deposited in Taiwan in principle.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

In Taiwan, when a Taiwan consumer purchases any goods from an offshore e-commerce platform, normally a customs broker would be engaged to carry out the customs declaration process, and only after completion of such process can the goods be delivered to the recipient's address by a logistics provider in Taiwan. Since May 16, 2020, the Customs Administration, Ministry of Finance launched the "EZWAY App", which can be used to verify the shipments with the consignee (for Taiwan citizens/R.O.C. nationals only) on a "real-name" basis. Through the App, a consignee may complete the customs clearance process as long as his/her identity has been registered with such App. This App is adopted in order to implement and expedite the customs clearance procedure with new technology, with an aim to protect the personal data of the customers, as well as to prevent unlawful acts involved in customs clearance process (e.g., misrepresentation made to customs).

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

In our view, a noteworthy barrier in local practice is that smaller companies might not have sufficient resources to adopt digital technologies and incorporate digital transformation trends, especially during the COVID-19 pandemic. Generally speaking, a possible solution might be for the Taiwan government to provide more support and resources to those companies to help them leverage digital technologies more efficiently.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Currently, in Taiwan, there are no tax incentives specifically provided for digital businesses, while offshore e-commerce service providers may, for example, be entitled to tax-exempt under relevant tax treaty (if applicable), subject to the approval by the Taiwan tax authority.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

For cross-border e-commerce transactions, whether an offshore e-commerce operator would need to make relevant tax registrations and make relevant tax filings in Taiwan has been an issue widely discussed in Taiwan. Take income tax, for example. There is an issue as to whether the source of income is within Taiwan territory for offshore e-commerce service providers rendering services to Taiwan customers, which might easily lead to disputes.

Another tax-related issue hotly debated in Taiwan is the tax treatment of cryptocurrencies, which is still unclear mainly because it is rather difficult for the tax authority to gain sufficient knowledge about the economic features of every type of cryptocurrency in order to set out fair and reasonable tax rules in response thereto.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

From a Taiwan legal perspective, there are two primary methods concerning resourcing work in Taiwan: employment and independent workers (on a contractual basis).

Generally speaking, in case of "employment" (i.e., the employee has a subordinate relationship with the employer and thus falls within the definition of "worker" under the

Labour Standards Act (LSA)), while an employee would need to act under the instruction and supervision of the employer, the employer would be subject to more legal requirements provided for under the LSA or other labour-related laws and regulations intended for providing “minimum protection” to employees. For example, an employer may not terminate an employment contract unilaterally unless any of the events specified in Article 11 (layoff with advance notice and severance pay) or Article 12 (dismissal without notice or pay) of the LSA occurs. Also, in local practice, generally an employee may be entitled to employment-related benefits such as employment insurance coverage.

As to a company engaging independent workers, unless otherwise provided for in the contract, the company’s termination of the employment contract is subject to less restrictions and requirements and, generally speaking, the LSA (and other labour-related laws and regulations) would not apply, meaning the compliance costs are generally lower. However, the company would have less “control” over the independent workers in terms of the assigned tasks, so there could be higher costs to ensure the quality of the work or services provided by the independent workers.

Please note that the courts in Taiwan have their own discretion to determine whether a “subordinate relationship” exists between two parties and whether labour laws will apply.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation’s physical premises?

According to the LSA, in principle, the determination of a workplace and any changes afterward shall be agreed upon by both the employer and the employee. Although the employer may instruct an employee to carry out work away from an organisation’s physical premises, such instruction shall comply with relevant statutory requirements. For example, according to Article 10-1 of the LSA, any relocation must not breach the provisions of the employment contract and must follow the following principles:

1. the employee may only be relocated based on the company’s business needs and without improper motives or purposes, unless otherwise provided for in the laws and regulations;
2. the wages and other working conditions shall not be changed to be unfavourable to the employee concerned;
3. the employee shall still be able to satisfactorily perform the duties required in terms of physical ability and skills after the redeployment and relocation;
4. the employer shall provide necessary assistance if the relocated workplace is too far away for the employee concerned; and
5. the livelihood interests of the employee and his or her family shall be considered.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Due to the COVID-19 pandemic and the advances in communication technology and internet access, teleworking has become an accepted practice in many offices. In 2020, many companies in Taiwan changed their workplace policies and encouraged employees to work from home, and we expect that this trend will continue. However, there are no specific regulations

regarding issues that arose accordingly (e.g., how to maintain worker attendance records in the work-from-home situation), so it is generally expected that the LSA would need to be re-examined to address the situations resulting from COVID-19 as well as the remote working trend.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

In our view, the most essential legal issue faced by a digital business operating in Taiwan is the difficulty in making best use of data under the current personal data protection regime in Taiwan, especially in fintech and digital health areas. Please see our responses to questions 2.2 and 2.3 above.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

From a legal perspective, we do not think there are any notable advantages for a digital business in Taiwan compared to other jurisdictions, but from a commercial perspective, as mentioned in our response to question 4.3, the Taiwan digital business market still has room for growth.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

According to our observation, the government is now focusing more on the laws and regulations governing online payments. Please see our responses in Section 11 below.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The Electronic Payment Institutions Act (E-payment Act), which governs the online payment sector in Taiwan, was enacted in 2015. The E-payment Act mainly regulates the activities of electronic payment institutions that engage principally in: (i) collecting and making payments for real transactions as an agent; (ii) accepting deposits of funds as stored value funds; and (iii) transferring funds between e-payment accounts.

In December 2020, Taiwan’s parliament, the Legislative Yuan, made an amendment to the E-payment Act, which will take effect on 1 July 2021. Under the amended E-payment Act, the scope of business of a new e-payment institution will include (1) core businesses, and (2) ancillary and derivative businesses. For the core businesses, in addition to the existing businesses of (i) collecting and making payments for real transactions as an agent, and (ii) accepting deposits of funds as stored value funds, small amount domestic and cross-border remittance services and foreign exchange services relating to the core businesses will also be opened to e-payment institutions from the effective date of the amendment. The ancillary and derivative businesses are all new to the e-payment institutions, which include (a) assisting the contracted merchants with integration and

transmission of acquiring and payment information, (b) sharing terminal equipment at the contracted merchants, (c) assisting the information exchange between the users and between the users and the contracted merchants, (d) providing an electronic Uniform Invoice system and its value-added services, (e) taking custody of paid price of vouchers/tickets of goods/services, and assisting in the issuance, sales, validation and related services for vouchers/tickets, (f) providing services for integration of bonus points and offsetting/settling payments for real transactions with bonus points, (g) providing value storing blocks in electronic stored value cards or application programmes for use by others, (h) providing any planning, instalment, maintenance or consultancy services for the information system and facilities in relation to the above seven ancillary and derivative businesses of e-payment institutions, and (i) other businesses approved by the competent authorities.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Online payment providers may be interested in understanding the scope of the businesses that they may carry out under the amended E-payment Act, which would be subject to further interpretation by the FSC. Therefore, it is suggested online payment providers closely follow the development of the enforcement and implementation rules and regulations to be further set out or adjusted under the amended E-payment Act.



Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on banking, IPO, capital markets, M&A, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan, including providing advice on compliance and regulatory issues, setting up a banking branch or bank subsidiary in Taiwan and customer complaints. He has been involved in many M&A transactions of financial institutions. He has also been involved in government projects in e-payment regulations in Taiwan.

Lee and Li, Attorneys-at-Law
8th floor, No. 555
Section 4, Zhongxiao East Road
Taipei 11072
Taiwan, R.O.C.

