International
Comparative
Legal Guides

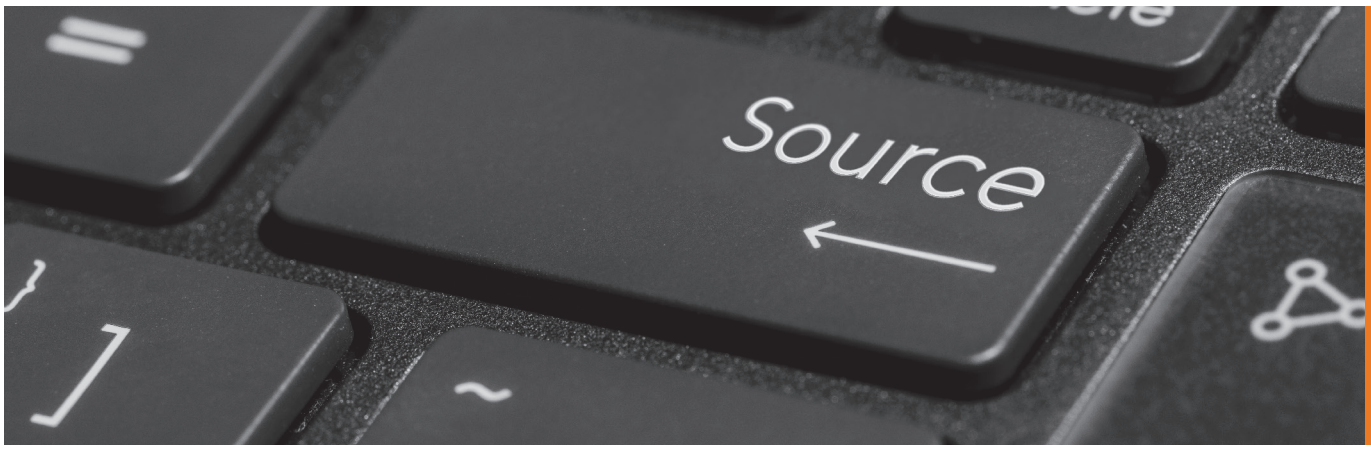
Technology Sourcing

2024

Fourth Edition

Contributing Editor:
Mark Leach
Bird & Bird LLP

glg Global Legal Group



ISBN 978-1-83918-359-1
ISSN 2752-6909

Published by
Global Legal Group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
customer.service@glgroup.co.uk
www.iclg.com

Publisher
Ben Lawless

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
Fraser Allan

Strategic Partners

International Comparative Legal Guides

Technology Sourcing 2024

Fourth Edition

Contributing Editor:
Mark Leach
Bird & Bird LLP

Expert Analysis Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the fourth edition of *ICLG – Technology Sourcing*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to technology sourcing laws and regulations around the world, and is also available at www.iclg.com.

This year the expert analysis chapters focus on sourcing AI solutions, and driving sustainable strategic sourcing.

The question and answer chapters, which in this edition cover 17 jurisdictions, provide detailed answers to common questions raised by professionals dealing with technology sourcing laws and regulations.

As always, this publication has been written by leading technology sourcing lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Mark Leach of Bird & Bird LLP for his leadership, support and expertise in bringing this project to fruition.

Ben Lawless
Publisher
Global Legal Group

International Comparative Legal Guides

Sourcing AI Solutions


Mark Leach


Will Bryson

Bird & Bird LLP

Introduction

As the modern economy continues to be transformed by rapid advances in digital technology, technology sourcing lawyers continue to face many new challenges. Traditional ways of procuring technology are changing and new technologies are being deployed at speed and scale across many industry sectors. This has created a need to review tried and tested technology contracting models and to ensure that the risks created by new and emerging technologies are properly addressed.

One area where this is has been sharply thrown into focus in relation to the adoption of Artificial Intelligence systems. The last year or two has seen AI explode onto the public consciousness (particularly with advances in generative AI systems), at the same time that approaches to AI regulation have been confirmed and adopted (in the EU at least). All of this leaves more and more business grappling with the issues that arise when sourcing AI systems.

This chapter discusses the nature of some of the legal issues and risks that a customer seeking to implement such a system will face. It will then discuss where and how the contract for the sourcing of an AI system should seek to address and mitigate these issues and risks.

What are we Talking About?

To start with, it is worth defining what exactly we are talking about when we refer to AI-based systems. As with many new technologies, advances in Artificial Intelligence or "AI" have been accompanied by more than their fair share of hype and a somewhat bewildering array of jargon. This has often served to obscure the nature of the systems that are being deployed by organisations on the ground.

When we refer to "Artificial Intelligence" or an "AI system" in this chapter, we are (to paraphrase the definition in the EU AI Act) referring to a computer system which is designed to operate with a certain level of autonomy which, based on the input date it receives, infers how best to achieve a human-defined objective. For example, this could be a system that could classify images or text, a system that makes recommendations based on data it is presented with, or a system that creates images, text or code based on natural language input.

What AI systems that we see today have in common is the techniques used in their development – particularly machine learning. Machine learning is a subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed. Instead, an AI system is fed vast quantities of training data and uses a set of algorithms designed to identify the underlying relationships in that data (through a process that mimics the way the human brain operates) in order to complete the task it was presented with. This enables a system, for example, to "learn" to recognise particular features in data that is fed to it (e.g. recognising particular images) or to identify patterns and insights in large data sets which would be hidden to a human being. This kind of technology is a core component of many digital transformation programmes and is behind developments as diverse as digital assistants, smart thermostats, chatbots, content generation systems and virtual assistants on online shopping platforms, predictive maintenance of industrial equipment and self-driving cars.

AI Regulation

Before addressing the contractual issues, some consideration needs to be given to the regulatory landscape that applies, or will shortly apply, to the development and use of AI systems. At the time of writing, in the UK (and in many other jurisdictions) there is currently no general statutory or regulatory framework that governs the development and use of AI technology. In March 2023, the UK Government published its white paper on AI regulation (entitled "A pro-innovation approach to AI regulation") which does not propose specific regulation of AI at this stage. Instead, it outlines a framework of five guiding principles which are intended to drive consistency across regulators while also providing them with the flexibility needed to regulate such a fast-developing technology. The white paper proposed that existing sector-based regulators have responsibility for managing AI systems within their remit and applying the principles. Following a consultation, the UK Government published its response in February 2024. This largely maintained the original position, but it added more emphasis on safety (in addition to the original pro-innovation approach). Also, for the first time, the UK Government acknowledged that it would consider introducing binding measures on the developers of the most capable general purpose AI systems if certain circumstances arise. Following a request from the Government, many of the UK's key regulators have recently published their AI strategies to show how they are responding to AI risks and opportunities.

In the EU, by contrast, a different approach is being adopted. The EU's "Artificial Intelligence Act" is expected to come into force in August 2024, with the bulk of the provisions being applicable from August 2026.

The AI Act divides AI systems into four categories based on the risks they present to users' health, safety and fundamental rights. It imposes different obligations depending on the category:

- **Unacceptable risks**: AI systems falling within this category are prohibited, as they are deemed to be against EU fundamental rights and values. Banned AI systems include those used for social scoring and predictive policing.

- High risks:
  A system is high risk if:
  (i) it is listed in Annex III (as long as the four exceptions don't apply). Systems in Annex III include AI systems used in recruitment, critical infrastructure and border control; and
  (ii) it is a product or part of a product listed in Annex I and that product is required under the relevant product law to undergo a third party conformity assessment. The product laws in Annex I cover products such as medical devices, machinery and toys.
  High-risk AI systems will be allowed only if the AI systems themselves comply with certain mandatory requirements. These include risk management, data governance, technical documentation, record-keeping, human oversight and accuracy and robustness. Providers of high-risk systems have a multitude of obligations to comply with, which include fixing a CE marking onto the system, keeping documentation and ensuring that the AI system undergoes a conformity assessment. Deployers of high-risk systems have separate obligations to comply with including assigning a human to carry out human oversight of the AI system. Other actors such as importers and distributors have other separate obligations on them under the AI Act.
- **Transparency risks**: Where an AI system falls into one of four scenarios set out in Article 50, it would be in the transparency risk category and certain obligations apply. For example, where a person is interacting with a chatbot, the provider of the chatbot must ensure that the person is informed they are interacting with an AI system, unless it's obvious from the circumstances. Also, where deep fake content has been produced by a chatbot, deployers need to disclose that it has been artificially generated. An AI system could fall into the transparency category as well as the high-risk category.
- **Minimal risks:** This last group comprises all other AI systems. These are considered not to constitute a risk or pose a threat to citizens' fundamental rights and to which no specific obligation will be applied.

Providers of all general purpose AI (GPAI) models must comply with a set of minimum requirements such as technical documentation and transparency measures. For the absolute largest foundation models such as GPT-4 (known as "GPAI models with systemic risk") there are increased requirements to meet.

As will be evident from the above, future contracting models will need to reflect these legislative requirements, particularly where the AI system in question is going to be used within the EU. We expect to see additional indemnities introduced into contracts. While it is currently too early to assess the precise impacts, this is an area that businesses will need to keep a close eye on.

Contracting for AI Systems

So, aside from the emerging regulatory considerations, what issues need to be considered when contracting for AI systems of the kind discussed above? It is important to state at the outset that, while artificial intelligence is often associated in the popular imagination with robots and artificial humans, for now at least AI systems are still software. They may be sophisticated software systems comprising complex algorithms and deploying cutting edge computing techniques, but they remain software systems, nevertheless. This is important to bear in mind as it means that many of the same issues and considerations that arise in the context of any software development or licensing arrangement or (where applicable) in any software as a service contract will be equally relevant to a contract for the provision of an AI system. Indeed, in our experience, many standard form contracts being proposed by suppliers in respect of for their AI systems look remarkably similar to the terms for traditional software systems or SaaS solutions. However, due to the intricacies of the way in which AI systems are developed and operate, we would suggest that there are a number of issues that need to be approached differently and certain areas where a more nuanced approach is required. The remainder of this chapter will look at a number of these issues and areas, namely:

- how an AI system will be licensed;
- the manner in which an AI system is implemented;
- acceptance testing;
- Intellectual Property issues;
- data considerations; and
- issues regarding liability.

Licensing Model

When sourcing an AI system, the way in which it is to be provided will be an important consideration for a customer. The primary decision will be whether the system will be provided on an "on premise" or a "software as a service" basis (or some combination of the two).

A major driver in this decision will be the way in which the system will be used and the computational needs of the system. For some AI applications a SaaS/cloud model would make sense (e.g. an automated document review solution). In fact, for certain systems (current large language models, for instance) the computational power needed to run the model means anything other than a cloud-based system could be unworkable. For other applications, software will need to run locally (e.g. driverless cars, where to rely on intermittent connectivity would impede the safe functioning of the car) or take a hybrid approach (e.g. digital assistants). Ultimately this is not a decision driven because the system in question is AI-based, but more that AI is enabling solutions which may not have been possible through traditional software.

The other licensing model question to be considered is how usage of the system will be charged for. For an AI system, the "traditional" commercial models of "per user" or "per instance" licences could be inappropriate (as each customer may only need one instance, and where a system is effectively replacing a human user, there may only be a limited number of admin users required). Instead, it may be more appropriate for charges to be based on the number of tasks performed (for example, per image created), or by volume of data processed (this is the approach taken with a number of LLMs, where charging is on a "per token" basis, dependent on the number of tokens in the input data).

The contract will also need to address a number of issues that would also be relevant in the context of a traditional software system such as:

- the number of individual users who need to use the system;
- whether other group companies and third party out-sourcing providers will also need to be licensed;
- whether the rights to use the system are granted on an exclusive or non-exclusive basis;
- any geographical restrictions as to where the system can be used or accessed from; and
- the purposes for which the customer may use the system.

This last point may be particularly relevant for AI systems. The AI system may have been designed and trained to perform specific tasks. Suppliers of these systems may, therefore, want to limit customers' rights to use these systems in line with the intended use, and not grant a right to use the system for "any

business purposes" as it might otherwise have done. Such restrictions would be particularly relevant where applicable regulation imposes restrictions or further obligations on certain use cases, e.g., the EU AI Act upon "high-risk" use and GDPR on automated decision making.

Implementation Issues

For an AI system, many of the issues to be addressed in the contract in relation to implementation of the system are fundamentally the same as for other IT projects. For example, the parties will want to consider appropriate milestones and project planning issues, and any dependencies on the customer.

However, with an AI system there may need to be additional steps involved. The system may need to be trained (or "tuned") on data relevant to the customer's use case in order to suit the customer's needs. Where this is the case, the parties may need to identify appropriate training data, potentially review and clean that data to remove bias and anomalies, and then train the system on that data, before the system can be tested to ensure it meets the agreed acceptance criteria. These steps need to be catered for contractually and reflected in the project plan and milestones.

The parties will also need to consider certain legal issues around the training data as discussed more fully below.

Acceptance Testing

Testing an AI system is important to avoid bugs and errors when it goes live, as with any IT system. But for an AI system, the approach also needs to grapple with the issue of testing a system which has probabilistic (rather than deterministic) outputs; where the system may give different answers to the same question (and is not "wrong" in doing so).

If the AI system has been adapted for a specific customer or purpose (possibly using customer data), testing should check if that has caused bias or affected output quality.

The parties should also keep track of the testing of the AI system in case there are problems later. Keeping records may be more important for AI systems than for normal IT deals, so the contract needs to cater for this accordingly – with customers potentially requiring suppliers to keep and maintain records in a repository the customer can independently access.

Customer Obligations

The supplier may seek to place obligations on the customer's use of the AI system, to limit or disclaim the supplier's liability for inappropriate use.

This may include:

- prohibiting uses of the AI system which the supplier considers inappropriate, whether due to the risk posed, potential reputational impact of being associated with such use, or requirements of applicable regulation;
- requiring the customer to use the AI system in compliance with applicable law. This obligation will become increasingly relevant as AI specific regulation is put in place; or
- requirements for human oversight, input, and review where appropriate.

Attributing Liability for AI System Failures

Traditional software contracts typically include warranties from the supplier about the quality of the software or service. For example, suppliers often warrant that the software will meet the requirements of the specification and that it will be free from material defects. In the event something goes wrong with the system, the customer would typically point to the relevant warranty as the basis for requiring the issue to be rectified or bringing a claim for damages.

This approach relies on it being relatively clear and easy to establish that there has been a failure in the system in the first place, and also a general acceptance that that an issue with performance is something which the supplier should be responsible for. However, when it comes to AI systems, there is a significant risk that it will prove more difficult in practice to establish such a failure and be able in turn to claim such contractual remedies. The reason for this is the so-called "black box" problem.

There is also, perhaps, a shift in perception as to what is to be expected of an AI system. This is very much application specific, but there will be situations where getting it wrong is less of an issue (such as an imperfection in a generated image) but others where an error has much more profound consequences (driverless cars, for example).

In order to understand this problem, it is worth taking a step back and looking at how AI systems actually make decisions in practice. In broad terms, when a human mind thinks, it takes in data, processes it based on experiences and knowledge gained over a lifetime, and based on that decides whether (and what) action needs to be taken. So, for example, if data I am receiving tells me that I am thirsty, from experience I know that water quenches my thirst so I decide to drink a glass of water.

In a "traditional" piece of software, human minds have used their experience to design algorithms to tell a computer what to do based on the input data it receives. It implements algorithms which look at input data and human designed logic resulting in a particular behaviour. So a human developer may have programmed the system so that "IF hydration < 0.5 THEN consume_water".

Generally, an AI system is different as it is no longer relying fully on human designed and written logic. As mentioned earlier, many AI Systems are created using machine learning techniques: training the system to develop its own logic by promoting logic which makes successful decisions. It does not consider "why" a particular output is the best answer when confronted with the input data given, but rather outputs what answer is most statistically probable. The same is true of generative AI systems – they do not "understand" the input prompt and then reason an answer to it (in the way a human would) but instead generate an output which is statistically probable based on the input. The issue that this creates it that the logic relied on by an AI system becomes a "black box" to a human observer.

This has a number of implications in practice. Firstly, it may be difficult to establish that a bad outcome is a defect or error in the system at all. AI systems may produce outputs or decisions which are just not "human", but not necessarily wrong. Sometimes an error will be manifest – an image generator, when asked to produce a drawing of a horse in the style of Stubbs, may create a very convincing image, but one where the horse has five legs. But other outputs might be perfectly correct, just not what a human would have done or what the user envisaged in their mind's eye.

This leads onto a second problem with attributing liability for losses caused by AI: proving who is at fault. It may not be possible to unpick the background to the making of a bad decision to see what previous experience caused the decision to be made. Also, it may not be because of previous experience at all – where an image generator creates a five-legged horse, it's not because the system has been trained on images of horses with extra limbs. Without this ability to interrogate the decision, it would not be possible to say if it was an error in the original code written by the software house, the particular model adopted or resulting

from the diet of data it was fed (and in the latter case, whether it arose from the training data or the real "live" decisions made once in use by the customer), or something else entirely. In the near term at least for generative AI systems, there is likely to be continued reticence from the developers to accept any form of liability for errors (or "hallucinations" as they are often known). It is already widely acknowledged that when a generative AI creates an output, that output is unlikely to be entirely correct (be that by stating incorrect facts, adding an extra leg to a stallion, or something else). Where a supplier of such a system knows of the propensity of that system to be inaccurate, that supplier is not going to stand behind the system's accuracy. Therefore, performance warranties that rely on ascertainable defects in the underlying code are likely to be less effective. It may also become the case that they are less relevant. If a customer accepts the outcomes of the system are not perfect (though whether this is appropriate of course depends on the application itself), then the customer's concern shifts towards other attributes which are to be expected of any software system – that the system is suitably available and that it responds promptly.

This is not to say that traditional warranties should not be included in an AI system contract, but customers should recognise that they may provide a less effective remedy than has been the case in traditional software contracting. It also means that customers would be well advised to think a bit more broadly about remedies and practical mitigations against the risk of failure. It may be appropriate, for instance, to push for commitments from the supplier regarding the quality and accuracy of the outputs generated by the system and, where the supplier is taking the lead in "training" the system, seek appropriate warranties that this work is undertaken to a standard that is in accordance with good industry practice. From a practical point of view, greater emphasis may need to be placed on testing the system before it goes live to ensure it is performing as expected, together possibly with a greater use of trial periods during which the system can be tested in a limited live environment prior to being fully deployed. Once accepted, the use of the system in a fully live environment should be closely monitored so that incorrect or potentially incorrect results can be identified and investigated at an early stage. The incorporation of technical circuit breakers within AI systems themselves that suspend the system or enable manual overrides where certain output parameters are exceeded can also be helpful in this regard.

As the technology continues to evolve, particularly if there is a regulatory focus on "explainability" or "trustfulness", technical solutions to the "black box problem" may well be developed. There is certainly already a significant focus on developing explainable AI (or "XAI") systems. It of course remains to be seen whether the fact an AI system can explain why it made a particular decision would result in the persons involved in the inputs into that decision accepting responsibility for them but, depending on the use of the relevant AI system, having an explainable decision may well provide a further useful check and balance against potential unforeseen consequences.

Intellectual Property Rights

The AI system

As with any software contact, ownership of the intellectual property rights in an AI system will need to be clearly addressed. At one level, the issues are no different from those that apply in relation to a more traditional software system. Where the customer is commissioning a bespoke system it will often look to own the IPR in the newly developed software but where the AI system is a proprietary "off the shelf" product or a software as service solution made available on a "one to many" basis, the supplier will wish to ensure it continues to own all the relevant IPR.