Tel: +886 2 2763 8000 ext. 2208
Email: robinchang@leeandli.com
URL: www.leeandli.com/en



Eddie Hsiung is licensed to practise law in Taiwan and New York. His practice focuses on M&A, securities, financial services, general corporate and commercial, start-ups, etc. He has participated in many corporate transactions (M&A, IPO, JV, cross-border investments) spanning a broad range of industries and areas, including TMT, bio-tech, big data, digital financial services, etc. In addition to the abovementioned traditional practice areas, he is familiar with legal issues regarding digital economy, digital transformation and the application of new technologies, such as fintech, blockchain, virtual assets, AI, data protection, and is often invited to participate in public hearings, seminars, and panel discussions to provide advice to the government, regulators, legislators and university/research institutions in these areas on regulatory policies.

Lee and Li, Attorneys-at-Law
8th floor, No. 555
Section 4, Zhongxiao East Road
Taipei 11072
Taiwan, R.O.C.

Tel: +886 2 2763 8000 ext. 2162
Email: eddiehsiung@leeandli.com
URL: www.leeandli.com/en

Lee and Li, founded more than half a century ago, is the largest law firm in Taiwan providing legal services in the Greater China area by collaborating with law firms and intellectual property agencies in Mainland China. Besides our headquarters in Taipei, we have offices in Hsinchu, Taichung and Kaohsiung, as well as strategic alliances in Beijing and Shanghai. Our services are performed by a total of around 860 employees, including nearly 200 Taiwan-qualified lawyers, 50 foreign lawyers, over 100 Taiwan patent agents/patent attorneys, more than 100 technology experts, and specialists in other fields such as Taiwan and U.S. certified public accountants, as well as the PRC patent attorneys and PRC-qualified lawyers of our strategic alliances. We restructured our resources and formed practice groups, which span six departments (banking and capital markets, corporate and investments, trademark and copyright, patent and technology, litigation and dispute resolution, and Japan practice). Our professionalism and achievements have long been recognised by international professional institutions.

www.leeandli.com/en



United Kingdom

Charles Russell Speechlys LLP



Jason Saiban



Caroline Swain

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

There are no specific registration requirements that apply to an “online business” over and above the usual registration requirements that apply to all businesses.

All online traders are required to provide a certain amount of mandatory information to their service users. The Trading Disclosures Regulations 2015 require companies to provide details of the company’s registered name, registered number, registered office, confirmation of the part of the UK in which the company is registered and details as to whether the company is a limited company or has another company structure. Online traders should display this information on their business letters and order forms and on all websites.

The E-Commerce Regulations 2002 (the “Regulations”) apply to both B2B and B2C e-commerce, although online traders can contract out of most requirements in a B2B context. The Regulations require online traders to provide a certain amount of mandatory information to their service users; most information is required before a service user places an order (i.e. pre-contract). As a minimum, online traders must provide their name, address, email address, company registration number, VAT number (if applicable) and details of any supervisory authority (if subject to an authorisation scheme). It is accepted that including such information on their website satisfies the requirement to ensure the aforementioned information is easily, directly and permanently accessible.

If an online trader provides services (rather than goods), the Provision of Services Regulations 2009 should also be considered. In addition to the mandatory information above, an online trader must provide sufficient detail on the main features of the service including details of any multi-disciplinary services and any non-judicial dispute resolution procedures to which the online trader may be subject. An online trader must also provide its general terms and conditions (if applicable) and contact details to use for requesting further information or making complaints.

Under English law, it is possible to enter into simple contracts electronically and electronic signatures are accepted. However, it is not certain whether deeds can be executed by electronic means and the approach to the formality requirements continues to develop. As with written contracts, the terms of online contracts must be clearly brought to a service user’s attention before the contract is formed to be binding.

Importantly, Brexit and the end of the UK-EU transition period have had little impact on the UK rules that regulate trading online, even though the key legislation in this area is EU-derived.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In addition to the mandatory information requirements required within a B2B context, the Regulations also require online traders to provide additional information about the electronic contracting process, where operating in a B2C context. Online traders must outline, prior to the placing of an order, the different technical steps required to conclude the contract, the contract languages offered and details of how the consumer can identify and correct input errors prior to placing their order. Online traders must also provide an order confirmation without undue delay. In addition, if the pre-contract information was not initially provided in a durable form, online traders must provide this to consumers at the order confirmation stage.

Online traders must also comply with two consumer-specific regulations: the Consumer Contracts Regulations 2013 and the Consumer Rights Act 2015.

The Consumer Contracts Regulations require online traders to supply additional pre-contract information to consumers. This includes confirmation of the main characteristics of the goods, services or digital content, the total price or the manner in which it will be calculated, which means of payment are accepted, any delivery restrictions or additional delivery charges and, for contracts with an indeterminate length, information about the total costs per billing period or the total monthly costs must be provided. Under the Consumer Rights Act, consumers generally also have a right to cancel online contracts and receive a refund within a 14-day “cooling-off” period. Any right to cancel, including any applicable conditions, i.e. a requirement for a consumer to pay the delivery costs of returning the goods to the online trader, must be clearly communicated to consumers.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Data protection law is probably one of the fastest developing

areas of law internationally, and this is certainly the case in the UK. There have been numerous developments in legislation, regulatory guidance and case law in the last year. Some of the most significant events are listed below:

Brexit. As a result of Brexit, from 1 January 2021, the General Data Protection Regulation 2016/679 (EU) (GDPR) no longer applies in the UK. Instead, the Data Protection Act 2018 (as now amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019)) now applies a separate regime under the 'UK GDPR'. Whilst the GDPR and EU GDPR remain alike in substance, the very fact that the UK courts and CJEU jurisprudence will inevitably diverge over time means that Brexit will have a significant long-term impact.

Continued regulatory guidance. The UK ICO has continued to develop its regulatory guidance, complementing the provisions of the UK GDPR. The introduction of the ICO Children's Code (or 'Age Appropriate Design Code') in September 2020, which the ICO will begin to apply from September 2021, and the publishing of the ICO Data Sharing Code of Practice in December 2021, which will apply once the code has received parliamentary approval, were of particular significance.

Regulatory enforcement. In the last 12 months, the ICO has for the first time issued multi-million-pound fines, exercising its power to do so under the GDPR (now the UK GDPR). These fines have included:

- British Airways: £20,000,000 – for a data breach affecting more than 400,000 customers.
- Marriott International Inc: £18,400,000 – for failing to keep customers' personal data secure.
- Ticketmaster UK Limited: £1,250,000 – for failing to protect customers' payment details.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

A number of privacy challenges are relevant in these areas. These include how to manage the quality of data being deployed (and the related potential impact on individuals' right to privacy), the challenges of making these complex areas transparent and explainable, security and, underpinning each of the above, the need to develop and compete internationally in this fast-moving area.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

In 2016, the UK Government launched a National Cyber Security Strategy with the objective of making the UK secure and resilient to cyber threats. This had various parts, one of which was the setting up of the National Cyber Security Centre which assists organisations with cyber resilience.

There are various other initiatives from both the Government and the privacy regulator, including:

- Fintech: UK Government for industry, including FinTech Export Academy and FinTech Champions scheme.
- AI: ICO publication: Guidance on AI and data protection (July 2020), ICO and Alan Turing Institute publication: Explaining decisions made with Artificial Intelligence (May 2020), existence of the AI Council (an independent expert committee advising the UK Government on artificial intelligence).

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

In common with most jurisdictions, the UK does not have an overarching cybersecurity legal framework. Instead, cybersecurity is regulated by a mixture of cybersecurity, privacy and national security legislation, many of which will be relevant to e-commerce businesses. These include primarily:

- The Data Protection Act 2018 and UK GDPR – which govern the processing of personal data by any organisation.
- Network and Information Systems Regulations 2018 – which impose various cybersecurity and incident reporting obligations on 'relevant digital service providers' (the definition of which can include e-commerce businesses).

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The following legislation may also be relevant (although to a lesser degree) to e-commerce businesses:

- Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Communications Act 2003.
- Computer Misuse Act 1990.
- Official Secrets Act 1989.
- Investigatory Powers Act 2016.
- Specifically in relation to the financial services sector, the FCA Handbook and PRA Rulebook.

These pieces of legislation are enforced by a number of regulators, including the Information Commissioner's Office, Ofcom (the UK's communications regulator) and the Financial Conduct Authority (one of the key UK financial regulatory bodies).

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

E-commerce is widely used and accepted within the UK as a means of obtaining goods and services. We have heard from clients working in e-commerce that during the Covid-19 pandemic their sales increased substantially from both new and existing customers. Interestingly, the new customers have come from customer groups that were previously not regular e-commerce users, which demonstrates how Covid-19 has influenced shopping habits. It is unclear whether this trend will continue following the Covid-19 pandemic.

According to the Bank of England, debit cards overtook cash as the most frequently used payment method in the UK in 2017. It is widely felt that the Covid-19 pandemic will hasten the decline of cash in the UK.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The UK is a nation of debit and credit card holders – while

mobile payments are just one step removed from card payments, uptake in the UK has been surprisingly low particularly in contrast to other comparable nations. It is thought that the reason for this is that debit and credit card trends like contactless payments were advanced in the UK before smartphones became widespread.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

There is no evidence that UK-based websites perform better on average in other jurisdictions than in the UK.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

E-commerce firms in the UK are able to rely somewhat on the widespread use of the English language around the world when selling products/services in other jurisdictions. As a result, this has not been a huge focus for e-commerce firms in the UK.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

User-friendly, simple but impactful interfaces are preferred by consumers in the UK.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Yes, as described above, Covid-19 has sped up the decline in the use of cash in the UK and the increase in reliance on e-commerce as a means of obtaining goods and services. It is anticipated, albeit not guaranteed, that these trends will have a lasting effect.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Online brand infringement can take various forms. These include using a brand name as part of or as a domain name, and selling infringing goods or services.

Online Marketplaces

Infringing goods do find their way onto online marketplaces, such as eBay and Amazon. Such platforms often have procedures allowing brand owners to report infringement using these notice procedures, in order to remove the infringing products from the online platforms.

Amazon has an online form to complete once you have signed in using a registered Amazon account. The form requires the nature of infringement (copyright, trade mark, design, etc.), the details of the protected brand, and any further information demonstrating how the infringing goods are infringing the brand owner's rights.

Similarly, eBay has its own procedure, whereby the brand owner must to complete a Notice of Claimed Infringement form, and send it to a dedicated email address. The form is similar to that of Amazon; the brand owner must detail the nature of infringement, the rights that have been infringed and provide further information demonstrating infringement.

Domain Name Complaints

Occasionally, third parties will either inadvertently or deliberately take advantage of your brand and use it as part of a domain name. In the first instance, brand owners may write to the Registrant (the individual or entity who registers the domain name) requesting them to cease using the domain name and perhaps transfer it. If the negotiating route is not successful, you may initiate a dispute resolution procedure. The Nominet Dispute Resolution Service can handle disputes that relate to '.co.uk' and other '.uk' domain names.

For the Nominet Dispute Resolution Service, brand owners would need to demonstrate (1) rights in the brand, and (2) that the domain name is an abusive registration when in the name of the Registrant.

There is a list of factors that can be used as evidence to demonstrate that the domain name is an abusive registration. One of those factors is that the primary purpose of registering the domain name is to prevent the brand owner from using it and of disrupting the brand owner's business.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Online Marketplaces

Brand owners are entitled to file takedown requests using marketplaces own procedures provided that they have, and can demonstrate, their rights. These requests are assessed by the online platform which may decide it needs more information in order to fulfil the request. Sometimes, the platforms do not find the evidence strong enough to establish infringement, resulting in the supposedly infringing products not being taken down.

There are some instances where the online marketplace will not recognise certain aspects of infringement. For example, Amazon does not enforce Barcode, EAN or UPC infringement, which store product information (e.g. pricing and inventory levels) as they do not carry intellectual property protection.

Brand owners should note that following Brexit, an EU trade mark no longer covers the UK. If the EU mark was registered as at 31 December 2020 then a so-called comparable UK mark will be created automatically. If, however, the EU application was still pending at that date then a comparable UK trade mark application should be filed in the UK. If a brand owner does not have registered trade mark protection, they may have a claim in passing off, but this is a high threshold to achieve and marketplaces will be much more reluctant to respond positively.

Domain Name Complaints

Since the introduction of the General Data Protection Regulation (GDPR), identifying the name and contact details of the Registrant has become much harder. This makes the process of initiating domain name recovery procedures more difficult than before and can lengthen and complicate the overall process of resolving the issue.

If the Nominet Dispute Resolution Service is used, there are defences that the Registrant can raise to indicate that the registration was not abusive. These include, but are not limited to, the domain name being generic or descriptive, or the domain being used fairly – for example for a fan site.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Data Protection

Generally speaking, colocation data centres are not regarded as “processing” data for the purposes of applicable Data Protection law – the Data Protection Act 2018. As such, colocation data centre operators are not regarded as data processors. However, care must be taken to ensure that beyond pure colocation activities, if the Data Centre operator does provide so-called “hands and eyes” services or any other services where it may be affecting personal data, a full analysis of those activities must be performed to establish whether any processing activities are taking place. Data centre operators are generally data controllers of data processed for their own employment, security and operations.

Now that the European Data Protection Board has published its opinion on adequacy for the purposes of GDPR (19 April 2021), EU Member States will proceed to approve the draft decisions under the comitology process, before the final adoption by the European Commission by the end of June 2021, it is likely the United Kingdom will not be a third country for the purposes of data transfers from the EU. Data centres and Cloud operators must ensure that their customers have put in place appropriate data transfer solutions for the transfer of personal data into and out of the United Kingdom where necessary.

Law Enforcement Access to Data

The Investigatory Powers Act 2016 provides British Intelligence Agencies and the Police with electronic surveillance powers if a warrant has been issued on the grounds of national security, the interests of economic wellbeing of the UK, or the prevention or detection of a serious crime. The UK Data Protection Act provides that the processing of personal data by competent authorities for law enforcement purposes (e.g. police investigating a crime and for national security purposes) is outside the scope of the GDPR and exempt from the provisions of Data Protection Act 2018 by way of parts 2 and 3 of the Act. Cloud operators generally have processes and procedures in place for dealing with law enforcement access to data requests. Colocation operators generally do not have any access to or control of data so are not usually subject to law enforcement requests.

There is also the possibility of extra territorial requests for access to data. For example, from the United States of America, the PATRIOT Act expands the ability of law enforcement to surveil citizens on the grounds of national security in tackling foreign terrorism, and the CLOUD Act allows federal law enforcement to compel US-based technology companies via warrant or subpoena to provide requested data stored on their servers, whether or not the data is stored in the US or on a foreign soil. The courts can reject or challenge warrants or subpoenas if by providing the data, there is a violation of the privacy rights of the foreign country in which the data is stored.

NIS Regulations

The Network and Information Systems (NIS) Regulations 2018 are the UK’s implementation of the European Union’s Network and Information Security Directive. These enable supervision by Member States of the cyber security of Operators of Essential Services and Relevant Digital Service Providers in each country.

Operators of Essential Services (OESs) include digital infrastructure, which are regulated by OFCOM.

Relevant Digital Service Providers (RDSPs) (online search engines, online market places or Cloud Computing Services), are regulated by the UK Information Commissioner (RDSPs).