Where the situation can become more complex with regard to an AI system is where customisations are made to an underlying proprietary platform that are specific to a customer. Where this is the case, a customer may feel it should own those bespoke customisations but, in practice, ownership of these customisations alone may be of little value without continuing access to the underlying system. The position is further complicated where those customisations take the form of algorithms that have been developed by means of machine learning and without active human involvement. Where this is the case, it may be questionable as a matter of copyright law whether those algorithms will actually qualify as a copyright work (see the answers to question 10.3 in the Q&A Chapters in this Guide).

Ownership of outputs

Another question in relation to IPR ownership relates to the results or outputs generated by an AI system. Putting aside the issue of whether there are, in fact, any IP rights in the outputs for one moment, these results will often be specific to a customer and where intellectual property rights subsist in such results a customer should consider including provisions in the contract to ensure that it owns these. This will be particularly important if the customer wishes to keep open the possibility of taking the specific results and using them with another supplier in the future. A supplier, on the other hand, may well seek to use its ownership of these rights as a way to lock the customer in to using its AI system. At present, it is probably fair to say (in the UK at least) that the size of the market for AI service providers means that the ability for a customer to switch suppliers in this manner is relatively constrained, but this may change over time if the adoption of AI technology continues to grow and the number of providers increases.

There is, however, the fundamental issue of whether IP rights will subsist in outputs from AI systems. Generally, intellectual property regimes are founded on the principle that the work being protected has a human author; in fact, it is the intellectual endeavour of a human that is being rewarded by the grant of intellectual property rights in the fruits of that endeavour. This is a point which legal systems will need to address. The question of authorship cannot be amended by contract as it is a matter of status and fact, but the parties can contractually agree who will be the owner of any copyright that resides in the outputs.

For generative AI systems which create text, images, music and code, the most relevant intellectual property right would be copyright. However, as things stand (in the UK and the US at least) there are significant unresolved questions under English law about whether computer generated works can be protected by copyright at all. To benefit from copyright protection, the output needs to be original which, following a line of pre-Brexit CJEU case law, requires a work which is the expression of an author's own personality and in which they have made free and creative choices. Therefore, anything that contributes to the originality of the output must come from a human as opposed to the AI itself. The uncertainty regarding the copyright protection of computer-generated works under current English law was recognised in a 2022 Government consultation, which decided not to amend the current position for fear that it would have unintended consequences.

While entering a simple text prompt to a generative AI system may not attract copyright protection under current English law, there are many grey areas where copyright may still arise notwithstanding the use of a generate AI system in the process of creating a work. These include a human using a generate AI system as a tool to achieve a specifically desired result or mosaics/further manipulates the outputs from a generative AI system to create a new original work. Under current US Copyright Office Guidelines, the latter would be registerable as a copyright work (subject to disclaiming protection for the purely AI generated elements) but the former would not.

In that scenario, parties would need to overcome the fact there is nothing to "own" in the outputs and include contractual mechanisms to seek to achieve the same result – much in the same way as they would need to do for data.

Data

Rights around data need to be considered especially carefully when contracting for AI systems. It is helpful in this regard to distinguish between training data that is used to "train" the AI system, input data which is fed into a trained system, and output data, being the actionable insights, reports or recommendations or other content that is generated by the operation of the system.

Training data

With regard to training data, the first question to ask is who is responsible for training the system? From a customer's perspective, if it is providing training data then, as part of its pre-contract due diligence, it will need to consider where the data are to be sourced from, and whether it has the right to use the data from that source for these purposes. That question is easier to answer if it is data which the customer has gathered itself (though then it would still need to ensure that the data is sufficiently clean to be properly used), but will need further consideration when the data are being sourced from a third party. In that case, the customer should be sure to obtain a clear contractual permission for the third party to use the data for the purposes of training the relevant AI system and, where necessary for these purposes, to disclose the data to the AI system supplier. If the training data provided by the customer incudes data obtained through web scraping, the supplier will want to ensure that any risks it has in relation to this are backed off under the contract. Customer data obtained by web-scraping can be subject to third party IP rights. Handling such data on behalf of a customer without permission of the third-party rights holder can expose the supplier to a potential IP infringement claim, either directly for their own dealings with the data or via secondary liability theories e.g., joint tortfeasance. Web scraping undertaken by a customer may also involve a breach of website terms and conditions. A supplier will not have primary liability for such breaches. However, recent years have seen a growth in secondary liability claims relating to web scraping before the UK courts, with the torts of procuring breach of contract and unlawful means conspiracy being relied on to pursue parties who benefit from web scraping undertaken by others.

Where the AI system has been trained by a supplier, a customer seeking to use that system would still need to be aware of potential infringement risks. There are currently a number of claims being brought against developers of generative AI models that allege that when the output of a generative AI system reproduces content that was contained in the input training data, it is infringing IP rights in that input data. While to date these claims have focussed on the developers of these systems, there is no logical reason why they could not be brought against a customer. Traditionally, customers of technology products mitigate against the risk of third party IP claims by seeking an indemnity from the supplier. However, with this being such a live issue at the moment, suppliers may simply be unwilling to offer customers this protection.

Input and output data

As has been mentioned above, it is critically important to ensure that the contract deals clearly with the input data and outputs and results generated by an AI system. Where these inputs and outputs take the form of data, it may be possible (as discussed above) for a customer to assert an ownership right over the inputs, outputs and results in question where the relevant data are protected by identifiable intellectual property rights. That may be the case, for example, where copyright subsists in the data, where the EU database right applies (to an aggregation of the data) or if the data can be considered to be confidential information. However, it is important to recognise that in many cases this will be difficult to establish. In these circumstances, the position of a customer who wishes to exert control over the data is further hampered by the fact that, in many jurisdictions, there is a reluctance to treat data or information as a form of property to which a legal right of ownership can apply. Where this is the case (as it is under English law for example), a well drafted agreement should place less emphasis on the concept of the ownership of data, but rather focus on the rights and restrictions that should apply to the access, use and disclosure of that data. The English courts at least have expressly confirmed that such an approach is possible and creates enforceable rights as between the parties, even where no intellectual property rights apply to the data in question. It should be noted, of course, that contractual restrictions of this kind in the absence of any ownership rights will not provide a customer with any protection against a third party who seeks to assert an ownership right or otherwise prevent the use of the relevant data. As a result, it is still prudent for the recipient of any data to take an indemnity from the provider to cover it against this risk.

Where data being processed by an AI system contains personal data, careful consideration of various data protection and privacy issues is required. The technical complexities of AI systems and the unique risks involved can make data protection issues particularly challenging to deal with. The use of AI to process personal data often triggers the need for a data protection impact assessment and information from the supplier may be needed to complete this. A detailed discussion of these issues is beyond the scope of this chapter and we recommend that specialist advice is taken whenever personal data interacts with an AI system.

Supplier's use of customer data outside the scope of the contract

Suppliers may push for the right to use the customer data for purposes other than training or fine-tuning the AI system for the customer, e.g., general improvement and fine-tuning of their AI product.

Customers are often wary of agreeing to this, particularly due to concerns that their data may be inadvertently disclosed to other customers as outputs of the AI system. Suppliers will need to evaluate whether the ability to re-use customer data is genuinely useful to them (over and above the training data they have already procured) and, if it is, what they may be able to offer to customers as technical assurances that the data they provide will not be disseminated by the model.

Limitation of Liability

The practical difficulties concerning the attribution of fault are often compounded by the approach taken to the limitation of liability in many supplier contracts. As mentioned above, many AI systems are licensed on an "off the shelf" basis on supplier standard terms and the provisions limiting and excluding liability therefore often reflect the approach taken in respect of traditional software systems. This tends to mean that liability caps are set by reference to annual licence or subscription fees and the supplier excludes all liability for financial and business losses. In the context of AI systems this is often coupled with an express exclusion of the supplier's liability for any losses resulting from the decisions taken by the customer based on the outputs generated by the system. While this approach is understandable from a supplier's perspective, particularly where the AI system or core platform is being provided to multiple customers, it can leave the customer with very little recourse against the supplier in the case of a major system failure.

As the importance and criticality of AI systems grows and IT systems generally become ever more core to a customer's business operations, there may be an argument to reconsider this basic model.

However, that is a broader question and, for now at least, there is little discernible sign of a change in market practice – particularly given the propensity for generative AI systems to "hallucinate", as discussed above. As a result, a customer will often face an uphill struggle to negotiate higher limitations on liability or to persuade a supplier to accept a greater scope of liability. The onus therefore remains on the customer to ensure that it undertakes a fully informed assessment of the risks of deploying an AI system. For generative AI systems (at least with the current state of the technology) the fact that there will be errors or inaccuracies in outputs is effectively regarded as an inherent aspect of the technology. Whether or not this is tolerable depends on the error rate and the proposed application of the system – but the assessment needs to be made from a place of understanding the nature of the errors that occur. It should also review the extent of the insurance policies it has in place and how far those will cover those risks. And finally, it should consider what practical mitigations it can implement alongside its contractual protections.

Mark Leach is a partner in Bird & Bird's London office and co-head of the firm's International Outsourcing and Technology Transactions practice groups. He specialises in complex technology transactions, outsourcings and large-scale transformational projects. He also advises regularly on systems integration contracts, cloud computing arrangements and software licensing and development deals.
Mark's clients include financial institutions and major corporates (particularly in the aerospace and defence and technology sectors), as well as a number of technology vendors.
Mark speaks regularly at industry events on outsourcing and commercial technology issues and has been regularly named as a 'Leading Individual' in outsourcing in the latest edition of the *Chambers Guide to the UK Legal Profession* and has been recognised in *The Legal 500's Hall Of Fame* for IT and Telecoms work.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: mark.leach@twobirds.com
LinkedIn: www.linkedin.com/in/mark-leach-bb83b94a

Will Bryson is an associate in Bird & Bird's Tech Transactions team, advising on a variety of technology contracts with a focus on complex and cutting-edge procurement. This ranges from software development, licensing and maintenance agreements, cloud and SaaS projects, complex technology procurements, to multi-billion pound contracts for the building of naval vessels.
Emerging technology is Will's focus area, Artificial Intelligence in particular. He helps clients navigate the risks and legal issues which present themselves when buying or selling new technologies. Being surrounded by likeminded individuals at Bird & Bird is an important part of this.
During his time at Bird & Bird, Will has spent time on secondment with Arm Limited (a leading semiconductor design business), a large defence company, a middle eastern giga project, and a US-based AI provider, giving Will a real appreciation of the concerns clients have and how to best meet their needs.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: will.bryson@twobirds.com
LinkedIn: www.linkedin.com/in/will-bryson-29b51938

Calling all Technology and Business Services Sourcing Professionals. Your Industry Needs You!

Global Sourcing Association

Kerry Hallard

In the 2023 edition of *ICLG – Technology Sourcing*, I talked very much about the advent of "Modern Sourcing" and how new approaches to traditional sourcing practices were coming to the fore and improving the efficiency and effectiveness of strategic sourcing. This movement has accelerated significantly and here at the GSA, our programme of work throughout 2024 and 2025 is dedicated to driving "sustainable" strategic sourcing – and we mean sustainable in the broadest sense of the word. Yes, absolutely environmental sustainability, yes, social responsibility, but also being sustainable by driving operational efficiency and business resilience.

Throughout this chapter, I hope to articulate not only what sustainable strategic sourcing is, but also make a very clear call to action for every single reader to play a role in driving more sustainable strategic sourcing for the good of *business*, *people* and *planet*. Working better together, I believe we can make a seismic difference to all three.

I will share the programme of work we are undertaking globally and crystalize not only the benefits of this approach, but also how comparatively small corporate changes can make a massive difference. This is illustrated perfectly by a case study from GSA Award winner, GSK, which, although dating back a number of years, showcases GSK's visionary approach to sustainable strategic sourcing which absolutely increased GSK's operational resilience and business performance.

Case Study

The work undertaken by GSK's Tech Sourcing department won the company our "Sourcing Works" Award several years ago and since then has been a poster child for the GSA. This is a fantastic example of the changes corporates can make to deliver true sustainable strategic sourcing. Doing the right thing with suppliers treated as partners can deliver very tangible business benefits.

Introduction

GSK is a science-led global healthcare company that aims to deliver growth and improving returns to shareholders through the development of innovative pharmaceutical, vaccine and consumer healthcare products and employs 70,000 people worldwide.

Backdrop

On 8th September 2015, GSK's competitor base increased exponentially. On this date, the pharmaceutical world changed forever when the FDA approved the first digital therapy, providing treatment through *technology*, rather than molecules, making the "traditional" pharma market an untapped opportunity for the world's tech giants, including the likes of Google and Amazon. This was a game changer: how could a company that had existed for 300 years compete with nimble tech companies that can change like the wind with a tendency to simply buy start-ups to acquire capability. Whereas for many pharma companies, contracting with these innovative start-ups can be nigh on impossible due to risk aversion and strict levels of compliance. Furthermore, the request for proposal (RFP) cycle in which GSK's traditional procurement had been eternally caught, had stifled partnerships and collaboration.

The truth of the matter was that GSK was losing significant market share, falling from fifth to ninth position globally – and a lot of this was to do with its technology sourcing. It had mega deals with tier one service providers that were not flexible and could not innovate quickly. And due to GSK's RFP and contracting processes, let alone its 120-day payment terms, no smaller tech companies could – even if they wanted to – partner with GSK. GSK realised this all needed to change. GSK needed to challenge and disrupt its old ways of sourcing.

Project overview

GSK set out to fundamentally change the way it conducted business with its third parties, aiming to:

- become the **fastest** and **easiest** company to contract with disruptive start-ups and to drive thought leadership and innovation, reducing the standard 24-week procurement lifecycle;
- create a specialist Tech Sourcing Function to enable delivery of innovation at **pace** compared to the industry standard;
- replace the continuous RFP cycle with strategic partnerships based on **trust**, **transparency** and **co-investment**, whilst driving tangible business value; and
- drive a **cultural change** to embed agile ways of working and the fail fast mentality, whilst changing the company's historically strong stance on being risk adverse.

> *"I have worked with many large multinational companies and can honestly say how impressed I am at how quickly we were able to get through the procurement processes. GSK ranks as the top most efficient. GSK has really defined the way large multinationals should engage with start-ups."* CEO of Retechnica, Marco Iannone

Business value

The results far exceeded GSK's ambition. GSK cut its contracting templates for start-ups from 120 pages to just

four pages – saving 134 trees per year and 40,000 hours of negotiations. Being able to secure contracts in days, rather than months, gave GSK a competitive advantage. Fourteen-day payment terms made GSK a very attractive customer to partner with. This approach enabled it to conduct over 100 experiments in four months – some of them promising potential life changing results for customers.

GSK also formed strategic partnerships with 11 suppliers, concentrating on co-invested transformational activities rather than draconian RFP cycles. In return, those 11 partners removed sales targets and instead teams were measured purely on joint value creation.

These initiatives created more than an additional £100m savings – allowing more investment in research and enabling patients to "do more, feel better and live longer".

Although now six years on, I personally believe there is still so much other companies can learn from this example – and the GSA is leading the charge to make this happen – globally. With the introduction of artificial intelligence (AI), blockchain and other newer technologies, and the increasing focus on all things ESG, traditional procurement of technology and business services will become obsolete and evolve into sustainable strategic sourcing.

Welcome to FormIGA, the Industry for Good Alliance for Global Technology and Business Services

The global technology and business services industry is taking a monumental step forward with the launch of FormIGA, a pioneering initiative that unites global buyers and service providers to improve the tech and business services industry with best practices, ethical standards, sustainability and innovation. Developed collaboratively by industry association leaders (the Global Sourcing Association (GSA) in the UK and the International Association of Outsourcing Professionals (IAOP) in the US) and supported by a Global Advisory Council of enterprise organisations, FormIGA represents a movement with profound purpose, aimed at fostering a better world for business, people and planet.

The work of FormIGA has been developed by the industry, for the industry. The technology and business services industry is unlike any other industry. It is incredibly global in its nature and is very advanced in its use of transformative technologies. It is highly innovative and people centric. It is for this reason that FormIGA exists. Work undertaken by both the GSA and IAOP will be fed into FormIGA, where best practices and guidelines are reviewed and agreed by a global standards board. Organisations can be assessed, then audited for their performance towards meeting these guidelines and either accredited or given the opportunity to revise – with advice – before accreditation.

Our Mission and Objectives

Our vision is for partnerships to significantly reduce global poverty and create a sustainable planet for all to enjoy.

Our mission is to drive the transformation of the global technology and business services sector by pioneering best practices and establishing clear guidelines and standards for sustainable partnerships.

Our purpose is to enhance the buying and delivery process, instilling an ethos of ethical conduct and promoting innovation to position the industry as a force for good.

We strive to elevate the reputation of the sector, expanding its reach and creating sustainable value for all stakeholders, reinforcing our industry as an integral contributor to societal advancement.

FormIGA's Programme of Work

The first pillars supporting our programme of work for 2024 include:

The Service Provider Sustainability Index

A key initiative of FormIGA is the recently-launched Service Provider Sustainability Index (SPSI). The SPSI (www.formigaspsi.com) is an industry index based on the self-assessment of service providers' sustainability and ESG maturity. It delivers benchmarks and insights to create a level playing field. The SPSI is the first standardised sustainability index specifically designed for service providers in the technology and business services sector, offering a clear and consistent framework for evaluating and improving social and environmental performance.

For buyers, SPSI offers:

- A robust, ready-made questionnaire for buyers to use with all service providers.
- An easy-to-understand score.
- An easy way to understand how well your service providers are performing against each other and against the rest of the industry – across all parameters that are key to your company.
- A detailed report highlighting your providers' strengths and weaknesses, enabling an action plan on where improvements need to be made.
- The ability to change the weightings of sections/questions to reflect what's most important to your company.

For providers, SPSI offers:

- A detailed report highlighting strengths and weaknesses, enabling an action plan on where you need to make improvements.
- Data insights to highlight how the industry is changing over time.
- The ability to change your score as you make changes to your processes/policies – so you are always putting your best foot forward.
- Once information has been filled in once, it can be shared many times, leading to significant time and cost savings.
- An easy way to understand how well you are performing against the rest of the industry.

The ambition is to have an Index of the ESG performance of technology and business service providers across all their sites around the world, offering regional as well as corporate trend insights.

FormIGA Directory

One of FormIGA's key innovations is the creation of a central repository that consolidates assessments and performance data for all service providers and technology partners worldwide. This repository enables buyers to evaluate and compare their partners' social responsibility performance, ensuring they collaborate with companies that excel in this area. Simultaneously, providers gain insights into their strengths and areas for improvement, fostering continuous enhancement across the industry.

Agile sourcing

We have published our maturity assessment framework and best practice guide on how buyers and providers can enjoy a more collaborative and fruitful approach to the traditional RFP.

Impact sourcing

"*Impact Sourcing is all about intentional inclusive employment. It is a business practice centered around a commitment to hiring and providing career development opportunities to people in marginalized[1] communities who are often excluded from the mainstream world of work.*"

Our industry has created millions of jobs and taken many more millions of people out of poverty. There is so much more to do here. Through the reinforcement of impact sourcing best practices, we will create many millions more jobs and truly give transformational employment opportunities to disadvantaged communities. A new global impact sourcing standard is in the making.