The NIS Regulations apply where an OES or RDSP has its head office in the UK or has nominated a UK representative, and must be larger than a micro or small enterprise (generally, small enterprises have less than 50 staff and an annual turnover or balance sheet of €10 million).

The NIS Regulations apply to “Network and Information Systems” which are (1) Electronic Communications Networks as defined in Section 32(1) of the Communications Act 2003, and (2) apparatus used for switching or routing of the signals. The regulation applies to ensure that a relevant OES or RDSP’s network and information systems have sufficient security to prevent an action that compromises the data stored on related services they provide. This is not limited to third-party cyber threats, so a power or environmental failure in a data centre causing servers operated by an OES or RDSP could trigger a reportable event.

Energy Regulation

Note that for colocation services, power costs are a very significant proportion of the overall cost of operating a data centre. Some data centres are able to claim exemptions from environmental taxes by way of a reduction on the energy bill as members of an exemption to the UK’s Climate Change Agreement (CCA). You should check with your provider whether they are enrolled in this scheme, or the CRC Energy Efficiency Scheme which also operates.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Data Sovereignty

The concept of data localisation or data sovereignty is becoming heavily discussed in Government but does not yet have a formal legal definition. There are no general requirements in Data Protection law requiring data to be located in a particular territory; however, appropriate measures under the Data Protection Act 2018 must be taken in order to transfer data outside the UK to a third country.

The Companies Act 2006, Section 388 requires companies to keep accounting records at its registered office, or such other place as the directors think fit, and those records must at all times be open to inspection by the companies’ offices. If the accounting records are kept at a place outside the United Kingdom, accounts and returns with respect to the business dealt within the accounting records must be sent to and kept at a place in the United Kingdom and must be at all times be open to such inspection (Section 388 to Companies Act 2006).

UK Export Control

UK Export Control governs the transfer of international trade in certain sensitive goods, software and technology. The regime can apply to some intellectual property (specifically software code, primarily in relation to the dual-use export controls, i.e. where the item can be used for military purposes as well as commercial and civilian purposes), as well as in the case of items specifically designed for military use.

Outside the example of dual use (or military use software), it is unlikely UK Export Control would apply to data.

Specific care must be taken when dealing with Government or Defence sectors, and UK Public Sector Health to confirm that there are no specific requirements imposed as part of specific projects which could contain a restriction on the transfer of data.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

UK customs has long used digital technologies in its clearance processes. The growth in air traffic and the increased pressure to clear goods quickly led the UK to develop IT systems from the mid-1970s to process clearance requests more rapidly.

By the 1990s, the UK had developed the Customs Handling of Import and Export Freight (CHIEF) system. CHIEF was designed to review an application and provide an instant response to a customer within five seconds. Its functionality involves, *inter alia*, validating more than 50 data items, calculating the value of goods and the revenue to be charged and automating the payment and collection of duty.

CHIEF remains in use in the UK. As at 2017, it was estimated to process more than 99% of all import and export entries and was responsible for around 67 million import and export applications. However, because the technology was ageing, the UK introduced a new, complementary solution initially to work alongside CHIEF. The Customs Declaration Service (CDS) went live in 2018. It had been intended to replace CHIEF with CDS completely by March 2021. To that end, all traders were required to migrate from CHIEF to CDS by September 2020. However, CHIEF remains in place for trades into mainland Great Britain while CDS has replaced CHIEF in Northern Ireland. In April 2021, the Government advised businesses that CDS was still intended to be the “long-term replacement for the current CHIEF platform”.

Alongside the government software, traders will usually have in place their own software packages to help them complete customs applications. One solution, for example, stores the customer organisation’s commonly used entries on application forms in a CRM system and then repeats these entries predictively in any new form filled out by the user.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

The transition away from CHIEF to CDS has been far from seamless. As with any migration from one system to another, a certain amount of time may be required for users to adjust to the new system. HM Government has noted that CDS will need to provide new or different data based on the requirements of the Union Customs Code (UCC), established in May 2016. The Government advised businesses to consider investing in staff training for the proper use of CDS, as well as inviting software developers or community system providers to work closely with HMRC to prepare for CDS.

A number of criticisms have been levelled against CDS. In November 2020, Chair of the Association of Freight Software Suppliers Steve Bartlett told the EU goods sub-committee of the House of Commons that “CDS [was] causing grave concerns as it [was] unproven, [had] only been tested at a simplified level and [lacked] the functionality for the new customs processes”. Many stakeholders called on the Government to retain CHIEF as a fallback option in case CDS failed to work as well as hoped.

The UK departed from the European Union on 31 January 2020. The transition period negotiated under the EU-UK

Withdrawal Agreement came to an end on 31 December 2020. Since then, the number of customs applications is expected to rise by around 200 million entries per year. This increase in volume offsets some of the efficiencies generated by digitised customs systems. On the other hand, that makes digitised systems for the processing of applications – both on the side of businesses and the Government – even more vital. It is perhaps unfortunate that traders must contend with the higher levels of required use while contending with the requirements of a new customs system.

Towards the end of 2020, it was reported that software suppliers were having difficulties devising trader facing software solutions which were capable of interfacing with the new CDS service. The problems included developers finding bugs within CDS and not being willing to stake their reputation on something which was unproven.

As a result of Brexit and the provisions of the Northern Ireland Protocol negotiated as part of the EU-UK Withdrawal Agreement, the UK has been required to operate certain customs checks for goods moving between Great Britain and Northern Ireland. In November 2020, UK software supplier AMS informed HMRC that there was no realistic chance it would be able to develop a CDS compliant automated customs solution for traders by 1 January 2021. One estimate said solutions would not be ready until March 2021. Writing in May 2021, it is unclear the extent to which these problems have now been resolved.

To assist businesses in Northern Ireland to complete applications on CDS, the Government developed the Trader Support Service (TSS) which was billed as “a unique service that will ensure that businesses of all sizes can have import processes dealt with on their behalf at no cost”. TSS, which is designed to interface with CDS, went live on 21 December 2020 and attracted 25,000 registered users. It has been reported, however, that TSS operates at a slow speed with businesses reporting it could take several hours to make an application.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

The UK tax regime provides a number of reliefs and tax incentives, both for investors in digital businesses and the businesses themselves.

The Enterprise Investment Scheme (EIS) and the Seed Enterprise Investment Scheme (SEIS) allow growing independent digital businesses to raise new capital from UK-resident investors with the benefit of a range of reliefs from income tax and/or capital gains tax.

EIS relief, for example, is not limited to UK companies – the issuing company must have a UK permanent establishment, but the money raised can be used for qualifying purposes in the UK and elsewhere. Companies can raise up to £5 million from equity issues in one year (£10 million for so called knowledge-intensive companies) with an overall cap of £12 million (£20 million for knowledge-intensive companies).

Venture Capital Trusts (VCTs) are listed investment companies that raise capital tax efficiently from investors and then invest into independent unlisted companies. Digital businesses may take in money from VCTs.

In all cases, the rules are detailed and professional advice should be taken – investee companies are required to meet certain ongoing conditions for up to three years to avoid the clawback of tax reliefs at shareholder level.

The UK operates a system of Research & Development (R&D) tax credits and expenditure credits, which can provide significant benefits to both SMEs and larger companies, respectively. The UK Patent Box regime also provides a reduced 10% rate of corporation tax rate on profits from patents and similar intellectual property.

With the announcement of a significant increase in UK corporation tax rates to 25% from 19% effective as of 1 April 2023 and the Government's public commitment to enterprise and technology, we can expect to see further initiatives here.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The pressure on the Government to improve public finances, together with the continuing focus on cross-border taxation, transparency and both perceived and actual tax avoidance, will weigh heavily on the relationship between the taxpayer and tax authorities for the foreseeable future.