Supplier diversity

Most companies want great diversity in their supply chains, as much as they want great diversity, equality and inclusion (DEI) in their workforces. Sadly, this isn't as easy as it sounds. GSA, as a founding member of the Council for Supplier Diversity and Inclusion UK, will present the latest research on the adoption of Supplier Diversity, case studies from those companies that have pledged significant spend with diverse suppliers, as well as the best practices on how to build and manage a good diverse supplier programme and juxtapose this with learnings from the advanced supplier diversity programmes in the US.

Industry standard terms

The Standardisation revolution continues. Great work continues from the Chancery Lane Project. In 2023, the GSA launched Industry Standard Terms for an IT and Professional Services framework agreement governed under English law, as well as a standard non-disclosure agreement (NDA). Both are housed in Clausify.co, a unique legal tech platform that ensures all terms are locked from editing. We are reviewing whether this standard contract could be adopted globally, before moving on to negotiate a balanced and fair full outsourcing agreement for the whole industry to use.

Ethical adoption of AI

We will cover global topics from safeguarding IP, avoiding bias, renegotiating gainshare through to the impact of conversational AI on the customer experience (CX) industry. We are also reviewing the opportunity of developing a global competences and capabilities framework for AI skills with bodies around the world, whilst simultaneously reviewing how we can reduce the significant environmental impact of using AI.

Commenting on the intersection between AI and Industry Standard Terms, David Jones, Founder Clausify commented:

"*The increasing utility, acceptance and adoption of generative AI technology will, we see, further accelerate the drive towards standardisation. We believe this will occur for two, mutually reinforcing, reasons: (a) AI achieves better results when it is presented with a consistent format and structure. If a machine knows where to look for specific content, it is more likely to be able to interpret that content than if the content was instead randomly spread around other different types of content; and (b) we believe that in a world where the highest functionality generative AI negotiates against highest functionality generative AI (on the other side), the net result is a balanced agreement. If asked to perform this negotiation a second time, logic suggests the two machines would end up with the same document. This then effectively becomes a standard agreement.*

The benefit to adopting standardisation now, is that we get to shape it, rather than waiting for computers to force these inarguable efficiency gains upon us."

Conclusion

Imagine a world where all enterprise buyers followed sustainable strategic sourcing best practice, akin to GSK. Idealistic? Perhaps, but if we don't set a vision and try to achieve it, we never will.

Through agile sourcing we can partner faster and include more diverse suppliers and therefore innovate more.

Through adopting industry standard terms, we can get to contract and therefore production/service faster, whilst also levelling the playing fields to help SMEs thrive, in doing so driving even more innovation.

Through comparing ESG performance at an industry level, we can showcase high performers and help lower performers improve. In doing so, we can improve the ESG performance of the whole industry, boosting the reputation of the industry so it continues to grow and thrive.

Through sharing the industry's excellent ESG performance and best practices on a global stage, we can help other industries improve and further improve the impact of climate change.

Through engaging only with partners in countries that have really effective DEI programmes, we could collectively influence unjust political regimes.

Through a committed approach to impact sourcing, we could collectively work to achieve massive inroads to the UN's number 1 Sustainable Development Goal, which is to eradicate global poverty whilst simultaneously addressing the global talent crisis.

All technology sourcing professionals – buyers, providers, lawyers, advisors, consultants, analysts, academics, etc., have a vital role to play in driving this change. We need to encourage these best practices to be included in all sourcing arrangements and collaborate to drive the thinking and standards forward to drive meaningful change.

Let's make this change together. All whilst making companies more robust and more profitable – truly delivering to the triple bottom line of business, people and planet.

Endnote

1 We define marginalized as people who are living in poverty or under-represented in the workplace in any given country.

Kerry Hallard, MBA, is the Chief Executive Officer of The Global Sourcing Association (GSA), Chair of the Global Technology & Business Services Council, Co-founder of the Council for Supplier Diversity and Inclusion UK and co-Founder of FormIGA, the Industry for Good Alliance. Kerry speaks on the importance of sustainable strategic sourcing all around the world and advises companies and delivery destinations how to align themselves to the very latest in industry best practices.

Global Sourcing Association
Kemp House
152–160 City Road
London, EC1V 2NX
United Kingdom

Tel: +44 77 7469 0447
Email: kerryh@gsa-uk.com
LinkedIn: www.linkedin.com/in/kerry-hallard
URL: www.anindustryforgood.com

The Global Sourcing Association (GSA) is the industry association and professional body for the buying and provision of global technology and business services. The GSA is a social enterprise striving to make a difference and promote positive change across the technology and business services industry.

The GSA is the consistent voice for the future of the industry and the professionals working within it; promoting sustainable and ethical sourcing to create a positive future for our businesses and our shared planet.

The GSA is the founding member of the Global Technology & Business Services Council (gtbsc.org), an alliance of a dozen of the leading industry associations from around the world focused on looking at the macro factors affecting the industry globally. The GSA is also a founding member of the Council for Supplier Diversity UK, the focus of which is to develop the best practice for building and managing a diverse supply chain. The GSA welcomes buyers, providers and advisors, as well as technology start-ups into its ecosystem.

www.gsa-uk.com

Australia


Hamish Fraser


Kate Morton


Madeleine Clift

Bird & Bird

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, in general private sector procurement of technology products is not the subject of regulation in Australia. However, purchasers in some regulated industries may bound by certain industry specific regulations such as the Australian Prudential Regulation Authority's Prudential Standards or the *Security of Critical Infrastructure Act 2018* (Cth). Requirements under such regulation may include mandatory terms to be included in technology supplier agreements and may impose reporting or audit requirements on suppliers.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

In Australia, we have two levels of legislation: (1) federal legislation, which applies Australia-wide; and (2) state and territory legislation, which only applies in each state and territory.

At a federal level, procurement by government or public sector bodies is regulated generally under the *Public Governance, Performance and Accountability Act 2013* (Cth) and Commonwealth Procurement Rules (**CPRs**), dated 13 June 2023. The CPRs ensure that public resources are used in the most efficient, effective, ethical and economic manner and reflect the Australian Government's commitment to improving the competitive capability of small and medium enterprises.

The procurement of information and communications technology (**ICT**) products and services are also specifically regulated by the Digital Sourcing Framework (**Framework**), which sets out a set of principles, policies and guidance that regulate how the Australian government buys digital products and services. The Framework has a number of policies that provide guidance including the Consider First Policy, Fair Criteria Policy, Panels Policy, Contracts Limits and Reviews Policy and Hosting Certification Framework. There are also state and territory laws, regulations and policies that regulate procurement, including the *Government Procurement Act 2001* (*ACT*), the ACT Government Procurement Framework, the *Public Works and Procurement Act 1912* (NSW), the NSW ICT Purchasing Framework, Queensland Government Procurement Policy 2021, the Queensland Information Technology Contracting (**QITC**) framework, the Tasmanian Procurement Framework and Treasurer's Instruction under the *Financial Management Act 2016 (Tas)*, the South Australian Government Procurement Framework, the *Procurement Act 2020 (WA)*, the Western Australia Procurement Rules, the *Procurement Act 1995* (NT), the NT Procurement framework, and the *Financial Management Act 1994 (Vic)*.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No. Australian law does not regulate the term of the supply of technology-related solutions.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No. Australian law does not directly regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services.

However, in some cases, a term which gives one party, but not the other party, the right to terminate could be considered an unfair contract term under the Australian Consumer Law at Schedule 2 to the Competition and Consumer Act 2010 (Cth). The unfair contract terms regime (**UCT regime**) apply to standard form contracts with individuals or small businesses with 100 or fewer employees, to protect parties that have little or no opportunity to negotiate the terms. A term will be unfair if it causes a significant imbalance in the rights and obligations to the parties, it is not reasonably necessary to protect the legitimate interests of a party and would cause financial detriment to

the individual or small business. Businesses can be penalised for including unfair terms, with the maximum fine being up to $50,000,000; three times the value of the benefit obtained from the conduct (if the court can determine this); or if a court cannot determine the benefit, 30% of adjusted turnover during the breach period.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

No. There is not an overriding legal requirement for a customer and/or supplier of technology-related solutions or services to act fairly according to a general test of fairness or good faith. There is some uncertainty under Australian law regarding the extent to which a duty of good faith or fairness can be implied into contracts. In some circumstances, a court may find that a duty of fairness or to act in good faith can be implied into a contract after considering the terms of the contract. Legislation also prohibits some behaviours that would be considered unfair or that lack good faith, including the prohibitions on unconscionable, misleading or deceptive conduct under the Australian Consumer Law, as well as the unfair contract term provisions referred to in the response to question 2.2 above.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The principal remedy available to a customer under general law in Australia for a breach of contract by the supplier is a claim for damages, which is generally a monetary award to compensate the customer for its loss. Other remedies that may be available include injunctions or orders for specific performance. Also, consumer guarantees under Australian Consumer Law apply to contracts for goods and services (including those provided in a B2B context) with a value of AU$100,000 or less and AU$100,000 or more for goods and services ordinarily provided for personal or domestic use.

Statutory remedies for a breach of consumer guarantees include:

a. repair, replacement or refund: where a consumer has the right to ask for a free repair for a minor problem, or a free replacement or refund for a major problem;
b. compensation for damages and loss: a consumer can seek compensation for damages and losses suffered due to a problem with the product or service if the supplier could have reasonably foreseen the problem; or
c. cancellation of the service: a consumer can cancel a service where there is a major problem with the service or a minor problem that cannot be fixed within a reasonable period of time.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

The additional remedies or protections that are typically included will depend on the nature of the solutions or services and the relevant parties. Possible remedies include the right to service level credits for breaches of service levels and the right to terminate if material breaches are not remedied within a certain time. For more complex solutions or business critical services, remedies may include software escrow provisions, step-in rights or transition assistance requirements.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

There must be a specific right to terminate in the contract. If there is no contractual right to terminate, there may be a common law right to terminate if the other party breaches an essential term, the other party's breach of a non-essential term is sufficiently serious or the other party repudiates the contract.

2.7 Can the parties exclude or agree additional termination rights?

Yes. The parties may exclude or agree additional termination rights.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Liability can generally be limited or excluded under Australian law by agreement between the contracting parties. However, legislation may prevent the ability to exclude or limit liability in some circumstances; for example, if the contract is a standard form contract with an individual or small business, a clause that limits one party's liability but not the other may be unenforceable for being an unfair contract term and pecuniary penalties may apply (see question 2.2 above). Additionally, liability for some breaches of the Australian Consumer Law may not be excluded or limited.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes. In general, parties are free to agree a financial cap on their respective liabilities. However, legislation may limit the ability in some circumstances; for example, if the contract is a standard form contract with an individual or small business, a clause that limits one party's liability but not the other may be unenforceable for being an unfair contract term and pecuniary penalties may apply (see question 2.2 above). Additionally, liability for some breaches of the Australian Consumer Law may not be excluded or limited.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

The general principles described above apply to all the types of technology procurement contracts listed.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Parties usually (and contracts usually mandate the parties must) first attempt to resolve disputes through good-faith negotiations.

If negotiations fail, parties can agree they must try to resolve disputes through alternative dispute resolution methods such as mediation, expert determination or arbitration. Mediation is often preferred because it is cost efficient (can be done with no external costs – although mediation is frequently better if lawyers and an independent mediator are engaged), expedient (can be done quickly) and can also lead to better outcomes (a "win/win" as opposed to a litigation-based "winner takes all"). As a last resort, parties can resolve disputes through litigation; however, litigation is expensive and may not be justified in many technology transactions.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

Usually IT companies (in the business of IP creation) will own any IP rights developed by it. Typically, the IP in a technology sourcing transaction will be copyright in any source code.

The contract should explicitly address IP ownership and licensing/usage rights and will ensure IP rights land where the parties intend. If the contract involves bespoke IP generation, usually a developer will retain any background IP, but the customer will seek to own any developed IP or a broad licence to use that IP. The developer and the customer may agree to some exclusivity to protect the customer's investment.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Any assignment of the ownership of IP rights must be in writing and signed by the assignor. For registered IP, such as trademarks and patents, the formalities for assignment are determined by the relevant registry managed by IP Australia. There is no register for copyright in Australia.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

There is no specific statute law in Australia that protects trade secrets, know-how and business-critical confidential information. However, trade secrets, know-how and confidential information are protected under common law principles of equity, where equity imposes a duty of confidence whenever a person receives information he/she knows or ought to know is fairly and reasonably to be regarded as confidential. The *Corporations Act 2001* (Cth) also provides broad protection against a person who obtains information as an officer or employee of a corporation from improperly using that information.

It is common for all contracts (including employment and independent contractor agreements) to have confidentiality clauses.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes. Personal data in a technology context is protected by a range of laws including:

a. *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles included in Schedule 1 of the Privacy Act (**APPs**);
b. privacy legislation in each state and territory, which may apply in the context of technology services provided to state or territory governments and public sector entities;
c. health data legislation in some states and territories, which may apply in the context of technology services that deal with health records;
d. telecommunications legislation, which applies to some personal data in the communications context; and
e. *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**), which applies to certain assets deemed to be critical under the SOCI Act.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside Australia. Under the Privacy Act and APP 8, before personal data can be transferred overseas, either reasonable steps must be taken to ensure that the overseas recipient does not breach the APPs; whoever is transferring the information must be reasonably satisfied that the overseas recipient will be subject to a law that is at least as protective as the APPs and there is a mechanism for Australian individuals to enforce those protections; or alternatively, the individual must be specifically advised that reasonable steps will not be taken to protect the personal information and the individual must consent to the disclosure after being so advised. Similar requirements generally apply if the data is subject to state or territory privacy laws.

The Australian government is in the process of reviewing the operation of the *Privacy Act 1988* (Cth) and the APPs and has agreed in principle to the following reform proposals:

(a) introducing GDPR inspired standard contractual clauses for use in overseas data transfers; and
(b) strengthening consent and notification requirements when disclosing information overseas.

5.3 Are there any legal and/or regulatory requirements concerning information security?

APP 11 requires organisations to take steps that are reasonable in the circumstances to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Other relevant legal requirements, including data breach notification requirements (based on type of information and industry), include those under:

a. the Privacy Act;
b. the *Crimes Act 1914* (Cth);

c. State and Territory criminal laws;
d. the *Security of Critical Infrastructure Act 2019* (Cth);
e. the *Telecommunications (Interception and Access) Act 1979* (Cth);
f. part 13 of the *Telecommunications Act 1997* (Cth);
g. regulation by the Australian Securities and Information Commission; and
h. in relation to financial services, *Prudential Standard CPS 234 – Information Security*.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Yes, employees can be transferred; however, there is no automatic transfer by law in an outsourcing transaction – employees will only transfer if they accept an offer of employment with the new employer.

Section 311 of the *Fair Work Act 2009* (Cth) (**FW Act**) provides that a "transfer of business" occurs where:

a. the employment of an employee of the old employer has terminated;
b. within three months of the termination, the employee becomes employed by the new employer;
c. the work the employee performs for the new employer is the same, or substantially the same, as the work the employee performed for the old employer; and
d. there is a "connection" between the old employer and new employer.

For the purpose of the fourth limb in the above definition, there will be a "connection" where:

a. there is a transfer of assets from the old employer to the new employer in relation to the transferring work (e.g. machinery or computer systems);
b. the old employer outsources work to a new employer;
c. a new employer ceases to outsource work to the old employer; or
d. the new employer is an associated entity of the old employer (meaning they are related bodies corporate or one has a controlling interest in the other).

Provided that the above definition is met, a transfer of business having occurred will mean that the employee's prior service with their 'old' employer will count as service with their new employer, including for the purpose of:

a. in all cases, including where a transfer of business has occurred between two non-related corporate entities:
   i. the right to request flexible working arrangements;
   ii. unpaid parental leave rights; and
   iii. accrued but unused personal/carer's leave; and
b. in the event of a transfer between two related corporate entities (i.e. businesses within the same corporate group), in addition to the above entitlements:
   i. eligibility to make an unfair dismissal application;
   ii. accrued but unused annual leave;
   iii. accrued but unused long service leave (subject to the applicable long service leave legislation and an employee's employment location history);
   iv. the minimum periods of notice to be given by either party in exercising the right to terminate the employment with notice; and
   v. recognition of the employee's prior period of service for the purpose of calculating their entitlement to redundancy pay.

6.2 What employee information should the parties provide to each other?

The FW Act and *Fair Work Regulations 2009* (Cth) (**FW Regulations**) contain record-keeping obligations, including to make and retain accurate and complete employee records for a period of seven years. Where there is a transfer of business, the old employer must transfer each employee record concerning a transferring employee to the new employer.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

No, only the employer/outsourcer can dismiss an employee. A customer/service provider could, however, inform the employer/outsourcer that they no longer require the employee to perform services for it.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, the new employer can offer terms consistent with existing employment terms, subject to the following:

a. a transferable instrument, such as an enterprise agreement that covered a transferring employee of the old employer, will continue to cover those employees with the new employer; and
b. where the service provider agrees contractually in the outsourcing agreement or alike, to make offers on no less favourable terms, the harmonised offers would need to provide terms that are at least as beneficial as the transferring employees' terms with the old employer.

If the new employer does not offer terms and conditions of employment which are substantially similar to, and, when considered on an overall basis, no less favourable than the employee's terms and conditions of employment with the former employer, the former employer may be required to pay the employee statutory redundancy pay.

6.5 Are there any pensions considerations?

Where the transferring employee is a member of the old employer's superannuation scheme, unless the employee nominates a particular new superannuation fund, the new employer will need to arrange for future superannuation contributions to be made into that employee's superannuation scheme.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Broadly, the main consideration will likely be which entity is the employing entity, i.e., does the employer still have a connection to Australia and is it governed by the FW Act? Consideration should also be given to entitlements, including whether entitlements should be in accordance with Australian or foreign provisions.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

In Australia, there is no federal legislation that specifically regulates outsourcing transactions, and the applicable regulatory regime will depend on the industry sector to which the outsourcing relates.

Federal government entities have specific accountability regulatory regimes that they must comply with including the *Public Governance, Performance and Accountability Act 2013* (Cth) (**PGPA Act**), which requires procuring federal government entities to conduct themselves to enable the efficient, effective, economical and ethical use of limited public resources.

For the financial services sector, the Australian Prudential Regulation Authority (**APRA**) will enforce prudential standards and practice guides on outsourcing (for example, *Prudential Standard CPS 231 Outsourcing, Prudential Standard HPS 231 Outsourcing, Prudential Standard SPS 231 Outsourcing and Prudential Standard CPS 234 Information Security*), which set rules for APRA-regulated entities to outsource a "material business activity" and require entities to maintain minimum procurement standards and address requirements such as liability, indemnity, subcontracting, information security and insurance.

From 1 July 2025, CPS 230 will replace and consolidate CPS 231 and 232 and their associated standards. CPS 230 will expand the scope of CPS 231 to apply to all material service providers and material arrangements on which the entity relies to undertake a critical operation (being operations that if disrupted would cause a material adverse impact) or that expose it to material operational risk. The new prudential standard will also introduce additional obligations for regulated entities.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The simplest structure is a contract between the customer and the supplier.