HMRC's focus on actual and perceived tax avoidance will continue – the use of contractors and payroll taxation has been and will remain a priority. Transfer pricing, and a range of anti-avoidance provisions designed to protect the UK fiscal base (e.g. diverted profits tax) will be areas of likely dispute with HMRC in a judicial environment where the courts continue to apply a purposive interpretation to tax legislation.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

Methods of resourcing work have become subjected to increased scrutiny and are in a state of flux following the Supreme Court's landmark decision in the *Uber v Aslam* case in February 2021, which held that the drivers were "workers" for employment status purposes rather than self-employed. Workers are entitled to basic rights such as paid holiday, rest breaks and the national minimum wage, but do not have employment rights such as protection against unfair dismissal or entitlement to a statutory redundancy payment. The decision has implications for those operating via digital platforms with innovative ways of working that ultimately do not fit with the traditional employment status tests. The added difficulty is that employment status for tax purposes is not aligned with status for employment rights purposes.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

Changes in working practices with increased working from home may affect the collection, storage and movement of sensitive

data. This may include client data or confidential information being taken offsite by remote workers or third parties, which may have security and GDPR implications. Organisations need to be alive to issues related to the integrity of their IT systems particularly where employees use personal devices while working from home. Issues include ensuring securing information, policing the use and content of devices, consistency and confidentiality.

Employers also have duties under health and safety legislation to ensure that risk assessments are carried out in relation to employees working from home, which includes making sure they have the right equipment and a safe workspace.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

The impact upon workers of social distancing, self-isolation and more limited access to health services are likely to have a long-term effect on the mental health and wellbeing of workers, particularly younger workers, and there is likely to be a significant increase in hidden disabilities such as stress, depression and anxiety as a result.

The ability to have remote 'face-to-face' meetings, and manage work effectively will, for some, change the way employees want to work going forward. Employers are likely to be faced with more requests for flexible/agile working on a long-term basis. The increased familiarity with remote meetings is also likely to have a significant impact on the future of business travel particularly as long-haul trips raise environmental concerns and sustainability issues. Businesses may consider moving away from traditional face-to-face only meetings as part of annual appraisal processes towards the greater use of data analytics to inform staff performance.

There is also the potential for vaccine passports to be required in future for entry to the workplace.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Outdated regulation – Following the UK's exit from the EU, the UK's legal and regulatory framework remains broadly in line with other EU countries. As with other EU countries, the legal and regulatory framework governing digital businesses in the UK is outdated. In December 2020, the European Commission published the first draft of its proposed Digital Services Act Package which will serve as a much-needed modernisation of the e-Commerce Directive (2000/31/EC) (implemented in the UK by the Electronic Commerce Regulations 2002), which has increasingly struggled to keep up with the accelerating digitisation of society and the economy. It is unclear, however, the extent to which the UK will adopt legislation comparable to that contained in the Digital Services Act Package.

Data Protection – The regulatory requirements imposed by the Data Protection Act 2018 are complex and the fines for non-compliance can be extensive. It is unclear, following Brexit, the extent to which the UK will adopt the proposals contained in the Council of the European Unions' ePrivacy Regulations (currently in draft form), which could potentially impact the requirements to obtain end user GDPR (or equivalent) consent in order to place a cookie.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

The growth of digital business in the UK is a key area of focus for the UK Government. A new digital strategy was expected in the Autumn 2020 but was delayed due to the Covid-19 pandemic. It is anticipated that the strategy will set out the Government's plans to: (a) build a skilled workforce in the digital sector and help people move into the tech sector; (b) assist people in adjusting to a digital-led economy; and (c) provide help to businesses so they can become digital.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

Online Harms: The Online Safety Bill (which is still in draft form) applies to businesses whose services host user-generated content or facilitate interaction between users and will impose strict and wide measures to tackle terrorist material, child sex abuse, suicide promotion and cyberbullying online.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

This is a heavily regulated sector. However, the main regulations that apply to the online payment sector in the United Kingdom are:

1. the Payment Services Regulations 2017 (PSRs); and
2. the Electronic Money Regulations 2011 (EMRs).

Various parts of the Handbook of Rules and Guidance of the Financial Conduct Authority (FCA) (in particular, the Perimeter Guidance Manual) also include provisions that are relevant to the online payment sector.

Various "technical standards" also apply under the PSRs and the EMRs.

PSRs

The PSRs set out the list of payment services (Payment Services) which come within the scope of the PSRs.

The PSRs apply to persons that provide one or more Payment Services as a regular occupation or business activity in the UK. Depending on the relevant circumstances, a provider of Payment Services may need to be registered with the FCA as an authorised payment institution (API) or as a small payment institution (SPI). The PSRs set out the conditions that a firm must meet before it may be registered as an API/SPI (collectively PIs). The PSRs also set out various ongoing requirements with which PIs must comply (such as requirements in respect of capital and record keeping).

In terms of customer-facing matters, the PSRs require PIs to provide various pieces of information to customers at various stages of the customer journey. Importantly, the PSRs also set out rules governing the authorisation and execution of payment transactions. The PSRs also include rules governing the allocation of liability for defective or late execution of payment transactions.

EMRs

The EMRs provide a definition of "electronic money". The EMRs apply to persons issuing electronic money by way of business in the UK.

Depending on the relevant circumstances, an issuer of electronic money may need to be registered with the FCA as an authorised electronic money institution (AEMI) or as a small electronic money institution (SEMI). The EMRs set out the conditions that a firm must meet before it may be registered as an AEMI/SEMI (collectively EMIs). The EMRs also set out various ongoing requirements with which EMIs must comply (such as requirements in respect of capital and safeguarding).

Supervision and redress

The FCA is responsible for supervising PIs and EMIs and these firms may face FCA enforcement action if they fail to comply with their regulatory obligations.

Clients of PIs and EMIs may also have access to the Financial Ombudsman Service.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

General Regulatory Compliance

On 9 July 2020, the FCA sent a "Dear CEO Letter" to PIs and EMIs. In this letter, the FCA said that it had "identified six key areas where non-compliance with [FCA] obligations harms consumers". These areas are: (i) safeguarding; (ii) prudential risk management; (iii) financial crime; (iv) financial promotions and customer communications; (v) governance and oversight; and (vi) records management and reporting. The FCA provided a description of "action to take" in respect of each of these areas. As such, many firms have been reviewing their regulatory compliance in the areas identified by the Dear CEO Letter.

Strong Customer Authentication

As described above, the PSRs and related technical standards include rules regarding the authorisation of payment transactions. These rules were updated in September 2019 to reflect the "Strong Customer Authentication" provisions of PSD2 and they already apply to many firms. The Strong Customer Authentication rules do not currently apply in the context of e-commerce, but they are due to come into force for e-commerce on 14 September 2021. Firms operating in this space need to ensure that they will be ready to comply with the relevant obligations on and from the date on which they come into force.

GDPR

On 15 December 2020, the European Data Protection Board published its "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR". These guidelines explain the operation of the GDPR in the context of payment services. *Inter alia* they cover: (i) lawful grounds for processing data; (ii) consent; and (iii) data minimisation.

While the UK is no longer a member of the European Union (EU), much of the UK's data protection law derives from EU legislation and payment services firms will wish to take note of these guidelines.

Brexit

As the impact of Brexit on the financial services sector becomes clearer, many PIs and EMIs are considering the basis on which they may provide services to clients in the European Economic Area (EEA). While many such firms had "passports" into various EEA jurisdictions, there is now some debate in the industry about the extent to which these were in fact required in some cases. Firms with EEA clients will wish to keep any eye on developments in this area.



Jason Saiban is a commercial contracts specialist, with a focus on TMT, sport and retail & leisure. In TMT, he has particular expertise in outsourcing, managed services, logistics, procurement and licensing, and acts for a number of software developers and procurers of technology. His retail practice is focused on franchising, distribution, supply and logistics. Clients in the retail space include brands, restaurant chains and manufacturers, and he is particularly active in advising retail clients on the adoption of digital solutions, including online offerings and e-commerce. Jason's client base ranges from large multi-nationals to start-ups and entrepreneurs. In sport, Jason has significant experience in sponsorship, digital media, merchandising, endorsements and event management work. He is the relationship partner for a number of the firm's key sports clients, ranging from international sports brands to leading sports agencies.

Charles Russell Speechlys LLP
5 Fleet Place
London, EC4M 7RD
United Kingdom

Tel: +44 20 7203 5347
Email: jason.saiban@crsblaw.com
URL: www.charlesrussellspeechlys.com



Caroline Swain advises clients on a range of commercial contracts, typically with our retail, hospitality and brand clients. She has expertise in sponsorship arrangements, manufacture and distribution terms, marketing and advertising activities, and terms of sale. She has experience advising on consumer law, advertising regulation, data protection and e-commerce. Caroline acts for a range of large international corporations, innovative start-ups and family businesses, and has completed secondments at Westfield and a luxury fashion brand.

Charles Russell Speechlys LLP
5 Fleet Place
London, EC4M 7RD
United Kingdom

Tel: +44 20 7203 5158
Email: caroline.swain@crsblaw.com
URL: www.charlesrussellspeechlys.com

Charles Russell Speechlys has a broad range of skills and experience across the full spectrum of business and personal needs. We know it is not enough to understand the law – we have to understand our clients just as well. So we apply a people-focused lens to every action we recommend for you. Our unique approach to law has made us a leader in the world of dynamic growth and family businesses, and among the world's leading creators and owners of private wealth and their families.

Our firm is headquartered in London with offices across the UK, Europe, Asia and the Middle East. Our international connections mean we can work with you anywhere in the world. Whether your business operates in a single country or across borders, we will put together your perfect team – pulling from our sector and geographical expertise and our partnerships with the best law firms across the world covering 200 legal jurisdictions.

www.charlesrussellspeechlys.com

CRS | Charles Russell
Speechlys

USA

Cozen O'Connor



Victor J. Castellucci

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

In the United States, there are myriad local, state, and federal laws applicable to e-commerce businesses, and an exhaustive discussion is outside the scope of this article. As obligations, including licensing requirements, vary by state, establishing or operating an e-commerce business in America should involve legal counsel. Below are some key considerations.

Generally, e-commerce and non-e-commerce businesses are treated similarly. For example, like other businesses, an e-commerce business may be required to obtain a business operation licence or otherwise register with governmental authorities.

There are also specific issues that an e-commerce business must consider. For example, the business should ensure that its terms and conditions are contractually binding on its website visitors and customers, by including mechanisms by which the contracting entities can manifest their assent. Certain state laws governing sales taxes may also be applicable. Finally, laws governing data privacy and security may be applicable to a B2B e-commerce business.

Other legal requirements, including export control laws, may also be implicated.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The issues discussed above apply with equal force to B2C e-commerce businesses. In addition, numerous consumer protection laws apply to e-commerce transactions. Certain key considerations are discussed below.

Applicable to all persons who provide a written or implied warranty concerning a consumer product, the federal Magnusson-Moss Warranty Act (MMWA) requires such persons to disclose any such warranty in simple and readily understood language. The MMWA also prohibits suppliers from disclaiming or modifying any implied warranty to a consumer under certain circumstances.

In addition, state and federal data privacy laws may obligate e-commerce businesses to post clear and conspicuous privacy policies prior to collecting any personal information of consumers, to implement appropriate safeguards to protect such information, and to take steps to dispose of data securely. Furthermore, the American with Disabilities Act has been held by some courts to apply to websites, thereby obligating e-commerce businesses to take steps to ensure their websites are ADA-compliant.

Myriad advertising laws also apply to digital advertising. The CAN-SPAM Act requires that certain information be included in all unsolicited commercial e-mail, including a clear and conspicuous opt-out mechanism. The FTCA prohibits certain unfair or deceptive acts or practices in or affecting commerce. Other state and federal regulations govern the shipment of goods and the issuance of or notices concerning refunds.

Finally, issues surrounding user-generated content, use of third-party trademarks, and the use or reproduction of advertising materials frequently arise in the e-commerce context, and navigating those issues requires an understanding of intellectual property laws.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

American privacy laws have taken a sectorial approach to regulating individual industries. While largely still a patchwork, California recently enacted an overarching consumer privacy protection law, the CCPA, which applies to many e-commerce businesses. The CCPA became effective as of January 1, 2020. On March 27, 2020, the AG published a second set of modified CCPA regulations to address compliance.

After the CCPA, multiple states (including Colorado, Connecticut, Illinois, New York, Pennsylvania, Texas, *etc.*) either proposed or passed similar legislation.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

Fintech, AI, and digital health companies primarily conduct business online, thereby providing convenience by covering the entire country at once, but raising special compliance challenges given the intersection of various state and federal privacy laws; online retail experienced a boost in 2020, given the global pandemic lockdowns and the shuttering of many brick-and-mortar retail options, and so these compliance hurdles have

recently become more important for online retail organisations. Consumers in different states have different rights regarding personal data – in terms of notice, consent, access, and/or deletion. Thus, companies face the decision of whether to provide a uniform privacy policy (according to the strictest state law) or to provide different policies tailored to individual states (with potentially conflicting laws). In either case, there is complexity in ensuring compliance.

When a company is faced with a data breach, each individual state AG may bring an independent enforcement action. Reporting and/or responding to each state AG may be daunting. Adding to the complexity, the Federal Trade Commission (FTC) may bring enforcement action at the federal level. Moreover, state laws may provide a private right of action, which may increase a company's liability exposure.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

Most AG offices maintain resource webpages that publish various rules, policies, and opinions. The California AG's privacy resource webpage for businesses (including retail establishments) can be accessed here: <https://www.oag.ca.gov/privacy/ccpa>. Moreover, the CCPA specifically allows businesses to seek an advisory opinion from the California AG on how to comply.

The FTC also maintains a webpage laying out its policy framework and enforcement philosophies. Publicly available FTC enforcement actions also reflect the FTC's position on privacy issues and provide guidance to the public. The FTC has also hosted various workshops related to children's privacy, connected cars, education technology, drones, and smart televisions, and has, since 2016, hosted *PrivacyCon*, an annual event that brings together various stakeholders to discuss the latest trends and research.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

Federally, the Federal Trade Commission Act (FTCA) applies to e-commerce businesses, and has been applied to prohibit businesses from implementing insufficient cybersecurity measures that unfairly harm customers. Many states have similarly implemented overarching cybersecurity laws. Irrespective of local statutes, almost all American jurisdictions ascribe to a "reasonable security" standard (which is relative and proportional, rather than prescriptive and definitive) for cybersecurity issues. The National Institute of Standards and Technology (NIST) published in April 2018 a Framework for Improving Critical Infrastructure Cybersecurity, which is widely accepted as meeting the "reasonable security" standard.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Federally, for financial institutions including fintech companies, the Gramm-Leach-Bliley Act requires cybersecurity measures

appropriate for the size and complexity of the financial institution, and for the nature and scope of its activities. For the healthcare industry, the Health Insurance Portability and Accountability Act requires reasonable security measures. The Children's Online Privacy Protection Act requires businesses that collect personal information from or related to children to have security measures that protect such data. The Sarbanes-Oxley Act applies to public companies and contains provisions related to data security, integrity, and oversight. There are numerous other applicable laws.