However, parties may also choose to enter into:

a. joint venture arrangements, such as unincorporated/incorporated joint ventures, where the customer and the supplier enter into an agreement to provide services together by contributing capital, resources and/or sharing the benefits; or
b. multi-sourcing arrangements, where customers require multiple suppliers to execute similar contracts.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Most contracts still rely on some form of price adjustment (service credits, rebates, etc.) for a failure to meet applicable service levels. The adjustment will usually be capped (for example, capped at a certain percentage of the monthly fees). There can be protracted negotiations regarding whether the customer is also entitled to more general damages for a failure to meet the service level (for example, is the failure to meet a service level a breach in and of itself).

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Charges can be fixed monthly charges (often with collars and caps to prevent abuse or profiteering) or variable charges per type of transaction (often with a floor and a ceiling) or a combination of both.

Usually, fixed charges are used in circumstances where there is a baseline of costing or the outsourcing is more predictable, or the customer requires a smaller volume of work.

Most contracts will have a schedule of additional fees for unexpected items.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

The method of transfer will determine the formality necessary. The method of transfer will be determined by a consideration of the importance of the third-party contract and risk of failure. There is not one particular way that a third-party contract can be transferred to a service provider. Common formalities include:

a. Tripartite Agreement between the third party, new service provider and the customer. A properly drafted tripartite agreement is the best way to clearly set out who owes what rights to whom.
b. Deed of Novation between the third party and service provider. A Deed of Novation usually transfers the entire contract and the outgoing party has little or no further involvement, but may require a reversion clause for when the outsourcing transaction is complete.
c. Deed of Assignment, where the customer can transfer the benefit of a third-party contract (e.g. the right to receive services); however, the customer retains the ongoing obligations under the third-party contract to the outsourcer. A plan to assign necessarily involves a review of the third-party contract as many contracts prohibit assignment.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Please consult a tax expert for advice on these issues.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

For on-premises implementations, the issues remain largely the same as they have for 20+ years:

a. **Implementation**
Who is implementing the software and the nature of the changes to be made to it are central to any implementation contract. This is linked to an important question of whether the software itself works and the implementation is to adapt it to the customer environment, or if there is some doubt that the software can be made to work at all. These questions are important to ensure a proper allocation of risk and failure. Vendors will often have revenue recognition requirements, meaning that the licence fees cannot be made contingent on implementation.

b. **Waterfall *vs* agile**
The waterfall model of on-premises software installation still has a place. It requires a clear understanding of the customer's needs and a robust acceptance testing regime with suitable deeming processes. It is important for these to be drafted in line with actual or likely processes and not based on positional or relative bargaining powers.
However, particularly where software is being developed, there is an increasing shift towards agile development models. Agile contracting can be challenging for lawyers, as often all that can be drafted in an agreement is the process, and the developer in essence needs to be trusted to deliver the outcome.

c. **Licence restrictions**
Vendors of software for on-premises use will still have various licencing models that need to be considered and managed within the customer's environment. User types (e.g. concurrent users or permitted users), related entities and contractors need to be reviewed and matched with the customer's needs. Other questions such as processor types (e.g. quad core or virtual machines) are also common, as are geographic restraints.

d. **Other issues**
The other matters to be considered include warranties, noting that very few software vendors will warrant that software is uninterrupted or error-free. Warranties surrounding security threats increasingly require closer examination.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Key issues to consider include:

a. faults: definitions of what comprises a fault's severity and what steps are to be undertaken (repair or merely respond) and by when;

b. scheduled maintenance: when maintenance is scheduled and when maintenance outages must occur – in a 24/7 business world, this is a question of increasing importance;

c. updates: customers must carefully consider the terms on which the supplier may install (or insist on) the adoption of new versions (as well as the difference between a version, release or patch); and

d. security: customers should be aware about how updates and maintenance will affect their security.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes, they are used and are enforceable in Australia, but are increasingly uncommon for on-premises due to the rise of Software as a Service (**SaaS**) cloud-based software.

A well-drafted software escrow arrangement can be a critical component of risk mitigation for customers. Software escrow agreements should ensure that the customer has access to the source code on the occurrence of certain events, such as insolvency, and that there is minimal disruption to the customer's business.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No, there are not. However, regulation of the procurement of cloud computing services often involves the Privacy Act if dealing with personal information and APRA standards if in relation to financial services.

The SOCI Act may also apply to the procurement of cloud services where the services are classed as a critical infrastructure asset or where the cloud provider is aware that they are providing services relating to business-critical data of a critical infrastructure asset.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Australia is generally a keen adopter of cloud computing.

Australian organisations are expected to spend AU$23.2 billion on public cloud services in 2024, up 19.3% from 2023 (https://itbrief.com.au/story/australia-s-public-cloud-services-to-surge-to-23-2-billion-in-2024). Large enterprises across most Australian business sectors have adopted the public cloud.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Key issues include:

a. Ownership/access to data: there are no overt laws governing ownership right in data under Australian law. This is more important for cloud contracts, which are likely to involve access to data, where the parties must agree to the form in which that data will be supplied at the end of the contract (and whether the form is dependent on the basis for termination).

b. Liability for data loss: where there is data loss in the cloud, the contract will need to make clear which party must take what steps to remedy and report, as well as specify the allocation of liability and what sanctions will apply. Relevantly, for data breaches of personal information under the Privacy Act, the Office of the Australian Information Commissioner (**OAIC**) may seek civil penalties. Obligations under the SOCI Act should be taken into account where it applies.

c. Insolvency: where the cloud computing provider becomes insolvent, cloud users will be unsecured creditors and will have no special grounds to recover their data. Cloud computing users should consider transitional provisions, escrow (or escrow-like) arrangements and ensure they back up their data.

d. Data retention: The APPs require that entities destroy or de-identify personal information they hold when the information can no longer be used for the purpose for which it was collected. Guidance from the regulator has recommended that service agreements or contractual arrangements address data retention periods and processes for destroying or de-identifying data. The *Telecommunications (Interception and Access) Act 1979* (Cth) provides mandatory data retention laws for services providers (internet services

providers and carriers), requiring services providers to retain particular information about a communication that is facilitated by its service for a period of two years.

e. Compliance with the Privacy Act: users of cloud computing should be aware of their obligations under the Privacy Act, particularly in relation to when personal information can be collected, notifying individuals regarding when their personal information has been collected, use and disclosure of personal information and cross-border disclosure of personal information.

f. Compliance with the SOCI Act: users subject to the SOCI Act should be aware of their obligations to maintain appropriate cyber security and risk management measures and ensure, where relevant, that they notify the provider where it provides data storage or processing services in relation to the user's business critical data.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

There are no laws or regulations which specifically regulate AI solutions or technologies. However, the Australian government has identified AI as a critical technology in the national interest and has released various publications which will guide the future development of Australia's AI regulations, including the AI Ethics Framework to assist the design, development and implementation of AI in Australia. The Government has issued its interim response to the 2023 Safe and Responsible AI Discussion Paper and has committed to:

- developing a voluntary AI safety standard with the National AI Centre;
- consulting on further AI law reform and voluntary schemes;
- fostering government and industry engagement internationally to shape global AI governance; and
- continuing to consider opportunities to support the adoption and development of AI and other automation technologies in Australia, including the need for an AI Investment Plan.

The Australian Government has also signed the Bletchley Declaration and has committed to working with the international community to ensure AI is developed with the right guardrails in place.

The ACCC has made observations in the Digital Platforms Enquiry about the potential for AI to cause "undesirable, unequal and/or unfair outcomes". They noted that this can arise from unconscious bias of system programmers or biased datasets used by algorithms. Other publications include the Australian Human Rights Commission's 2021 Human Rights and Technology report, which sets out a number of key responsible AI recommendations and Standards Australia's 2020 AI Standards Roadmap, which provides a framework for the development of future standards with respect to the use of AI in Australia and working papers published by the DP-REG joint regulators forum consisting of the ACCC, the Australian Communications and Media Authority (ACMA), the eSafety Commissioner (eSafety) and the OAIC: *Literature summary: Harms and risks of algorithms (Algorithms WP) and Examination of technology: Large language models*.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Like English law, in Australia, there is no single property right that applies to data. Although some IP rights may exist, the best and safest way to control data is to treat it like confidential information.

Where these IP rights exist in the relevant training data, an appropriate IP or know-how licence can then be granted. Australian courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore be licensed on a purely contractual basis.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Australian law on AI and intellectual property has not progressed as significantly as in other jurisdictions and, as yet, there have been no changes to existing legislation to deal with the ownership of something created by AI.

The Full Federal Court's recent decision in *Commissioner of Patents v Thaler* [2022] found that AI cannot be an inventor under Australian patent law and is an indication of how AI may be treated in other areas of intellectual property. Further, as a general rule, copyright in Australia can only be attributed to a human creator who contributed independent intellectual effort.

AI and ownership or infringement of IP is an evolving space and has many complications and nuances that will need to be tested and/or legislated upon before this area of law is resolved in Australia.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There are currently no national laws that deal solely with the procurement of blockchain-based solutions.

Instead, laws have been confirmed also to apply to the use of blockchain solutions and cryptocurrencies such as the Electronic Transactions Act 1999 (Cth) expanding to enable electronic commerce and self executing contracts. There have also been amendments to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML Act**), which brought "digital currencies" within the scope of Australia's anti-money laundering regime and imposed obligations on exchanges that facilitated the purchase of digital currencies.

The federal *Digital Assets (Market Regulation) Bill 2023* is currently before the Senate; if enacted, the bill will, among other objectives, provide a framework for digital asset exchanges, digital asset custody services and the issuing of stablecoins.

Regulatory bodies have released guidance on the application of existing laws to blockchain-based solutions.

For example, the Australian corporate regulator, the Australian Securities & Investments Commission (**ASIC**) released an information sheet (INFO 225) in May 2019 on how and when cryptocurrencies could constitute "financial

products", which imposes additional compliance obligations on projects bound by these rules. The Australian Taxation Office also released guidance on the taxation consequences of disposing of cryptocurrency tokens, "Tax treatment of cryptocurrencies".

ASIC has been actively enforcing this existing legal framework to regulate crypto businesses, including in two recent Federal Court cases (*Australian Securities and Investments Commission v Finder Wallet Pty Ltd [2024] FCA 228* and *Australian Securities and Investments Commission (ASIC) v Web3 Ventures Pty Ltd* [2024] FCA 64) where the Court found that certain crypto products offered by the businesses were financial products and required an Australian Financial Services Licence.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

The main industries are finance, cybersecurity, supply chain management and healthcare.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Key legal issues include:

a. licensing for cryptocurrencies: in certain circumstances, ASIC has confirmed that cryptocurrency can constitute a financial product, depending on the asset's legal status and associated rights. In those circumstances, financial services licensing and disclosure requirements would apply;
b. cross-border issues for cryptocurrencies: carrying on a financial services business in Australia requires foreign financial services providers to hold an Australian Financial Services Licence;
c. reporting requirements: the AML Act applies to any entity that engages in financial services or credit activities in Australia (specifically including exchanges that facilitate the purchase of digital currencies) and obligations include reporting requirements;
d. the nature of the rights and obligations of the parties under a smart contract: e.g., whether copyright is transferred with a non-fungible token; and
e. competition and consumer law regulations: the solution provider needs to ensure it is not anti-competitive or providing materials which could be misleading or deceptive.

Hamish Fraser is the lead partner of Bird & Bird's Australian IT and Communications Groups in Sydney, with clients at the cutting edge of legal and regulatory developments in the region. Hamish advises on commercial issues and regulatory matters for clients in all facets of the information technology and communications industries. Whether buying or supplying IT and communications, he provides detailed advice and contracting experience on digital businesses, software, cloud, distribution, confidentiality, e-commerce, security, IT procurement and outsourcing. Hamish has acted in a number of patent, copyright and trade mark cases. Before joining Bird & Bird, he held a senior legal role at Optus, Australia's number two telecoms carrier. Over many years, Hamish has been a prominent contributor to public policy discussion in the industry and mainstream press as a result of his extensive practice in convergence, social media, privacy and data protection.

Bird & Bird
Level 22, 25 Martin Place
Sydney, NSW 2000
Australia

Tel: +61 2 9226 9815
Email: Hamish.Fraser@twobirds.com
LinkedIn: www.linkedin.com/in/fraserhamish

Kate Morton is a special counsel in the Bird & Bird Tech & Comms, Commercial and Corporate Group in Sydney, and advises the firm's leading clients on a wide variety of technology, communications and IP law issues, where her experience as a software engineer and consultant gives her additional practical insight. Kate has experience in negotiating and drafting private sector and government contracts for consulting and technology services and advises on the legal aspects of cloud computing, data protection and emerging technologies. In addition, Kate assists in business and share sale transactions for technology-rich companies. Kate's experience also encompasses licensing and protection of copyright, trademarks and patents and the regulation of the media and telecoms industries.

Bird & Bird
Level 22, 25 Martin Place
Sydney, NSW 2000
Australia

Tel: +61 2 9226 9882
Email: Kate.Morton@twobirds.com
LinkedIn: www.linkedin.com/in/kate-morton-26483722

Madeleine Clift is an associate working across the Commercial and Corporate Groups in Sydney. Madeleine has advised clients on both a local and multinational scale on a broad range of matters including data privacy compliance, commercial transactions and contracting, dispute resolution and regulatory compliance. In addition, Madeleine has experience in assisting clients to re-work their data management and IP ownership practices; drafting data sharing arrangements; undertaking privacy and commercial due diligence for transactional matters; providing regulatory advice; preparing privacy impact assessments; and commercial contracting and negotiations.

Bird & Bird
Level 22, 25 Martin Place
Sydney, NSW 2000
Australia

Tel: +61 2 9226 9888
Email: Madeleine.Clift@twobirds.com
LinkedIn: www.linkedin.com/in/madeleine-clift-a50299124

Bird & Bird has more than 1,600 lawyers in 31 offices across Europe, the Middle East, Asia-Pacific and North America and clients based in 118 countries worldwide. We specialise in combining leading expertise across a full range of legal services and aim to deliver tailored local advice and seamless cross-border services.

Our technology sourcing practice is widely recognised as having a leading reputation in the field and enjoys top tier international rankings in *The Legal 500* and *Chambers* Guides to the legal profession. We advise on the full range of technology transactions, including complex outsourcings and managed services deals, system implementation projects, telecoms infrastructure and regulatory matters, strategic alliances and collaboration agreements, cloud computing deals and contracts for the deployment of AI and blockchain-based solutions.

www.twobirds.com

Bird & Bird

France


Stéphane Leriche


Marion Barbezieux


Chris Ivey


Cathie-Rosalie Joly

Bird & Bird LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, private sector procurement of technology products is not the subject of regulation in France.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes, the procurement of technology products or services is regulated unless the financial stake of the contracts is below €40,000 (or €100,000 if the agreement relates to innovative products or services). The applicable rules can be found in the Public Procurement Code (Articles L. 2000-1 through 2728-1). Public procurement transactions rely on competitive bids and are governed by a very precise and stringent set of rules pertaining to tendering process, review and selection of the offers, monitoring of performance, etc.

The basic underlying principles are as follows:

- **Equal Treatment**: Buyers must treat all bidders fairly and without discrimination.
- **Open Access**: Every operator should have transparent access to public tenders.
- **Transparency**: Key rules must be clear, objective, and published. Changes during the bidding process are not allowed.
- **Public Procurement Efficiency**: Ensuring effective use of public funds.
- **Sustainable Development**: Public procurement should contribute to sustainable development objectives.

Contractual documentation will be provided by the buyer. In the context of technology products and services, the general terms and conditions will most commonly be based on the *Cahier des Clauses Administratives Générales* (CCAG-TIC) (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043310689), which is a set of pre-defined rules governing the procurement of services and products involving the use or creation of intellectual property (IP) rights. Those rules can be deviated from in the specific terms and conditions (CCAP) that capture the legal provisions specifically tailored to the projects. The technical specifications will be embedded in a document called the CCTP or Functional Program. There is usually little room for negotiation of the CCAG and CCAP and legal documentation originating from the bidders will generally not be discussed or agreed to, except, in certain cases, general licence terms. In any event, a vendor's terms will always be overridden by contractual documentation provided by the public buyer and will be listed at the lowest rank in the documentation precedence order.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

Private sector

French law does not regulate the term of the supply of technology-related solutions.

However, as a general note, French law prohibits perpetual commitments. A term will therefore have to be defined in the contract; otherwise, each party would be entitled to terminate the agreement at any time subject to reasonable notice.

Public sector

Public contracts must be entered into for a limited term. The duration of the contract is defined by taking into account the nature of the services and the need for periodic retendering, under certain conditions (Article L.2112-5 of the Public Procurement Code). A public contract may provide for one or more renewals provided that its characteristics remain unchanged and that the competitive bidding process has been carried out, taking into account its potential total duration.

Unless otherwise specified, the renewal provided for in the contract is automatic and the supplier cannot oppose it (Article R. 2112-4 of the Public Procurement Code).

Framework contracts (i.e., those allowing the order of services or products based on subsequent orders or agreements) can be entered into for a maximum duration of **four years**, except in exceptional cases where the performance of the contract requires investments to be depreciated over a longer term (Article L.2125-1 of the Public Procurement Code).

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No. French law does not directly regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services. It is left to the parties to negotiate.

However, a sufficiently long notice period must be given before terminating an "*established commercial relationship*". An established commercial relationship is a regular, stable and customary relationship, in relation to which one party could reasonably anticipate a certain continuity in the future flow of business with its commercial partner.

Article L.442-1, II of the French Commercial Code outlines the following:

- When a commercial relationship ends abruptly (even partially), and there is no written notice commensurate with the duration of that relationship, the party responsible for the termination becomes liable. They are obligated to compensate for any resulting damage.
- In case of a dispute about the notice period, the party terminating the contract will not be held liable if they provided **18 months' notice**.

Our experience shows that a three-to-six-month prior notice is market practice (save for exceptionally long relationships).

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes. Good faith is a fundamental notion of French contract law, a guiding principle enshrined in Article 1104 of the French Civil Code: "*Contracts must be negotiated, formed and performed in good faith. This provision is of public policy.*"

Legislation also prohibits some behaviours that would be considered unfair or that lack good faith, including prohibitions on misleading or deceptive conduct, as well as fraud and wilful misconduct.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Pursuant to Article 1217 of the Civil Code, a customer may:

- suspend the performance of their own obligations (e.g., withhold payment until the breach is remedied);
- seek an order for specific performance, if this remedy can be exercised;
- seek a price reduction;
- terminate the contract for breach (in whole or part); or
- seek compensation for the damages and losses suffered (or claim contractually agreed penalties that are considered a fixed and binding pre-estimation of damages).

Those remedies are cumulative unless they are incompatible with one another (e.g., terminating the contract and requiring specific performance).

Where the parties agree on contractual warranties in the contract, they may also agree on the remedies that would be available in the event of a breach of such warranty. These remedies for breach of warranty usually include repair or replacement of the product or service, refund and/or cancellation.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

The additional remedies or protections that are typically included will depend on the nature of the solutions or services and the relevant parties. The most common additional remedy consists of service credits that apply in case of breach of service levels. Service credits may qualify as penalties or price reductions, depending on the intention of the parties and drafting options.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

A contract with a definite term can only be terminated early for breach or *force majeure*, unless the terminating party has been granted a right to terminate for convenience. Where termination for convenience is exercised, the other party must be compensated. The compensation is generally based on a percentage of the fees that should have been invoiced until the end of the contract and/or unamortised costs.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties are free to exclude or agree specific termination rights. Please note, however, that any exclusion or additional rights should not create a significant imbalance between the rights and obligations of the parties, especially if the contractual terms are not negotiated (Article L.442-1 of the Commercial Code) and should therefore be mutual unless there is a valid legal, economic or technical reason that the termination right should only be available to one party. Please note also that the non-defaulting party will always have the right to terminate the contract in case of material breach, notwithstanding any clause to the contrary.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Liability can generally be limited or excluded under French law by agreement between the contracting parties.