At the state level, no fewer than 10 states have sought to harmonise cybersecurity requirements for insurers by following New York's lead and using the Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (Part 500) as a model.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Consumers in the United States have traditionally had favourable attitudes regarding e-commerce and related new technologies; America has a pool of consumers willing to embrace the online financial transaction paradigm. Recently, cash (that actually changes hands in a given transaction) is being viewed as an unsanitary mechanism that spreads contagion as readily as it effectuates financial transactions, and more Americans are viewing e-commerce or "touchless" point of sale technology as viable (and socially responsible) solutions to the traditional barter paradigm involving a physical exchange of tokens. This trend accelerated in 2020.

Some of the reported upticks in e-commerce transactions in 2020 and the early part of 2021 were a matter of necessity due to health concerns, but data (<https://www.digitalcommerce360.com/article/us-ecommerce-sales/>) and anecdotal evidence suggest that touchless payment options, electronic wallets, and e-commerce, in general, were on the rise in America even before the consumers were isolated from traditional brick-and-mortar establishments.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

The United States economy is one that thrives on consumer debt. It is fair to note that the overall amount (in terms of magnitude, as well as in terms of percentage of earned income) that Americans are willing to borrow is great. Generally, with certain exceptions, there is no stigma in America associated with being in debt. Those falling within the exceptions generally favour a debit card, direct debit, or cash on delivery paradigm, while the general American population has little to no compunction regarding assuming debt.

In the present economy, whether a consumer is prone to assuming debt or is more inclined to use a direct debit method of payment, virtual solutions such as e-commerce and related touchless or virtual transaction methodologies are gaining in popularity as discussed above.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

American retailer websites tend to perform best in the United States, which is typically where their target audience resides. E-commerce transactions are perfectly suited for American consumers, who require that the products they buy or the services they commission are readily available, easy to purchase, and delivered quickly. Many Americans also have come to trust personal data to the infrastructure that enables e-commerce platforms, even in a mobile context.

American consumers are also susceptible to context-sensitive and location-based advertising schemes, which American retailer and e-commerce platforms use very well to their advantage. These targeted advertising schemes work particularly well when consumers are engaged “on the road” or otherwise in a mobile context.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Many American e-commerce platforms rely upon the global prevalence of the English language and do not even acknowledge the sizable contingent within the United States that are not native English speakers. Some of the bigger e-commerce sites offer an option to select a language preference for display of content, but the list of languages from the URL in the United States is often very limited (*e.g.*, typically only English and Spanish).

Sophisticated platforms, however, host different, independent sites in different jurisdictions, and so the content may be tailored as the language is directed to the audience in the host country (*e.g.*, www.amazon.jp). These platforms, with a truly international or global footprint, target each audience separately, and tend to use analytics to optimise the user experience for the target jurisdiction, language, and culture.

4.5 Are there any particular web-interface design concepts that impact on consumers’ interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Americans typically do not like pop-up (dialog or other) boxes unless they specifically ask to view them, which is one reason why many browser applications offer an option to suppress such pop-ups. Typically, displaying too many pop-up boxes (or requiring a user to follow too many links) will quickly make an American consumer lose patience and move on to a different site.

There is an entire industry in the United States devoted to click-tracking, keystroke logging, and other data mining techniques to generate sufficient data to determine the point at which a prospective customer disengages from the e-commerce process. These analytics are used by platform operators to streamline their interfaces, to eliminate friction with would-be purchasers, and generally to improve the user experience based upon past user behaviour.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

If anything, the Covid-19 pandemic solidified these cultural norms, as Americans were forced to spend more time in isolation and to confront their environments intimately. In response, Americans relied upon e-commerce and remote retail purchases to address perceived deficiencies. As the data identified above show, Americans pumped 44% more dollars into e-commerce in 2020 than in the previous year. These dollars went to everything from home improvements and décor (to enhance the only environment that home-bound residents were allowed to enjoy) to office equipment, supplies, and consumables (since the “work at home” paradigm became closer to “living at work”). Anecdotally, many Americans, having recognised the efficiencies of working from home, have resolved not to return to the workplace, which will place a continuing strain on the e-commerce infrastructure.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

There is no single process for online brand enforcement in the United States. Businesses rely upon a suite of tools, laws and regulations.

Various third-party providers offer subscriptions to watch notice services, which can alert businesses to potentially infringing activity. Other service providers offer tools to assist business owners in enforcing their marks. Brand owners can also use procedures set forth in third-party terms of use to request the removal of infringing material.

Brand owners can also utilise the complaint mechanism under the Uniform Domain Name Dispute Resolution Policy to resolve disputes arising from abusive registration of domain names. A brand owner can also take pre-emptive steps to protect its brand by registering its trademarks with U.S. Customs and Border Protection.

Finally, businesses can rely upon state and federal laws, including the Lanham Act, as a basis to send infringing third parties cease-and-desist letters or to bring suit.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

The most common restriction that impacts brand enforcement efforts in the United States is the unavailability of WHOIS data or other contact information for bad actors. Since the passage of the GDPR, domain name registrars have been less forthcoming with providing contact information of registrants, making it difficult to contact or otherwise to locate a third-party malfeasor.

Jurisdictional challenges can also arise in enforcing brands. Trademark rights are largely territorial, making it difficult to enforce these rights against infringing activity occurring outside of the United States, and it can be difficult to find a jurisdictional hook over a foreign defendant. Even if jurisdiction is proper, a foreign defendant may refuse to appear, and enforcing judgment over same may be difficult.

Finally, it can be difficult to enforce brands against secondary or contributory infringers, such as online service providers, who may hide behind their purported lack of knowledge of infringing activity or may purport to lack the ability to control the infringing activity.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The relative sophistication of the customer seeking data storage services and the service provider determine the respective bargaining power of the parties. In many cases, smaller customers do not have much flexibility in negotiating such service contracts. Assuming some leverage during negotiation, the customer should consider: determining a desired service level to be received; understanding the data being retained and the applicable regulatory scheme; considering whether to shift the burden of compliance to the service provider; inquiring into the service provider's subcontracting activities; considering any relevant indemnification issues; reviewing the service provider's risk-based security programme; inquiring as to the ability to track and audit data transfers; and inquiring as to the interoperability of the service provider with other service providers.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Environmental laws and regulations should be considered; generally, a data centre is subject to no greater or more stringent environmental regulations than any other large building. Development in some areas, however, may involve national or California Environmental Quality Act review, air quality considerations, and issues that arise from regulations governing protection of wetlands and endangered species.

More than 20 states (many, coastal) have enacted electronic waste legislation. If setting up a data centre involves modification of specific zoning characterisations, relevant city ordinances and council hearing determinations should be observed.

If the data centre supplies its own power by use of solar panels, co-generation, or other means, or merely wants to install uninterruptible power sources, it is wise to consider applicable environmental issues, regulations of the Federal Energy Regulatory Commission, and possible tax incentives.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

The Automated Commercial Environment (ACE) is the system through which the trade community reports imports and exports and the United States government determines admissibility. ACE is the system of record by which electronic trade transactions are conducted and recorded by the United States' Customs and Border Protection (CBP) agency. ACE provides a unified, centralised access point for the trade community to connect with CBP and its Partner Government Agencies (PGA). Import manifests, entries for consumption, warehousing and bonding, post-entry submissions, such as protests and duty drawbacks, are all examples of transactions and data that must be filed electronically through ACE. The comprehensive use of ACE has resulted in reduced wait times at cargo points of entry and the faster processing of entries, bonds, and refunds.