However, legislation may prevent the ability to exclude or limit liability in some circumstances. In particular:

- Liability cannot be excluded in case of wilful misconduct or gross negligence.
- Tort (extra-contractual) liability cannot be contractually limited or excluded.
- A limitation or exclusion of liability provision may be deemed unenforceable under Article 1170 of the Civil Code if it voids the essential obligation of one party from its substance. This may be the case, for instance, where a party excludes its liability resulting from the breach of an essential obligation under the contract, or where the list of the damages excluded is so broad that it amounts to depriving the other party from any actual remedy in case of a failure by the breaching party to fulfil its essential obligations under the agreement.
- If the contract is a based on a non-negotiable standard form, a clause that limits one party's liability but not the other may be void for being an unfair contract term, especially with an individual or small business.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, subject to the limitations set out in question 2.8 above (based on Article 1170 of the Civil Code), the parties are generally free to agree on a financial cap on their respective liabilities.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement

contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, they do not. The general principles described above apply to all types of technology procurement contracts listed.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Disputes between commercial parties will be generally brought before the French Commercial Courts unless another Court has exclusive statutory jurisdiction (e.g., *Tribunal de Grande Instance* for IP right matters). Binding arbitration is sometimes retained notably in contracts involving US vendors.

It is common for technology contracts to provide for "alternative dispute resolution" processes as preliminary steps to be taken in order to try to resolve a dispute before the final stage of litigation or mediation/arbitration. Such steps often include:

- one party giving notice to the other of the nature of the dispute;
- levels of commercial negotiation between the parties about the dispute, first at an operational level with the issue being escalated up to project managers, any relevant steering/project committee and the parties' executives if it cannot be solved within specific periods of time; and
- mediation or expert determination.

Regarding litigation before State Courts, it should be noted that the procedure language is French and the briefs, the pleadings and the ruling will be made exclusively in the French language. Evidence may be submitted in English, but the Court may require that they are translated for the convenience of the judges or at the request of the other party.

Please note, however, that a special chamber was created at the Commercial Court of Paris in April 2018 dealing with international disputes and where briefs can be submitted and pleadings made in English.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In a technology services contract, the parties usually remain the owners of the IP rights they have developed before or independently from the technology transaction (Background IP). The contract will define which IP constitutes Background IP, and a limited licence to use the Background IP will be provided to the other party for the sole purpose of executing its obligation under the technology services contract and/or using these services. The intention is that any use outside of those parameters will be prohibited.

The parties will also have to consider what new IP rights may come into existence during the course of the technology transaction (Foreground IP). The technology services contract will need to make provisions for who will own the Foreground IP and what licensing/usage rights are granted.

If the contract involves bespoke IP generation (specific developments), usually a developer will retain any Background IP, but the customer will seek to obtain an exclusive assignment of rights on the developed IP or a broad licence to use that IP.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes – different formalities apply depending on the IP right being assigned:

- for patents, trademarks and registered designs, the assignment must be in writing and signed by the assignor. The assignment must be recorded with the National Register (INPI) in order to be effective against a third party who acquires rights in the patent, trademark or registered design without notice of the assignment; and
- for copyright, the assignment must be in writing and signed by the assignor. According to Article L.131-3 of the Intellectual Property Code, the transfer of the author's right is subject to the condition that each of the transferred rights is mentioned separately in the transfer deed, and that the field of exploitation of the transferred rights is delimited as to its extent, destination, geographic scope and duration. Thus, in France, the law provides that any transfer of copyright, even partial and not definitive within the framework of a licence or an assignment, must be formalised by a contract whose content must precisely detail: (i) the work on which the rights are granted (as general and future assignments are unenforceable); (ii) the rights transferred and the modes of exploitation and destination; (iii) the duration of the licence; (iv) the geographical scope; (v) the exclusive or non-exclusive nature of the licence; and (vi) the financial terms of the licence. There are, however, no registration requirements. It should also be noted that under French law, moral rights cannot be sold, assigned or otherwise transferred: licence grant and assignment can therefore only relate to the economic rights.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

In France, trade secrets are protected by the Law of 30 July 2018, which transposes European Directive 2016/943 into French law. Article L.151-1 of the Commercial Code defines the protected trade secret as: "Any information meeting the following criteria: 1° It is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to persons familiar with this type of information due to their sector of activity; 2° It has an actual or potential commercial value due to its secret nature; 3° It is the subject of reasonable protective measures by its legitimate holder, given the circumstances, to preserve its secret nature." Articles L.151-4 to L.151-6 of the Civil Code describe trade secret breaches for which one may be held liable.

In order to protect their know-how, trade secrets and other business critical information, parties will typically agree to confidentiality provisions in technology services contracts. Confidentiality provisions in a technology services contract are likely to:

- define the know-how, trade secrets and confidential information of each party;

- create a contractual duty to maintain this information in confidence (subject to some typically agreed carve-outs); and
- define the duration of the confidentiality undertakings.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes. Personal data in a technology context is protected by a range of laws, including:

a. the General Data Protection Regulation ((EU) 2016/679) (GDPR) of 25 May 2018;
b. Act No. 78-17 of 6 January 1978 (as amended by Law No. 2018-493 dated 20 June 2018 regarding the protection of personal data) on Information Technology, Data Files and Civil Liberties (applicable to data protection issues); and
c. sector-specific rules that may also apply to certain types of technology services contracts, particularly in the financial, telecommunications and healthcare sectors.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Personal data can be transferred outside France, but the organisation will need to ensure that it has implemented safeguards and protection in accordance with Chapter V of the GDPR to ensure that the recipient of the data confers on the personal data a standard of protection that is comparable to that under the GDPR. This can be achieved through various mechanisms, including:

- transferring the data to a country for which the European Commission has issued an adequacy decision;
- entering into Standard Contractual Clauses (SCCs) with the importer, based on the new EU SCCs of 4 June 2021 (2021/914/EC) and carrying out a Transfer Impact Assessment to identify any supplementary measures that should be implemented; and
- executing binding corporate rules.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Under the GDPR, an organisation is required to protect the personal data in its possession or control by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The GDPR also contains a specific obligation regarding data breaches.

Sector-specific information security requirements may apply to certain types of technology services contracts (for example, the revised Payment Services Directive for digital payment transactions), while the Network and Information Security Directive contains requirements in terms of cybersecurity.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

French legislation on the automatic transfer of employees (Article L.1224-1 of the Labour Code) is likely to apply to outsourcing transactions and certain other technology services-based agreements, but a careful factual and legal analysis is required to determine whether each element of the test is met. The transfer legislation applies where there is a transfer of an "autonomous economic entity" that retains its substance and the business of that "entity" is continued in a similar way post transfer. An "autonomous economic entity" is defined as a self-standing organised grouping of individuals to which tangible and/or intangible assets are attached and are required to perform the business activity. This "entity" must therefore have its own objectives and purpose, and also its own means, in order to be autonomous.

If Article L.1224-1 of the Labour Code does apply, the employees who are, immediately prior to the transfer, wholly or mainly assigned to the "autonomous economic entity" that has, as its principal purpose, the carrying out of the relevant service, will automatically transfer to the transferee.

If the outsourcing or other technology services agreement comes to an end and the customer brings the relevant services back in-house, or if there is a change in supplier, this in itself does not automatically trigger the transfer of the employees, but if the conditions set out above are met, in particular with respect to the transfer of tangible and/or intangible assets, the employees who are wholly or mainly assigned to the transferred services will also be transferred.

Depending on the factual circumstances, where services are being split and transferred to multiple new suppliers, it may be possible for an employment contract of a transferring employee to be split between each of the transferees in proportion to the tasks being performed by the worker.

Under the transfer legislation, all of the rights, liabilities, powers and duties of the outgoing employer under or in connection with the transferring employees' contracts of employment will be transferred, with limited exceptions. This includes any pre-existing liabilities (e.g., arrears of pay, claims with current employees) and accrued contractual benefits. The transferee steps into the shoes of the transferor and legally it is as though the transferee has always been the employer. Specific rules apply in relation to the terms and conditions of employment provided for by collective agreements.

6.2 What employee information should the parties provide to each other?

Under the provisions of the Labour Code itself, there is no obligation for the transferor to provide any employee information to the transferee entity.

However, it is of course common practice to provide information such as the number of employees involved in the outsourcing, their job descriptions, key terms of their

employment contracts, and information relating to applicable collective agreements and unilateral commitments implemented within the transferor entity and applicable to the transferring employees, so as to enable the transferee entity to maintain those terms as required.

Where staff representative consultation is required, the transferor and/or transferee may require additional information around integration plans, in order to provide a full picture to the staff representatives and obtain their opinion on the project.

It should be noted that some industry sector collective bargaining agreements provide for additional information obligations in the context of a transfer of employment.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

If the dismissal is for a reason connected with the transfer itself and/or takes place immediately prior to the transfer, thereby effectively avoiding application of automatic transfer legislation, the dismissal will be void. The employee will be entitled to claim reinstatement within the transfer or damages for unfair dismissal.

It is, however, possible for the transferee to dismiss the employee post transfer for reasons not directly connected with the transfer itself.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Terms and conditions defined under a collective agreement applicable within the transfer will automatically apply to the transferred employees, who will also maintain the benefits of the transferor's collective agreements for a period of 15 months post transfer. During that period, the transferee should attempt to negotiate harmonised collective terms. If no harmonisation agreement is reached during that time, the transferred employees must continue to benefit from a level of remuneration at least equivalent to that applicable under the transferor's collective agreements, but other benefits will fall away.

Changes to individual terms and conditions of employment are possible subject to the employees' individual consent.

6.5 Are there any pensions considerations?

Standard mandatory basic and complementary pension schemes are not affected by the transfer in that the only obligation for the employer is to contribute to the schemes based on the employees' salary. Therefore, upon transfer, the contribution obligations will transfer alongside obligations related to other payroll taxes. If the transferor entity has a supplementary pension scheme in place, the transferee has the option to decide to implement a similar scheme.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

From a French law perspective, automatic transfer legislation is not considered to apply where the outsourcing would require a transfer to another country, as that would result in a fundamental change in the terms and conditions of employment, which would require the employees' consent (whereas an automatic transfer operates without requiring consent). The transfer of business to another country could form part of the basis for a redundancy procedure, subject to economic considerations and justifications as required by French law.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

There are no general national laws or regulations that specifically regulate outsourcing transactions. Outsourcing transactions in the financial services sector are subject to a specific regulatory framework deriving essentially from the European Banking Association Guidelines related to Outsourcing (February 2019) and *arrêté* of 3 November 2014 "*on the internal control of companies in the banking, payment services and investment services sector subject to the supervision of the Prudential Control and Resolution Authority (ACPR)*". Pursuant to such regulatory framework, financial institutions planning to outsource "critical or important functions" must comply with a set of rules and best practices in terms governance, audits, risk assessment, security of data and systems, business continuity, service levels, termination and termination assistance. Compliance with those rules must be assessed and reported on a regular basis and may be verified by the supervision authority (ACPR).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience (known as the DORA regulation) will complement this framework when effective in January 2025. It defines uniform requirements to strengthen and harmonise the management of risks related to information and communication technologies (ICT) and the security of networks and information systems at EU level.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The simplest structure is a straight contract between the customer and the supplier consisting of general terms and conditions and associated schedules.

However, parties may also choose to enter into a two-tier structure consisting of a Framework Agreement and Implementation Agreements where:

a. the customer wishes to set up a modular structure where lines of services can be subscribed, managed, charged or terminated individually; or
b. the customer wishes that affiliates (including foreign affiliates) are able to enter directly into a specific contract with the supplier on the basis of the Framework Agreement. The Implementation Agreement will then incorporate by reference the terms of the Framework Agreement and may include deviations in order to accommodate, *inter alia*, local law requirements.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Most contracts still rely on service credits for failure to meet applicable service levels. The service credits will usually be

capped (for example, at a certain percentage of the monthly or annual fees). The main negotiation point generally revolves around the ability for the customer to claim general damages on top of the service credits in case of severe breach (for example, material failure to meet a service level is a breach in and of itself).

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Charges can be fixed monthly/quarterly/annually or be variable per type of transaction (often with a floor and a ceiling) or a combination of both. Charges are generally invoiced on a monthly basis.

Usually, fixed charges are used in circumstances where there is a baseline of costing or the outsourcing is more predictable, or the customer requires a smaller volume of work.

Most contracts will define price adjustment mechanisms to account for significant volume variations or increase or decrease compared to the pricing baseline.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Consent from the assigned third party must be sought unless such third party has contractually agreed in advance to such assignment. Such consent must be expressed in writing (Article 1216 of the Civil Code).

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The most common tax issues that may arise in the context of an outsourcing contract relate to withholding tax where the service provider operates/invoices from a country where such taxes apply. Otherwise, outsourcing transactions do not raise specific tax issues.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

For on-premise implementations, the issues are basically the same in France as in any other jurisdictions. The following issues may be worth noting:

a. **Implementation failure:**
On-premise implementations are often carried out by ICT companies not related to the software vendor. Due to revenue recognition requirements, software vendors often refuse that payment of licence fees are made contingent on implementation. In such a case, customers may rely on Article 1186 of the Civil Code, which allows a co-contracting party to assert the "*caducité*" (i.e., nullification) of a given agreement in the event of termination or disappearance of a contract considered to be interdependent. Pursuant to indent 2 of Article 1186: "*When the performance of several contracts is necessary for the performance of the same transaction and one of them disappears, contracts whose performance is made impossible by this disappearance and those for which the performance of the contract disappeared was a determining condition of the consent of a party.*" This cross-default rule is often invoked in the context of IT projects especially to obtain the cancellation of a licence agreement following the termination of the integration services contract intended to implement such software in the customer's IT environment. This is generally upheld by French Courts in accordance with French Supreme Court case law (i.e., *Cour de Cassation*, 26 March 2013).

b. **Licence restrictions and audit:**
Vendors of software for on-premise use will still have various licencing models that need to be considered and managed within the customer's environment. User types (e.g., concurrent users or permitted users), related entities and contractors need to be reviewed and matched with the customer's needs. Other questions such as processor types (e.g., quad core or virtual machines) are also common, as are geographic restraints. Changes in the customer environment, whether or not prompted by the emergence of new technologies (e.g., virtualisation), are also often a ground for disputes. It should also be noted that Courts may set aside ambiguous licensing policies and that metrics are often ambiguous and refuse to enforce unilateral changes to such policies and metrics, which is also a cause for conflict, especially in the context of audits carried out by the vendor.

c. **Warranties:**
Typical US disclaimer of warranties will not be enforceable under French law (for instance, stating that the functioning software will not be uninterrupted or error-free is likely to be deemed invalid). Having said that, it should be noted that the breach of a so-called warranty does not trigger any specific remedy such as an "indemnity", which is an unknown concept under French law. The breach of a "warranty" may, under general law, entail the whole range of remedies available as listed under Article 1217 of the Civil Code (see question 2.4). An exclusive remedies clause may be enforceable provided it does not void the essential obligation from its substance (Article 1170 of the Civil Code).

Please note that the only relevant statutory warranty with respect to on-premise software is the warranty against latent defects (Article 1641 *et seq.* of the Civil Code) covering defects that could not reasonably be identified at the time of delivery. This warranty cannot be disclaimed except between professionals in the same field of business. It may result in total or partial refund of the price paid or in damages being paid. The warranty must be triggered within two years from the date the customer gained knowledge of the defects (or should have gained such knowledge).

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

French legal rules or market practices do not differ from those of other jurisdictions with respect to support and maintenance. The parties will, in practice, focus on the following aspects:

- **Business continuity**: Definition of outages/maintenance window/scheduled maintenance.
- **Service levels and service credits**: Please refer to section 7.
- **End-of-Support**: Customers should be granted access to sufficient notice (at least two years) when a software provider decides to discontinue support and maintenance support services for a standard software solution.
- **Termination assistance**: In case of a change in third-party maintenance supplier, the incumbent provider should assist the successor provider in gaining knowledge

of the maintenance environment and hand over all useful documentation, materials and data related to support and maintenance activities.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes, software escrow arrangements are commonly used and are, in theory, fully enforceable in the case of insolvency of the licensor/vendor of the software. However, insolvency judges have very far-reaching prerogatives and may prevent or delay the release of the source code where they consider that such release may undermine the recovery plan or divesting plan of the insolvent company.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

The "*Secure et Regulate the Digital Area Act*" of 24 May 2024 is the first statute that directly and specifically regulates the procurement of cloud services in order to foster competition in the provision of cloud services and establish trust between users and suppliers. The main provisions impacting cloud services are as follows:

- Prohibition of "cloud credits" whose duration exceeds one year or that are granted in consideration of exclusivity.
- Prohibition of "subordinate sales" whereby the purchase of goods or services is made conditional upon the subscription of cloud services and more generally of "self-preference" practices.
- Limitation of "switching fees" and "egress fees" invoiced by cloud computing providers to costs actually incurred by them.
- The obligation to comply with essential requirements in terms of (i) interoperability with other cloud providers providing the same type of services, (ii) portability of digital assets and exportable data to the customer's infrastructure or that of a competing vendor, and (iii) provision of APIs to customers and third-party providers designated by customers that are necessary to achieve the interoperability and portability purposes previously mentioned. In this respect, cloud providers will have to specify and regularly update a technical reference offer for interoperability.

Subordinate legislation will specify the date on which those provisions will come into force. To the extent that the provisions relating to switching, interoperability and portability are derived from EU Regulation 2023/2854 on harmonised rules on fair access to and use of data (the so-called Data Act), they should take effect at the latest in September 2025, as prescribed by the Data Act.

ARCEP (i.e., the electronic communications regulation authority) will have the responsibility of monitoring and enforcing these provisions).

Article 10 *bis* A of the GDPR lays down a sovereignty requirement for sensitive data (protection of public safety, public health or national security) and sensitive administrative documents in particular containing trade secrets or sensitive personal information. According to such requirement, any cloud provider will have to demonstrate that the technical and organisational specifications put in place do not allow access by the authorities of a third country (i.e., not within the EU). The above requirements will be complemented by subordinate legislation setting out the key criteria, which should be adopted within six months from the date of entry into force of the law.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing services are developing at a fast pace although their adoption rate is lower than in other European jurisdictions. In 2022, 35% of French companies had deployed at least one cloud computing service within their organisation. This rate was 71% among companies with more than 250 employees (*versus* 26% of enterprises with less than 50 employees).

9.3 What are the key legal issues to consider when procuring cloud computing services?

The main areas of concern when procuring cloud computing services are as follows:

a. Compliance with the GDPR (see section 5): It is necessary to ensure that, with respect to personal data, the cloud computing provider, which will in most cases act as a data processor, only processes data in accordance with the instructions of the customer (data controller), implements technical and organisational specifications to protect the security and confidentiality of such data, does not host or transfer the personal data in a country that does not have an adequate level of protection of personal data, and does not change the location of the servers or material subcontractors despite customer opposition.

b. Liability for data loss: Where there is data loss in the cloud, the contract will need to make clear which party is responsible for data backup, take steps to remedy and report the loss, as well as specify the allocation of liability and what sanctions will apply. Relevantly, for data breaches of personal information under the GDPR, CNIL (the data protection authority) may apply civil fines.

c. Switching and data migration: In case of expiry of termination of the agreement, the cloud computing provider should cooperate in the data migration process by making the customer's data available in a commonly used format and should refrain from hampering such data migration or switching of services by way of technical specifications, unreasonable switching fees or data egress fees (see question 9.1). The customer should be granted the possibility to extend the notice period/postpone the effective termination date to ensure that the data migration is completed before the terminated cloud computing services are switched off.

d. Specifically regarding software as a service (SaaS) offerings, implementation services are often carried out by ICT companies not related to the SaaS vendor. At the same time, the SaaS solution is often provided based on a multi-year subscription model with a yearly payment in advance of the subscription fee. Due to revenue recognition requirements, SaaS vendors generally object to the payment of subscription fees being made contingent on implementation, potentially putting the customer in a position where they have to pay for a solution that is not yet deployed or will not be deployed at all. In such a case, customers may rely on Article 1186 of the Civil Code, which allows a co-contracting party to assert the "*caducité*" (please see question 8.1 for further information).

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

There are no national laws or regulations regulating the procurement or use of AI-based solutions or technologies in France. However, the forthcoming EU AI Act adopted in April 2024 will be fully applicable in France when in force. As a reminder, the AI Act classifies AI systems based on risk:

- **Unacceptable risk**: Certain AI systems (e.g., social scoring and manipulative AI) are prohibited.
- **High-risk AI**: Most of the text focuses on high-risk AI systems, which are regulated. Developers and deployers of high-risk AI systems have significant obligations.
- **Limited risk AI**: A smaller section addresses limited risk AI systems (e.g., chatbots and deepfakes), subject to lighter transparency requirements.
- **Minimal risk AI**: Unregulated (including many existing AI applications on the EU market, such as AI-enabled video games and spam filters).

Notably, the users of high-risk systems must carry out and document a risk assessment, provide relevant information to the persons interacting with the AI system (capabilities, limitations, potential impact), monitor the behaviour and performance of the AI system, provide adequate incident reporting to competent authorities, and maintain human oversight over the system, etc.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

There is no concept of ownership of data under French law. Mere data cannot be subject to exclusive rights, except through contractual vehicles such as confidentiality agreements. However, extraction of data from databases, texts, designs, plans, etc., may give rise, respectively, to infringement of database rights, copyright, and trade secrets. Data scrapping carried out on websites may also be prevented by general terms of use of the relevant websites despite the fact that the extracted data are not protected by any exclusive right (CJEU, *Ryanair*, 15 January 2015, C30/14).

Whether protected by IP rights, trade secrets or only by contractual restrictions, data can be licensed or made available on a contractual basis. It should be noted that the EU Data Act, which will come into force in September 2025, will allow the legitimate users of connected equipment to access any data collected or generated by such equipment and require the holders of such data (e.g., the manufacturer or seller) to make such data available in a readable and accessible format. Users may also request that the data holders share such data with a third party specifically designated by them.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Algorithms are generally protected by trade secrets or, more generally, confidentiality. An AI system cannot be legally deemed a patent inventor (European Patent Office, 27 January 2020, EP 18 275 163 and 18 275 174) or an author for copyright purposes (*Cour de Cassation*, 15 January 2015) as those must be a physical person. As a result, the question of whether output created by an AI system can be the subject of IP rights and, if so, whom should be vested with such IP rights is still an open discussion bearing in mind that the answers may vary depending on the IP rights claimed, the nature of the input and the methods used to generate the output.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There are currently no national laws that deal solely with the procurement of Blockchain-based solutions, but a few sector-specific laws deal with specific uses of Blockchain: (1) digital asset service providers; (2) registration of financial securities on a Blockchain; and (3) a pilot scheme for market infrastructures based on Blockchain.

Digital asset service providers

France has had a regime applicable to digital asset service providers since 2019.

The French definition of crypto-asset as well as the regulated services are similar to those regulated under MiCAR (i.e., Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets), which will take precedence over the French regime from January 2025.

Under French law, a crypto-asset is:

- a token, which is any intangible asset representing, in digital form, one or more rights and **which may be issued, recorded, stored or transferred by means of a Blockchain**, enabling the owner of the asset to be identified, directly or indirectly, and excluding the tokens meeting the characteristics of financial instruments, medium-term notes and bills of exchange; or
- any digital representation of value that is not issued or guaranteed by a central bank or public authority, that is not necessarily attached to legal tender and that does not have the legal status of money, but is accepted by natural or legal persons as a medium of exchange **and can be transferred, stored or traded electronically**.

A service provider may qualify as a digital asset service provider if it provides at least one of the 10 services related to crypto-assets listed in the regulation.

Registration of financial securities on a Blockchain

French law allows the registration of some financial securities on a Blockchain, subject to the conditions laid down in the regulation.

Pilot scheme for market infrastructures based on Blockchain

In line with the European regulation on a pilot scheme for market infrastructures based on Blockchain, French law further modified its legislation to enable the issuance of bearer securities within a distributed ledger, such as Blockchain, under the pilot regime. The owner of a bearer security issued on a Blockchain pursuant to the pilot regime can also entrust an intermediary with certain tasks, such as the custody of cryptographic keys.

In addition to national legislation, the eIDAS 2.0 regulation will also have an impact on certain uses of Blockchain.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

The sector in which Blockchain-based technology has been most developed is banking and finance. Indeed, Blockchain technology has been developed to support transactions carried out via cryptocurrencies/crypto-assets, the main characteristics of which are that they are not dependent on a centralising body (such as a central bank) and are international.

However, the use of Blockchain is not limited to cryptocurrencies. Many other business sectors are already using Blockchain in France:

- **insurance** (e.g., automation of reimbursement procedures and simplification of certain formalities);
- **supply chain/healthcare** (e.g., product traceability, keeping track of the various stages in a production and distribution chain);
- **art/lux/IP** (e.g., fight against counterfeiting); and
- **regulated professions holding registers** (e.g., notarial profession).

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

The key legal issues to consider when procuring Blockchain-based technology vary according to the specific nature of each project. The key issues are generally the following:

- **Regulatory framework**: As explained in question 11.1, certain uses of Blockchain are regulated and may require a prior licence. It is thus necessary to check whether the use of Blockchain is regulated and, if so, ensure that the contractual framework aligns with the legal framework, taking into account the roles of each party (e.g., regulatory contractual requirements, geographical limits of the licence and of the provision of services, AML/CFT reporting obligations).
- **Data circulating on the Blockchain**: The type and processing of data on the Blockchain, as well as the rights, transfers and responsibilities associated with this data, and security provisions must be defined.
- **Smart contracts deployed on the Blockchain**: The smart contracts (i.e., development, audit, evolutions) as well as their legal effects (i.e., creation, termination, transfer of rights between parties, etc.) must be defined.
- **Responsibilities and insurance of parties and users**: The roles and responsibilities of the parties and users must be defined as well as the requirements in terms of guarantees and insurances where appropriate.
- **Dispute/jurisdiction**: Given the decentralised aspect and potentially large geographical footprint of Blockchain as well as the wide variety of geographical locations of the stakeholders, including users, the provisions in terms of dispute management, law and competent jurisdictions must be specified.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Delphine Frye in the preparation of this chapter. Delphine is a tech-friendly lawyer based in Paris, specialising in Fintech, cybersecurity, and data protection, committed to providing business-oriented and sustainable advice.

Stéphane Leriche is a partner in the firm's Tech & Comms Group in Paris, where he provides business-oriented advice on technology matters, notably in the field of software, cloud computing and electronic communications.
Stéphane's practice focuses on high-profile transactions and strategic partnerships, advising major companies in structuring strategic alliances, joint ventures, and IT and business process outsourcing deals. He has extensive experience of complex, structured contractual arrangements, particularly in regulated environments such as electronic communications or in the banking and finance sector.

Bird & Bird LLP
2 rue de la Chaussée d'Antin
75009 Paris
France

Tel: +33 1 42 68 60 00
Email: stephane.leriche@twobirds.com
LinkedIn: www.linkedin.com/in/stéphane-leriche-27637763

Marion Barbezieux is an associate working in the firm's Privacy Solution Team and in the Tech & Comms Group in Paris.
Since her qualification to practise law in France (Paris Bar) in 2015, Marion has worked in international law firms, providing business-oriented advice on commercial contracts and technology matters, notably in the field of software, cloud computing and electronic communications, as well as on data protection regulations (covering issues such as the General Data Protection Regulation and the ePrivacy Directive).

Bird & Bird LLP
2 rue de la Chaussée d'Antin
75009 Paris
France

Tel: +33 1 42 68 60 00
Email: marion.barbezieux@twobirds.com
LinkedIn: www.linkedin.com/in/marion-barbezieux-60712167

Chris Ivey is a partner in the International HR Services Group at Bird & Bird in France. He is dual qualified and advises on a broad range of individual and collective employment issues, both in France and on a European level.
Chris works with international companies conducting business in France on a wide range of employment issues, from day-to-day advice on issues with specific employees to restructuring projects and corporate transactions.
He has also built up specific expertise in cross-border work and multijurisdictional issues, including coordinating Europe-wide restructuring plans.

Bird & Bird LLP
Le Bonnel - 20, rue de la Villette
69328 Lyon Cedex 03 – Lyon
France

Tel: +33 4 78 65 60 00
Email: chris.ivey@twobirds.com
LinkedIn: www.linkedin.com/in/chrisivey

Cathie-Rosalie Joly is a partner in the firm's Finance & Financial Regulation, Tech & Comms and Media Groups, and leads Bird & Bird's French Fintech sub-group. She assists clients with disruptive digital technology adoption, providing legal advice and acting in regulatory litigation. She is based in Paris and often works in the firm's Belgium office.
Cathie-Rosalie has developed solid experience in regulatory and prudential matters (licensing or exemption procedures, freedom to provide services or freedom of establishment regimes, declaration of agents, distributors or intermediaries, contractual framing, etc.).

Bird & Bird LLP
2 rue de la Chaussée d'Antin
75009 Paris
France

Tel: +33 1 42 68 60 00
Email: cathie-rosalie.joly@twobirds.com
LinkedIn: www.linkedin.com/in/attorneycrjoly

Germany


Dr Henriette Picot


Michaela von Voß


Dr Rolf Schmich


Vincent Kirsch

Bird & Bird LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

There are no specific laws or regulations in Germany governing the procurement of technology products and services by the private sector in general.

However, the parties will be required to comply with general mandatory laws, such as the relevant provisions of contract law, standard terms and conditions and employment law under the German Civil Code (*Bürgerliches Gesetzbuch*, "**BGB**") or data protection requirements under the General Data Protection Regulation ("**GDPR**") and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, "**BDSG**").

Additional rules apply to specific industry sectors, products, and professions (such as, for example, the financial services sector, the healthcare sector, the telecommunication services sector, and providers of critical infrastructure).

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes. The procurement of technology products and services by government or public sector bodies in Germany is, in general – as all public contracts and concessions – regulated by the German Act Against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*, "**GWB**"), which implements EU requirements.

Under Section 97 GWB, procurement processes are in particular required to be (i) competitive, (ii) transparent, (iii) cost-efficient, and in accordance with the principles of (iv) proportionality, and (v) equal treatment/non-discrimination of all respective bidders/potential suppliers. Details of the applicable requirements depend on the type of tender process chosen by the tendering authority.

In addition, sector specific rules (including the German Sector Regulation (*Sektorenverordnung*, "**SektVO**") may apply for public contracting authorities active in specific sectors, such as, e.g., supply of drinking water, electricity, energy, transport services, defence and/or security.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

German law does not generally impose a minimum or maximum term for technology-related solutions and services contracts. However, specific rules may apply to contracts based on standard templates and to contracts with certain types of customers.

For example, in standard terms and conditions for the regular delivery of goods or the regular provision of services in B2C relationships, (i) contract terms of more than two years, and/or (ii) automatic contract renewals will be invalid and unenforceable unless a monthly right to terminate for convenience is granted after the expiry of the initial term (Section 309 no. 9 BGB). Conceptionally, similar boundaries may even apply in B2B relationships in case initial minimum contract terms imposed by a supplier are disproportionately long, depending, however, on the specific service provided and the circumstances of the individual case.

In addition, under Section 56 German Telecommunication Act (*Telekommunikationsgesetz*, "**TKG**"), the initial contract term for a telecommunications contract with a consumer (such as for internet or mobile services) may not exceed 24 months. If the contract is automatically extended, the consumer may terminate such contract at any time after the expiry of the initial term by giving one month's notice.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

German law does not generally regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services. However, specific rules may again apply to certain types of contracts and/or contracts with certain types of customers, as already mentioned (see above as set out in the answer to question 2.1).

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes. Under German law, the principle of good faith, known as "*Treu und Glauben*", is a fundamental legal concept that applies to all areas of law, including contracts for technology-related solutions or services. This principle is codified in Section 242 BGB and requires the parties to act in good faith and in a fair and equitable manner. In particular, this principle may influence the interpretation of contractual terms, the ability to exercise contractual rights, and may impose additional obligations not expressly set out in the contract.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Under German law, a customer can generally rely on a number of statutory remedies in case a supplier breaches a contract for the supply of technology-related solutions and services, including, in particular, the following:

a) **Claim for damages**: In the case of a culpable breach of contract, the customer may generally claim damages caused by the breach (Section 280 para. 1 BGB).
b) **Claim for performance**: The customer may demand performance, i.e., the actual fulfillment of the contract (Section 241 para. 1 BGB).
c) **Right to termination or rescission**: In the case of a significant breach of the contract, the customer may have the right to terminate or rescind from the contract (generally only upon fruitless expiry of a reasonable deadline for performance/fulfilment).
d) **Reduction of price/fee**: Depending on the type of the contract, the customer may have the right to reduce the purchase price/fees accordingly (Section 441 in the case of purchase agreements and Section 536 BGB in the case of lease agreements).
e) **Right to withhold performance**: The customer may have the right to withhold its own performance (usually the payment) if the supplier has not fulfilled its contractual obligations (Section 320 BGB).

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Typical additional contractual remedies or protections beyond statutory German law mainly depend on the type of contracted services and solutions, plus on the sector and bargaining position of the parties involved. Typical provisions include:

a) Service Level Agreements ("**SLAs**"), defining the level of service to be provided (including, for example, availability, quality, response times, service credits/penalties if agreed service levels are not met, and/or other performance metrics) and corresponding service credits/contractual penalties.
b) Contractual penalties, e.g. for breach of confidentiality or breach of data protection or data security obligations.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Under German civil law, a contract can be terminated without giving rise to a claim for damages in a number of ways, including:

a) **Termination for convenience**: If the parties have agreed on a right of termination for convenience or other contractual termination right (instead of, or in addition to, a fixed term), the parties may terminate the contract by giving notice within the agreed period.
b) **Termination for cause**: If a party cannot reasonably be expected to continue with the contractual relationship in light of the specific circumstances and considering both parties' interest (e.g., in the event of an uncured material breach of the other party), they may terminate the contract without notice (typically only after fruitless expiry of a deadline to cure the breach) (Section 314 BGB).
c) **Change of underlying circumstances**: Only in extremely exceptional cases, a party can terminate if (i) essential circumstances that have become the basis of the agreement have subsequently severely changed, and (ii) the relevant party cannot be expected to adhere to the contract in light of the contractual and statutory allocation of risk, and (iii) it is not possible or not bearable to adjust the agreement (Section 313 para. 3 BGB).
d) **Mutual consent**: The parties may, of course, also agree to terminate a contract by mutual consent.

2.7 Can the parties exclude or agree additional termination rights?

Under the principle of the freedom of contract, the parties are generally able to agree on additional contractual termination rights.

The statutory right to terminate for cause (see question 2.4 c) above) is mandatory and cannot be validly excluded by contract.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

The extent to which a contracting party can limit or exclude its liability under German law largely depends on whether the relevant contract qualifies as standard terms and conditions ("**T&C**") under German law or whether it has been individually negotiated.

In an individually negotiated contract, the parties cannot exclude or limit (a) liability for wilful misconduct, and/or (b) liability under the German Product Liability Act. The parties furthermore have to observe the general principle of good faith.

If a contract qualifies as T&C, the possibility for a party to exclude or limit its liability is very limited: In particular, a party cannot enforceably exclude or limit its liability (a) for damages caused by wilful misconduct or gross negligence, (b) for wilfully or negligently caused personal injuries, (c) for such damage as typically foreseeable at the time of entering into the contract in respect of damages caused by slightly negligent breach of a so-called material contractual obligation (*Kardinalpflicht*), (d) under the German Product Liability Act, or (e) to the extent a specific guarantee has been given.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Please see the response to question 2.8 above. The parties may (only) agree on a financial cap within the limits set out above regarding the limitation of liability.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

The principles set out above in the responses to questions 2.1–2.9 will generally apply to all of the above types of technology procurement contracts.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

In technology contracts under German law, regular dispute resolution before ordinary German courts is most frequently agreed, although binding arbitration clauses (often under the arbitration rules of the German Arbitration Institute ("**DIS**") are also common practice.

Litigious dispute resolution is often preceded by contractually agreed escalation mechanisms or (albeit less frequently) by other contractually agreed alternative dispute resolution mechanisms (such as mediation or expert determination).

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

As a contractual starting point, each party typically retains exclusive ownership in its so-called "Background IP" or "Pre-Existing IP", i.e., the intellectual property rights developed prior to or independently from the proposed transaction, including any enhancements or modifications made to same in the context of the execution of the transaction. In order to avoid subsequent dispute, the relevant Background IP is often defined/documented in the agreement. In relation to Background IP, non-exclusive licence grants are often required for the term of the agreement in order to enable the execution of the parties' contractual obligations.

In relation to new IP rights created in the course of a technology transaction, the parties will need to determine and regulate an appropriate allocation of IP rights and licence grants, depending on the overall intention and purpose of the transaction (e.g., whether it comprises bespoke development or whether protected work results might rather be a side effect or incidental outcome).

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Under German copyright law, ownership in the copyright as such (e.g., a copyright in a software program) cannot be assigned. Rather, the copyright as such will always remain with the individual human being who has created a protected work.

In order to enable another party to commercially exploit the copyright, the copyright holder can grant a comprehensive, exclusive and perpetual licence. A copyright licence grant generally does not require a specific form, except that a licence grant in relation to unknown future manners of use requires the written form in order to be valid. In any event, the written form is recommended for evidentiary purposes.

Similarly, the assignment of other intellectual property rights as such (e.g., patent rights, rights in inventions, rights in pending patent applications, utility rights, trademark rights, design rights) typically do not require the written form but should regardless be documented in writing at least for evidentiary purposes. An application is required in order to update the public registries.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

In Germany, trade secrets are protected under the Law on the Protection of Trade Secrets (*Geschäftsgeheimnisschutzgesetz*, "**GeschGehG**"), which implements the European Directive 2016/943 into German law.

Under Section 2 GeschGehG, a protected trade secret is defined as information fulfilling all of the following cumulative criteria: information (a) which neither entirely nor in its exact configuration and assembly of its components is generally known or easily accessible to persons typically handling this type of information and therefore is of economic value, and (b) which is subject to confidentiality measures appropriate to the circumstances that have been taken by its rightful owner, and (c) where a legitimate interest in the secret nature of the information exists.

In order to benefit from trade secret protection under the GeschGehG, the owner of the information must be able to demonstrate that they have taken appropriate protective measures, depending on the specific circumstances. In addition to organisational and technical measures taken to protect the secrecy, legal measures such as confidentiality agreements, often including a prohibition of reverse engineering, are common practice.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Processing personal data is in particular subject to the GDPR (EU) 2016/679) of May 25, 2018, the BDSG and the Telecommunication Digital Services Data Protection Act ("**TDDDG**"). In addition, further sector specific provisions may apply.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Where personal data is transferred to a country outside the EEA, the GDPR stipulates that the transferring party (data exporter) needs to implement safeguards and protections in accordance with Chapter V of the GDPR to ensure that the recipient of the data confers on the personal data a standard of protection that is comparable to that under the GDPR.

This can be achieved through a variety of mechanisms, of which the following are most commonly used:

a) Transferring the data to a country for which the European Commission has issued an adequacy decision.
b) Entering into Standard Contractual Clauses with the data importer, based on the new EU SCCs of 4 June 2021, 2021/914/EC and carrying out a transfer impact assessment ("**TIA**") to identify any supplementary measures that need to be implemented.
c) Reliance on binding corporate rules ("**BCR**").

5.3 Are there any legal and/or regulatory requirements concerning information security?

The GDPR requires the implementation of appropriate technical and organisational protection measures to ensure a level of security for personal data that is appropriate to the risk.

Depending on the relevant categories of personal data and the risk caused by a processing activity, such measures can include pseudonymization and encryption of personal data, technical measures ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident, as well as processes for regularly testing and evaluation of the effectiveness of technical and organisational measures.

The German Act on the Federal Office for Information Security ("***BSI-Gesetz***") imposes specific IT security related obligations, including registration and notification duties, *inter alia* on critical infrastructure providers in a broad range of sectors. Additional obligations are imposed by the EU NIS2 Directive and the EU RCE Directive, implementation of which into German law is due in 2024 and still in the legislative process.

Further sector-specific information security requirements may apply (e.g. the PSD2 Directive for digital payment transactions).

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

A transfer of employees by operation of German law occurs if the planned measure constitutes a transfer of business pursuant to Sec. 613a BGB.

The applicability of Sec. 613a BGB requires an "*identity-preserving transfer of a business unit*". This may apply if the key assets that characterise the business unit are transferred to another entity, with the transferred assets mainly utilised in a business unit as before. Therefore, the outsourcing of work previously carried out in-house basically only constitutes the risk of a transfer of business if relevant operating resources/assets are transferred to the external service provider. If no assets are transferred and only operational responsibilities are outsourced (e.g., a company completely closes its own IT department and then purchases IT services from third parties), Sec. 613a BGB will not be applicable.

In the technology sector, employees are usually the key asset because their know-how is crucial. The transfer of the majority of the employees of an IT department to another entity may therefore already trigger a transfer of business in the above-mentioned sense, with the consequence that all IT employees will automatically be transferred. However, technical equipment, software or intangible assets may also be important assets.

In the case of a transfer of business, the acquiring entity becomes the employer and generally takes over all rights and obligations in relation to the employment arising from all individual agreements, as well as collective agreements (if not being replaced). The employees have a right to object in writing to the transfer of their employment relationship within one month following receipt of a proper information letter pursuant to Sec. 613a para. 5 and 6 BGB. If the employees are not accurately and fully informed about the transfer, the one-month period does not start.

6.2 What employee information should the parties provide to each other?

The transfer of information needs to comply with data protection law. The processing of personal data must be necessary to achieve a specific purpose and must not conflict with a legitimate interest of the affected employees.

Information that is necessary for the performance of an (employment) contract and/or for compliance with a legal obligation (Art. 6 para. 1 (b) and (c) GDPR) may be provided to the transferee without the employees' consent.

In case of a transfer of business pursuant to Sec. 613a BGB, this means that typical data from the personnel file such as name, date of birth, address, bank details, as well as social, tax and payroll data shall be provided to the transferee at the earliest at the transfer date.

Special protected data (e.g., religious belief, trade union membership, health data) may be transferred if this is necessary to comply with employment, social security, and social protection regulations (Art. 9 para 1 and 2 (b) GDPR). For instance, the employer needs to know whether church tax is levied, the minimum ratio of disabled employees is met, or a collective wage applies.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

If a company completely shuts down the in-house IT department to procure IT services from third parties in the future and Sec. 613a BGB does not apply, the employees can generally be dismissed for operational reasons as there is no longer a role for them.

If the outsourcing measure constitutes a transfer of business, then according to Sec. 613a para. 4 BGB, the termination of the employment relationship by the previous employer or by the transferee due to transfer of a business is ineffective. The right to terminate the employment relationship for other reasons (e.g., breaches of employment duties or for operational reasons) will remain unaffected.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

In case of a transfer of business, the transferee takes over all rights and obligations arising from the employment relationship. As a rule, provisions of the employment contract cannot be amended without the employee's consent.

Pursuant to Sec. 613a para. 1 BGB, if rights and obligations are defined in a collective agreement or a works council agreement, they will become part of the employment relationship between the transferee and the employee and generally may not be changed to the employee's disadvantage before the expiry of one year after the date of transfer, except where the provisions are replaced by another collective agreement or have lost their binding effect.

6.5 Are there any pensions considerations?

The pension issue should be examined carefully. Provided a transfer of business in terms of Sec. 613a BGB applies, the transferee generally enters into the existing employment relationship with all rights and obligations including pension entitlements. If pension plans are based on collective agreements, particularities could apply.

However, it should be noted that the transferee does not simply enter into contractual relationships with third parties such as direct insurance companies and pension funds. Thus, precise planning and consultation with all parties involved will be required.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

In the case of cross-border asset transfers, it must first be clarified in accordance with Private International Law as to which national law is applicable. Within the EU, the Member States have implemented the "Transfer of Undertakings" Directive into national law in different ways.

Sec. 613a BGB is generally applicable to transfers of business from Germany to abroad. Thus, if the requirements are met, a notice of termination given in Germany due to the transfer of business would be invalid in accordance with Section 613a para. 4 BGB. However, in this context it is important to distinguish between the closure and reopening of another business and a transfer of business.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

There are no specific laws or regulations in Germany regulating outsourcing transactions in general.

However, additional rules apply to outsourcing transactions in regulated sectors and professions. In particular in the financial services sector, specifically strict requirements apply to outsourcing by banks and insurance companies both under EU Regulation and under national law (Section 25b German Banking Act (*Kreditwesengesetz*, "**KWG**", Section 32 German Insurance Supervision Act, *Versicherungsaufsichtsgesetz*, "**VAG**") and the related specific guidance by the German regulator (Federal Financial Supervisory Authority, *BaFin*) for IT outsourcing or use of cloud providers by the German regulator (such as the BaFin Circular 05/2023 – MaRisk,[1] Circular 10/2018 – VAIT (as updated in March 2022)[2] and Circular 02/2017[3]).

In addition, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience (known as the DORA regulation) will apply as of 17 January 2025.

Outsourcing may also be restricted in the health care sector (e.g., in relation to essential tasks of statutory health insurance funds under Section 197b Social Security Code V (*Sozialgesetzbuch V*, "**SGB V**").

German rules on professional secrecy impose very strict rules on disclosure of protected information to third parties, non-compliance with which is criminally relevant under Section 203 German Criminal Code (*Strafgesetzbuch*, "**StGB**"). Accordingly, outsourcing by customers subject to professional secrecy (e.g., physicians, lawyers, psychotherapists, tax advisors or insurances) is subject to specifically strict confidentiality obligations if and to the extent protected information is shared with a service provider.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

From a structural point of view, an outsourcing transaction typically comprises a main contractual document (master services agreement) accompanied by a larger number of attachments addressing detailed obligations in specific areas, as well as operational and commercial content (e.g., transition/set-up services, service level agreements, exit planning and exit obligations, emergency planning, IT security, data protection and fees).

Depending on the complexity of the overall arrangement (e.g., in case a modular structure is required to set up separately manageable and terminable services for one and the same entity or for different entities of a larger customer group), the structure can also be a framework master services agreement plus individual services contracts entered thereunder. In international set-ups, direct services agreements between the supplier and individual group entities (as service recipients) are common and may be advantageous, e.g. from a tax perspective and/or in order to accommodate for specific requirements by a local customer entity.

From a legal point of view, the most relevant statutory contract regimes in outsourcing transactions are, depending on the nature of the service provided and often combined in one and the same transaction, depending on the project phase and/or the type of services:

a) **Works Agreement** (*Werkvertrag*, Section 631 *et. seq.* BGB): Under a works agreement, the contractor is obliged to provide a specific outcome/success (e.g. a successful initial set-up or transition project).
b) **Services agreement** (*Dienstvertrag*, Section 611 *et. seq.* BGB): Under a services agreement, the service provider is (only) obliged to provide the specified service, but not a specific outcome or success.
c) **Lease Agreement** (*Mietvertrag*, Section 611 *et. seq.* BGB): E.g., regarding the licensing standard software during a specific term, hardware leasing or in case of SaaS (Software as a Service).
d) **Purchase Agreement** (*Kaufvertrag*, Section 433 *et. seq.* BGB): E.g., regarding perpetual software licensing or the sale of hardware.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Service levels and service credits are very commonly agreed, typically documented in an SLA):

a) **Service levels** outline the expected standard and quality of performance. They define the parameters against which the service provider's performance will be measured, such as response times, resolution times or system availability and also usually define the threshold to be met by the supplier in relation to each parameter.
b) **Service credits** are typically used as a performance incentive for the service provider. The overall amount of service credits is usually limited to a percentage of the monthly or annual service fee.

The details of service levels and service credits will, again, depend on the specific nature of the services being outsourced and the contractual parties.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The appropriate charging method depends on the type and predictability of services provided. Common charging models (often in combination with each other or as a hybrid model) include:

a) **Fixed pricing** per time period or per transaction (often subject to volume thresholds/within volume bands) or for a specific project or project part is used where a task or project has a well-defined and predictable scope.

b) **Time and material**-based remuneration is typically agreed where the scope of a project is subject to change or otherwise not predictable. Sometimes, time and material-based pricing is applied only during an initial phase of a project until certainty as to the overall scope or the efforts needed to carry out individual transactions has been reached.

c) **Milestone-based**: Payments are made when certain milestones or stages of the project are completed. This model can provide more control over the project for the customer and can help ensure that objectives are met before payment is made. Milestone payments can be structured as final payments or as mere advance payments on the remuneration due upon overall acceptance of the project results.

d) **Subscription or usage-based**: Commonly used for cloud services and software-as-a-service ("**SaaS**") arrangements. The customer pays a fee (usually monthly or annually) for access to, or the actual use of, the service.

In addition to the initial pricing arrangements, pricing adjustment mechanisms reflecting unexcepted volume changes (e.g. beyond pre-agreed bands) or depending on inflation are common. Agreements on larger, long term outsourcing transactions often also provide for benchmarking mechanisms to enable pricing changes based on a comparison with market prices for comparable services.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Under German law, the transfer of a contract generally requires the consent of all parties involved (Section 414 of the BGB). If an outsourcing transaction includes the transfer of third-party contracts, consent from the third parties is thus required. Accordingly, transfers are typically documented in a tripartite agreement between the original contracting parties and the service provider.

In relation to the transfer of employment contracts in the context of a transfer of undertakings, please refer to question 6.1.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The outsourcing of tax-related functions (like, for example, accounting) to a party outside Germany is subject to the restrictions of under Section 146 paras. 2, 2a and 2b of the German Fiscal Code (*Abgabenordnung*, "**AO**"). In principle, it must be ensured that the German tax authorities have unrestricted access to electronic data. Outsourcing to a country outside the EU requires the approval by the German tax authorities. Furthermore, for companies predominantly conducting a VAT-exempt business (financial institutions, insurances), outsourcing could lead to additional VAT cost, as these companies may not be able to (fully) deduct the VAT on the service fee as input VAT.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

From a German civil law perspective, perpetual software licensing is treated under the statutory concept for sales contracts, whereas term software licensing is qualified as a lease contract. In both scenarios, statutory warranties apply both in relation to defects in the software and in relation to defects in title.

Generally, a customer licensing software for on-premise installation should in particular consider the scope of the licence and the applicable licence metrics, contractual licence restrictions, the scope of software maintenance and support, provisions on warranty and liability, as well as review whether a data processing agreement (Art. 28 GDPR) is required in relation to remote or on-site support services enabling access to personal data stored in the customer's systems.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

When procuring support and maintenance services for software installed on customer systems, similar issues arise as in relation to the procurement of other technology-related support and maintenance services. The parties should particularly consider and include contractual provisions related to the following:

a) **Service Level Agreement** (please see our response to question 7.3 above for further details).

b) **Service description** (to clearly define the precise scope of the support and maintenance services to be provided).

c) **Termination** (to in particular stipulate (i) the conditions and notice period under which the parties may terminate the services entirely or partially, and (ii) whether, in the event of termination, support for transferring the services to a third party has to be provided).

d) **Security and confidentiality measures** (to be complied with by the service provider, especially if its employees require access to the customer's premises).

e) **Data protection**: A data processing agreement (Art. 28 GDPR) is required in relation to any support services enabling access to personal data stored in the customer's systems.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes, software escrow arrangements with professional software escrow service providers are commonly used to ensure continuity of source code access. Typically, a tripartite agreement is concluded between the software licensor, the customer, and a professional software escrow service provider. In order to increase the chances of enforceability in the event

of insolvency of the software licensor, granting rights of use to the source code already in the escrow arrangement (conditional upon the occurrence of an escrow trigger event) has become a common standard.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

There are no specific laws or regulations in Germany regulating the procurement of cloud computing services. Consequently, the principles outlined above in connection with questions 1.1 (private sector procurement of technology products and services) and 1.2 (government/public sector procurement of technology products and services) will apply.

In addition, the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, "**BSI**") has published the "C5 Criteria Catalogue for Cloud Computing" (updated in 2020) which specifies (non-binding) minimum requirements for secure cloud computing with the aim of giving cloud customers a guide to selecting a provider.[4] According to a study of the German Federal Network Agency, (*Bundesnetzagentur*, "**BNetzA**", most of the major Cloud Services Providers ("**CSPs**") (Amazon Web Service, Microsoft Azur, Google Cloud, IBM Cloud, Open Telekom Cloud) have obtained the relevant certification.[5]

At EU level, the EU Data Act (VO (EU) 2023/2854, "**Data Act**") is of particular relevance for CSPs as well. One of the main aims of the Data Act is to facilitate seamless (and ultimately free of charge) switching between different CSPs in order to promote competition while preventing vendor lock-in. The relevant provisions of the Data Act (Chapter VI, Art. 23 to 31 Data Act) specifically target the removal of obstacles faced by customers wishing to switch providers and to facilitate the transition from one CSP to another. Additionally, the Data Act stipulates detailed contracting requirements, obliging CSPs to include specific contractual terms related to switching (Art. 25 Data Act) and additional information/transparency obligations towards the customers (Art. 26, 28 Data Act).

Furthermore, the EU Data Protection Code of Conduct for Cloud Service Providers[6] is a (voluntary) transnational code of conduct endorsed by the EDPB (European Data Protection Board). It provides explicit guidance for CSPs to incorporate the obligations specified in the GDPR.

In 2023 the EDPR published a report focusing on the use of cloud-based services by the public sector, which also includes recommendations for public sector organisations when using cloud-based products or services.[7]

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions are widely adopted in Germany. According to the Bitkom Cloud Report 2023,[8] in 2023, 89 per cent of German companies with 20 or more employees were using cloud computing services (compared to 76 per cent in 2019 and 54 per cent in 2015). Additionally, 8 per cent were planning or discussing the possibility of using cloud services, which illustrates a clear trend towards increased cloud adoption among German businesses.

The most commonly cited reasons for using cloud services were:

a) cost reduction;
b) reduction of CO_2 emissions;
c) switching to platforms and SaaS in general; and
d) IT security.

9.3 What are the key legal issues to consider when procuring cloud computing services?

When procuring cloud computing services in Germany, the following key legal issues in particular should be considered:

a) **General contract law**: In the area of general contract law, the strict rules under the German law on T&Cs, which apply to a large extent even in business-to-business (B2B) relationships, come into play when dealing with standardised contracts offered by CSPs. German courts qualify cloud services contracts largely as lease contracts, with the consequence that the statutory regime for lease contracts, in particular statutory warranties, applies. Particular attention should be paid to provisions relating to service continuity and termination scenarios, including portability of data and migration assistance, as well as to liability for non-availability or loss of data.
b) **Data protection law**: In the area of data protection, the GDPR and BDSG) will be of major importance if personal data is processed by a CSP, in particular where data is accessed from or otherwise transferred to outside the EEA.
c) **Sector-specific regulations and authority guidance**: Depending on the nature of the business, additional industry-specific legislation and authority guidance may apply. Please refer to question 7.1 above.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

As of now, there are no specific national laws or regulations in Germany that regulate the procurement or use of AI-based solutions or technologies.

However, AI falls under the general regulatory framework that applies to all digital and automated decision-making technologies. This includes data protection laws, such as the GDPR and the BDSG, both of which contain provisions that are relevant to AI, such as specifying requirements for automated decision-making (Art. 22 GDPR, Section 54 BDSG).

At EU level, the forthcoming Artificial Intelligence Act, adopted in April 2024 ("**AI Act**") will be fully applicable in Germany when in force. As a reminder, the AI Act classifies AI systems based on risk:

a) **Unacceptable Risk**: Certain AI systems (e.g., social scoring and manipulative AI) are prohibited.
b) **High-Risk AI**: Most of the text focuses on high-risk AI systems, which are regulated. Developers and deployers of high-risk AI systems have significant obligations.
c) **Limited Risk AI**: A smaller section addresses limited risk AI systems (e.g., chatbots and deepfakes), subject to lighter transparency requirements.
d) **Minimal Risk AI**: Unregulated (including many existing AI applications on the EU market, such as AI-enabled video games and spam filters).

Notably, the users of high-risk systems must carry out and document a risk assessment, provide relevant information to the persons interacting with the AI system (capabilities, limitations, potential impact), monitor the behaviour and performance of the

AI system and provide adequate incident reporting to competent authorities, maintain human oversight over the system, etc.

The European Commission also published a Proposal for an Artificial Intelligence Liability Directive ("**AILD**") in September 2022. The purpose of the AILD is to lay down uniform rules for certain aspects of non-contractual civil liability for damages caused with the involvement of AI systems. It also addresses specific difficulties of proof linked with AI in order to ensure that justified claims are not hindered.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

In Germany, as in many other jurisdictions, data per se cannot be "owned" as data is not considered a physical object in which ownership is legally possible (Section 90 BGB).

However, training data can be protected and controlled through other legal concepts such as data protection, trade secrets and copyright laws. On a copyright law level, e.g., Sections 44b, 60d German Copyright Act ("**UrhG**") set out the prerequisites under which data mining is permitted, and Sections 87a *et seq.* stipulate the *sui generis* rights of database producers.

Whether protected by IP rights, trade secrets or only by contractual restrictions, data can be licensed or made available on a contractual basis.

It should be noted that the EU Data Act (VO (EU) 2023/2854) that will come into force in September 2025 will allow the legitimate users of connected equipment to access any data collected or generated by such equipment and require the holders of such data (e.g., the manufacturer or seller) to make such data available in a readable and accessible format. Users may also request that data holders share such data with third parties specifically designated by them.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

In light of the increasing use of generative AI, questions around IP ownership in machine-generated content are currently highly debated.

The position and starting point under German copyright law, as well as under German patent law is that a human creation, respectively invention, is a necessary requirement for protection, respectively patentability. Accordingly, purely machine-generated developments are generally not protected. However, in particular in relation to only partly machine-generated content, improvements or mere corrections of pre-existing works, there is a lot of debate as to the level and nature of human trigger activity required and sufficient to achieve protection and applicable thresholds for protection.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

The procurement of blockchain-based solutions is not directly regulated by specific laws or regulations in Germany. It will, however, be – like any technology procurement – subject to general procurement rules (please see our response to the questions in Section 1 above for further details).

The blockchain technology itself – if used for financial transactions – would be subject to the general regulations and laws concerning financial transactions (such as, e.g., the German Act on the Introduction of Electronic Securities (*Gesetz zur Einführung von elektronischen Wertpapieren* ("**eWpG**") and – more generally – the KWG, the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz* ("**ZAG**")), the German Securities Trading Act (*Wertpapierhandelsgesetz* ("**WpHG**"), the German Money Laundering Act (*Geldwäschegesetz*, "**GwG**", and the German Crypto Asset Transfer Regulation (*Kryptowertetransferverordnung*, "**KryptoWTransferV**")).

At an EU level, the blockchain technology would in particular be subject to the Regulation on Markets in Crypto Assets (Regulation (EU) 2023/1114, "**MiCAR**").

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain technology is becoming increasingly prevalent, or at the very least, being explored in various sectors in Germany, including:

a) **Financial Services**: Financial institutions are using blockchain for a variety of applications, including digital currencies, crypto-trading, cross-border payments, and securities settlement. Notably, Deutsche Bank is among the German banks actively exploring these technologies.
b) **Energy**: Blockchain is seen as a means to optimise the distribution of (in particular renewable) energy resources, such as by means of automated energy trading.
c) **Supply Chain**: Blockchain is being used to increase transparency and traceability in supply chains.
d) **Automotive**: German automobile manufacturers, including BMW and Volkswagen, have announced their intent to increasingly use blockchain technology for their solutions.
e) **Healthcare**: In the German healthcare sector, blockchain technology is being explored, particularly for secure storage, exchange of patient records, and consent management.
f) **Public Sector**: In the German healthcare sector, blockchain technology is being explored, particularly for secure storage, exchange of patient records, and consent management (for example in relation to the establishment of so-called "Self-Sovereign-Identities").

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

The key legal issues when procuring blockchain-based technology will vary according to the specific nature of each project (in addition to those arising in connection with any procurement of technology products and services in general). They will usually include the following:

a) **Regulatory Framework**: Depending on the specific nature of the project, blockchain-based technology may need to comply with sector specific regulations. For example, blockchain applications in the financial services sector may need to comply with securities laws, anti-money laundering regulations (including know-your-customer requirements) (see also our response to question 11.1 above). They may also require a licence by the German regulator (Federal Financial Supervisory Authority, *BaFin*).
b) **Data Protection** (usually one of the key challenges with blockchain-based technology due to its decentralised systems and immutable ledgers).

c) **Smart Contracts**: Smart contracts (i.e., implementation, development, audit, evolutions), as well as their legal effects (i.e., creation, termination, transfer of rights between parties, etc.) should be clearly defined.

d) **Liability**: The procurement contract should clearly define responsibilities and liabilities in the light of the decentralised nature of blockchain systems.

e) **Dispute Resolution/Jurisdiction**: Given the decentralised aspect and potentially large geographical footprint of blockchains, as well as the wide variety of geographical locations of the stakeholders, including users, the provisions in terms of dispute management, law and competent jurisdictions must be specified.

Endnotes

1 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html

2 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2018/rs_18_10_vait_va.html;jsessionid=534C7A4A595187E400F9FA0B46589953.internet002

3 https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1702_mago_va_en.html

4 https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

5 https://www.wik.org/fileadmin/files/_migrated/news_files/WIK_Report_AP1.pdf

6 https://www.edpb.europa.eu/system/files/2024-02/eucloudcoc.pdf

7 https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

8 Cloud-Report (https://www.bitkom.org)

Dr Henriette Picot is a partner in Bird & Bird's international Technology and Communications Group. She advises international and domestic suppliers and customers of software, hardware and innovative services in the planning and negotiating of technology-based or data-driven national and international projects and transactions, as well as in the development of innovative, often data driven business models.
She has longstanding experience advising clients on legal challenges around developing, licensing and distributing software, outsourcing and managed services transactions, cloud computing and software as a service, data analytics, open source software, digitisation projects, ecommerce and m-commerce, IT in M&A transactions, data privacy and data security. She represents clients in IT and data related disputes.

Bird & Bird LLP
Maximiliansplatz 22
80333 München
Germany

Tel: +49 89 3581 6239
Email: Henriette.Picot@twobirds.com
LinkedIn: www.linkedin.com/in/henriette-picot-1b180ba8

Michaela von Voß, as a member of Bird & Bird's international Tech & Comms Group, supports national and international clients on all aspects of IT and communications law and digitalisation related matters.
The focus of her work includes advising suppliers and users of software, hardware and IT services in the preparation, negotiation and implementation of technology-based projects, the distribution, licensing and development of software, cloud computing and software-as-a-service, outsourcing and managed services agreements, as well as IT law issues in M&A transactions.

Bird & Bird LLP
Maximiliansplatz 22
80333 München
Germany

Tel: +49 89 3581 6135
Email: Michaela.von.Voss@twobirds.com
LinkedIn: www.linkedin.com/in/michaela-von-voss-a1a0ab31

Dr Rolf Schmich is a partner in Bird & Bird's Frankfurt office. He has been advising on German and international tax law for over 20 years. His specialisation is in transaction-related tax advice (M&A, reorganisations, financing, inbound structures), in tax compliance matters related to Cum/Ex- and Cum/Cum-transactions as well as in corporate and reorganisation tax law. Rolf Schmich also represents clients in tax audits and tax disputes with the tax authorities, and before the tax courts.

Bird & Bird LLP
Marienstraße 15
60329 Frankfurt am Main
Germany

Tel: +49 69 7422 26 700
Email: rolf.schmich@twobirds.com
LinkedIn: www.linkedin.com/in/dr-rolf-schmich-294a67117

Vincent Kirsch, as a member of Bird & Bird's International HR Service Group, advises national and international employers on all legal aspects of individual and collective employment law.
His practice covers the entire spectrum of day-to-day HR questions as well as guidance on complex restructuring measures and corporate transactions. In particular, Vincent drafts all kinds of customised employment law documents, such as employment and managing director service agreements, termination agreements, as well as the required documents for the transfer of employees in the course of transactions. In addition, he advises on all aspects of collective bargaining agreements, as well as in the area of co-determination and dealing with works councils.

Bird & Bird LLP
Am Sandtorkai 50
20457 Hamburg
Germany

Tel: +49 40 460 63 6000
Email: vincent.kirsch@twobirds.com
LinkedIn: www.linkedin.com/in/vincent-kirsch-910793209

Bird & Bird has more than 1,600 lawyers in 31 offices across Europe, the Middle East, Asia-Pacific and North America and clients based in 118 countries worldwide. We specialise in combining leading expertise across a full range of legal services and aim to deliver tailored local advice and seamless cross-border services.
Our technology sourcing practice is widely recognised as having a leading reputation in the field and enjoys top tier international rankings in *The Legal 500* and *Chambers* Guides to the legal profession. We advise on the full range of technology transactions, including complex outsourcings and managed services deals, system implementation projects, telecoms infrastructure and regulatory matters, strategic alliances and collaboration agreements, cloud computing deals and contracts for the deployment of AI and blockchain-based solutions.

www.twobirds.com

Bird & Bird

Greece


Konstantinos Vouterakos


Elisabeth Eleftheriades


Dr. Victoria Mertikopoulou


Constantinos Kavadellas

Kyriakides Georgopoulos (KG) Law

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, procurement by private sector entities is not subject to regulation in Greece.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The procurement of works, supplies or services by contracting authorities through a public contract is regulated by: (a) Law 4412/2016 on public procurement of works, supplies and services, as amended and in force (adaptation to the Directives (EU) 2014/24 and 2014/25); (b) the contract notice provisions, as well as the terms of the contract; and (c) the provisions of the Greek Civil Code (hereafter "GCC"), which are applied in a supplementary way. Contracting authorities may be the State, local authorities, entities governed by public law, etc. According to this legislation, the general rules applicable to public procurement procedures, such as the equal treatment of the economic operators, transparency, etc. are set. The same Law 4412/2016 also regulates the procedures to be followed when awarding a public contract, including the awarding criteria, the grounds for exclusion of economic operators from public contracts, and the specific characteristics related to the performance of a contract, depending on the nature of the contract and whether it is a works, services or supplies contract.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

Public law: The duration of the contract is set in the relevant contract documents (in specific in the contract notice and/or in the relevant agreement). With respect to framework contracts, the law provides for a duration up to four years.

Additionally, in public procurement procedures for the supply of goods and for the provision of general services, tenders are valid and binding for economic operators for a period specified in the contract documents, which may not exceed 12 months from the closing date for the submission of tenders (Art. 97 para. 4 of Law 4412/2016, as amended and in force). Such duration might, however, be extended under the terms and conditions set in the above provision of Art. 97(4) of Law 4412/2016.

Private law: Regarding the private sector, there is no such provision under Greek law. As a general note, the duration of an agreement for the supply of goods can be freely determined by the parties.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

Public law: Contracting authorities may unilaterally terminate a public contract during its performance (Art. 133 of Law 4412/2016, as amended and in force) in cases where:

(a) the contract has been substantially modified, in a way that would require a new procurement procedure;
(b) the contractor, at the time of the award of the contract, fell into one of the grounds for exclusion and should therefore have been excluded from the procurement procedure; or
(c) the contract should not have been awarded to the contractor due to a serious breach of its obligations under the Treaties and Directive (EU) 2014/24.

The above general provision does not provide for a notification obligation from the customer's side.

However, under Art. 203 (4) of Law 4412/2016, the contracting authority serves the contractor a notification asking them to comply with their obligations and setting a time limit (not less than 15 days) for such compliance. If the deadline set by the special notice lapses idle, the contractor shall be declared as disqualified within a period of 30 days from the idle lapse of the compliance deadline.

Private law: In general, notice of termination of contracts under Greek law is not subject to a certain time limit, and the parties are allowed to freely determine the time limit for giving such notice. It is also possible to terminate a contract for good cause at any time and without notice. However, there are certain types of contracts, such as trade agency contracts, for which a period for termination is provided under specific acts.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Public law: Generally, pursuant to the provisions of GCC, which as already advised are supplementary applied, the principles of good faith and marketable quality play a significant role to the interpretation of the contracts and the fulfilment of the obligations of the contract, as well as to the execution of any right (Arts 178, 179, 200, and 288). According to Art. 18, para. 1 of Law 4412/2016, as amended and in force, contracting authorities must treat economic operators equally and without discrimination, and must act in a transparent manner, respecting the principles of proportionality, mutual recognition, protection of the public interest, protection of the rights of individuals, protection of competition, and protection of the environment and sustainable development.

Private law: As regards all contracts concluded between legal entities and/or individuals, the parties have a duty of good faith and fair dealings. These principles underpin Greek law and their scope has been further elaborated by case law. Any conduct of a party that deviates from good faith and fair dealings, besides constituting a breach of the contractual obligations, also constitutes unlawful conduct, which entitles the injured party to claim compensation for the damage caused by the breach.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The following remedies are available.

Public law:
- Compensation for pre-contract negotiations (Arts 197, 198 of the Civil Code).
- Right of unilateral termination of the contract (Art. 133 of Law 4412/2016, as amended and in force).
- Penalty clauses in public services contracts (Arts 148 and 218 of Law 4412/2016, as amended and in force).
- Right of exclusion of the economic operator from the competition in question, as well as from future competitions (Art. 73 para. 4 subpara. f, Art. 74 para. 1 of Law 4412/2016, as amended and in force).
- Penalties for late delivery of supply (Art. 207 of Law 4412/2016, as amended and in force).
- Penalties for rejection of contractual materials including the replacement of such materials (Art. 213 of Law 4412/2016, as amended and in force).
- Disqualification of the economic operator (Art.203 of Law 4412/2016 as amended and in force).

Private law:
- Termination.
- Actual and moral damages.
- Price reduction, if the breach relates to defects or the product not meeting the agreed specification. The product may also need to be replaced.

The limitation period for claims arising between traders is five years from the date of their accrual. Claims arising from the sale of goods are subject to a limitation period of two years.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Public law: In addition to the above remedies, if the contractor is declared to be disqualified, the following sanctions may be imposed (Art. 203(4) of Law 4412/2016):

(a) the guarantee will be forfeited in full;
(b) the advance payment will be collected and any interest due must be paid; and
(c) the contractor must pay the difference between the new award price for the delivery of the goods by a new contractor and the initial award price, multiplied by a factor of between 1.01 and 1.05.

Also, the customer may withhold payment.

Beyond all this, the customer can seek compensation for any further actual damages.

Private law: In addition to the remedies available at law, the customer could seek the following protections:
- provision of credit for the payment;
- inspection of the product upon delivery and immediate replacement of defective products or products lacking the agreed properties;
- confirmation that the customer is liable for accidental destruction or defects of the product only after the product has been delivered;
- if the defect is not due to the customer's behaviour, repair of the product by experts suggested and verified by the supplier in case of defects, within a certain period of time, or replacement of the product if repair is not possible;
- termination of the contract in the event that the supplier is declared bankrupt, forced into compulsory administration or liquidation;
- the option to become a guarantor of the products already purchased until the payment so that they do not form part of the bankruptcy estate in the event that they have been sold with retention of title;
- the submission of a letter of guarantee (issued by a credit institute) and in addition the submission of a parental company letter of guarantee; and
- punitive damages for failure to execute the contract or the continuous supply of defective goods.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Public law: The contractor can terminate a contract in cases of *force majeure*. In this case, the contractor is obliged to report in writing to the customer and to provide the customer with the necessary evidence of the events constituting *force majeure* within 20 days of their occurrence (Art. 204 of Law 4412/2016, as amended and in force). In view of the above, contractual parties cannot be held liable for breaches of contract that resulted from events of *force majeure*.

Private law: The parties are free to agree on the terms of the contract; the breach of such terms will justify the termination of the contract. Claims by the other party for damages are not justified if termination of the contract is in line with the causes set out in the contract, provided that the period of notice has been met (if any). In addition, the parties may terminate the contract immediately for good cause. Such good cause may be, in line with case law, the party's permanent inability to fulfil its contractual

obligations, the seizure of its assets resulting in the impossibility of performing its contractual obligations, an unforeseen change of conditions which renders the performance of the contract as such impossible, *force majeure*, etc. In such circumstances, claims for compensation cannot be successfully pursued.

2.7 Can the parties exclude or agree additional termination rights?

Public law: The parties are free to agree on additional termination rights, but they cannot exclude the ones provided for in the relevant legislation. In practice, the parties always follow the statutory provisions.

Private law: Under Greek law, in principle, contractual freedom allows the parties to either exclude or agree additional termination rights. However, a party cannot be excluded from terminating the contract when one of the above indicative good reasons applies, nor can an excessive or extremely limited period be set for exercising the right.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Public law: In principle, any limitations on liability cannot limit the implementation of the provisions of Law 4412/2016, as amended and in force, and the relevant contract notice provisions, with relation to damages, penalty clauses and sanctions. In any case, the terms agreed in a contract must also be in accordance with good faith, otherwise they may be considered null and void.

Private law: Under Greek law, the contracting parties of an agreement are allowed to limit the liability in advance by virtue of a contractual provision, but only up to a certain degree. Greek law does not recognise such a limitation where there has been wilful misconduct or gross negligence. Therefore, under Greek law it is only possible to validly agree upon the exclusion or limitation of liability arising out of simple negligence. Where there is liability established on wilful misconduct or gross negligence, there is no limit to the damages that can be awarded. Apart from the above, any limitation of liability must conform with the general principles of *bona mores*, as well as the requirements of good faith. In view of this, any clauses that excessively limit the liability of the party in the strongest bargaining position are likely to be judged as abusive and, consequently, null and void. In view of this, all clauses relating to the limitation of liability must be restrictively construed as to their scope of application. It is, however, possible to validly exclude or limit liability for all types of liability following the occurrence of the event giving rise to liability by means of a subsequent agreement between the parties, (e.g., by way of a settlement agreement).

Regarding the sale of goods, a limitation period shorter than the two years set out in the law is not valid.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Public law: There is no statutory financial cap on liability. The parties do not agree on a financial cap, because it is not possible for the cap to be less than the actual damages.

Private law: If liability is established on the basis of wilful misconduct or gross negligence, there is no limit to the damages awarded and the parties to a contract cannot impose a cap on total liability. However, the parties are free to agree a financial cap on their respective liabilities under the contract in cases where liability arises out of simple negligence.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, the same principles generally apply across all these types of technology procurement contract.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Public law: The main dispute resolution methods are judicial and administrative. Depending on the type of contract, a clause for the arbitration of disputes may also be included in the contract documents. More specifically, any dispute between the contracting parties shall be settled by bringing an action or claim before the Administrative Court of Appeal of the Region in which the contract is being executed (Art. 205A, 175 of Law 4412/2016, as amended and in force). Before an appeal can be brought before the Administrative Court of Appeal, a preliminary administrative procedure must be followed in accordance with Art. 205 of Law 4412/2016, as amended and in force.

In addition, the contract may include provisions that stipulate parties must attempt to settle a dispute before seeking relief.

Private law: The main methods of dispute resolution used in contracts are:

- The (extrajudicial) resolution of disputes by negotiation between the parties, allowed without restriction. Such negotiation may take place at any time.
- Non-mandatory mediation. Such mediation takes place before a certified mediator at the joint request of the parties or at the proposal of one of the parties. The parties may elect the mediator themselves, otherwise the mediator will be appointed by the Central Mediation Committee.

Judicial resolution of the dispute, by filing an action in the Court of First Instance of the place in which the contract was signed or in which the defendant is domiciled.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

Background IP: By virtue of the corresponding agreement definitions and clauses, pre-existing IP rights belonging to each party are laid out/defined, further determining whether and, in the affirmative, which rights of each party the other party can make use of, and to what extent.

Foreground IP: In case of the creation/development of new IP rights, the agreement should contain relevant clauses in relation to the ownership and, in certain cases, the licensed use by the licensee.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

By virtue of the respective applicable mandatory Greek law legal provisions, any transfer and assignment and any licensing IP rights should be in writing. In relation to IP rights, the registration of which is recorded in a public register (such as trademarks, patents, designs, utility models), the inter-partes force and validity of the transfer of such rights and the assignment and/or licence – always by virtue of a written agreement – is not affected by the non-recordal of the latter in the public register; however, the force and validity of a transfer and assignment and/or licence *vis-à-vis* third parties can be claimed only if it has been recorded in the public register. It is therefore advisable to record such rights.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

In transposition of Directive (EU) 2016/943 of the EU Parliament and the EU Council and by virtue of Article 1 of Law 4605/2019, articles 22A to 22K were added to Law 1733/1987 (on technology transfer, inventions and technological innovation), on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure.

Confidential information is usually the subject of an agreement