In the United States Mexico Canada Agreement (USMCA), an entire chapter is dedicated to digital trade. As currently drafted,

the USMCA seeks to ensure that data can be transferred cross-border, that limits on where data can be stored and processed are minimised, and that suppliers are not restricted in their use of electronic authentication or electronic signatures.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Digital technologies, in theory, should lower the cost of trade, thereby providing smaller businesses across the globe access to trading opportunities. However, digital technologies require capital investments, and must interoperate with other countries' platforms in a secure manner. These efforts take time and monetary investment. Issues concerning inclusiveness, privacy protection, and cybersecurity are likely to remain high priority discussion points within the future governance of digital trade. Governments will need to work together to develop a favourable legal framework, address competition issues, standardise intellectual property rules, and address challenges related to incompatible infrastructure for seamless information technology.

Special acknowledgment to Kristi Zentner, Thomas Wallrich, and Heather Marx for their contributions to Section 7.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Prior to 2018 and the U.S. Supreme Court's decision in *South Dakota v. Wayfair*, e-commerce businesses in the United States generally were required to collect state sales tax from customers only in states in which the e-commerce business had a physical presence. Since *Wayfair*, many states have adopted "economic nexus" laws, that is, laws based on the seller's level of economic activity within a state.

Generally, such laws have a small sales exception that exempt businesses from sales tax registration in that state if they do not satisfy a particular economic threshold. What qualifies for the exception varies greatly by state.

Federally, the United States offers a research and development credit to businesses in an amount equal to certain sums specified by statute, which could apply to at least some digital businesses.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

"Economic nexus" laws are susceptible to challenges. Moreover, taxing authorities and jurisdictions are increasingly taking the position that they can appropriately tax digital companies, even where those entities have little or no physical nexus to the jurisdiction. This can result in multiple jurisdictions assessing taxes on the same revenues or income of digital companies based on various, non-uniform rules.

Other disputed issues include whether the goods and/or services sold by the digital business are subject to sales tax in a particular state and determination of the proper sourcing of those sales to a state (or possibly more than one state). Another

issue involves determining whether certain research or development constitutes qualified research within the context of the research and development tax credit discussed above.

Special acknowledgment to Cheryl Upham and Dennis Cohen for their contributions to Section 8.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

There are two primary considerations concerning resourcing work in the United States. The first involves finding an available, qualified talent pool, and then incurring training costs for (and protecting trade secrets with) a sourced worker who may terminate engagement after receiving training. Second, the laws involving “independent contractor classification” and “joint employer liability” may impose liabilities and obligations on the business for claims by or against the sourced worker. Various aspects of these considerations are addressed on state and local levels, which means that a business may need to consult applicable law in multiple jurisdictions.

It is not unusual to attempt to address these and other issues in the United States via consulting agreements, employment agreements, or other on-boarding documents that the sourced talent is required to sign. In the event of damage to the company's business or reputation, in addition to available statutory remedies, the company may recover (for a contractual breach) from the sourced worker.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

Federal intellectual property laws may apply to this situation. Otherwise, businesses will often implement contractual provisions or policies regarding the use of resources or conduct of the business' work (electronic and otherwise) off-premises, as well as employee access to the business' systems and work product while the employee works remotely. The business may recover directly from a renegade or negligent employee under the theory of contractual breach (in addition to any statutory or regulatory remedies available), though such contractual provisions typically only have a real benefit to the company to the extent that they act as a deterrent of bad behaviour or to the extent that the employee has sufficient funds adequately to make the company whole again following a breach.

Special acknowledgment to Michael Schmidt for his contributions to Section 9.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

As noted above, the Covid-19 pandemic has re-focused many Americans, and even some employers, to accommodate a “work from home” paradigm. Accordingly, the implications of the immediately preceding discussion on carrying out work away from an employer's physical premises are greater now than they were a year ago.

Contractual obligations to deter undesirable behaviour on the part of an employee and data security measures to thwart unauthorised access to company data or otherwise to protect company proprietary information are now more important than ever.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The key legal barrier facing digital businesses in the United States is the sheer number of legal barriers; there is a truly massive body of law governing virtually all aspects of American digital business operations. Federal, state, and local laws are disparate, and constantly in flux and/or in conflict; in many cases, determining which law applies is not straightforward. Myriad areas of law are potentially implicated, so digital businesses must navigate tax, privacy, data security, labour and employment, corporate, intellectual property, and advertising issues, many of which present different requirements or compliance standards in different states and localities. The primary legal challenge is to understand the scope and contemplation of the changing legal landscape.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

One advantage for digital businesses in the United States is the accommodating consumer base. American consumers embrace the convenience of e-commerce solutions, have faith in the infrastructure (or are at least willing to ignore any misgivings regarding privacy breaches in favour of the convenience), and drive innovation by readily adopting new technologies and methodologies. Further, with the prevalence of “likes” and “recommendations” facilitated by social networking platforms, digital businesses can benefit from endorsements provided by influencers in the digital sphere. For at least these reasons, many businesses in America can thrive on the basis of a robust digital footprint and take advantage of current trends in ways that other businesses cannot.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The key take-away from the global reaction to the pandemic of 2020 is that digital businesses and electronic commerce in America are on an undeniable upswing. Whether out of convenience or by necessity, Americans are taxing the electronic infrastructure at an accelerating rate, and it will be incumbent upon e-business enterprises and regulators alike to adjust the technological and legal platforms to accommodate the increased traffic. Privacy and data security are likely to be increasingly important to American businesses and consumers, and it will be critical to the regulatory authorities to address those concerns and the practical realities of a virtual marketplace in a manner that accommodates business flexibility whilst affording consumers the anonymity that they expect.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The Payment Card Industry Security Standards Council (PCI SSC) has developed security standards that apply to organisations that accept payment cards and handle card data. The principal security standard is the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a set of technical and operating requirements designed to protect cardholder data and to foster consistent data security measures across the payment card system. The PCI DSS applies to all participants in the payment card system that store or transmit cardholder data or sensitive authentication data, including merchants, banks (both the merchant banks and card issuing banks), and third-party service processors.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

A consumer is usually only liable for up to \$50 in unauthorised credit card charges made before the consumer gives notice of the possible loss, theft, or unauthorised use of the card (15 U.S.C. § 1643(a)). Many card associations and financial institutions have reduced the \$50 limit so that a consumer generally has no liability. A consumer potentially has more liability for the unauthorised use of a debit card.

The Bank Secrecy Act and related Treasury Department regulations define whether a business is construed to be a financial institution or money services business for purposes of these applicable regulations.

Federal and state laws that apply to electronic contracting include the federal Electronic Signatures in Global and National Commerce Act and applicable state versions of the Uniform Electronic Transactions Act.



Victor J. Castellucci is a member of Cozen O'Connor's Intellectual Property group and is a registered patent attorney who has led the patent process for many of America's largest and most successful corporations. He has broad experience in all aspects of patent prosecution in the electrical and mechanical arts, emphasising computer hardware and software, robotic systems, telecommunications, networking and data encoding protocols, bioinformatics, and medical diagnostics systems.

Cozen O'Connor
301 South College Street
Suite 2100
Charlotte, NC 28202
USA

Tel: +1 704 348 3465
Email: vcastellucci@cozen.com
URL: www.cozen.com

Established in 1970, **Cozen O'Connor** has more than 775 attorneys who help clients manage risk and make better business decisions. The firm counsels clients on their most sophisticated legal matters in all areas of the law, including litigation, corporate, and regulatory law. Representing a broad array of leading global corporations and middle market companies, Cozen O'Connor services its clients' needs through 30 offices across two continents.

www.cozen.com



ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business

Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law

Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms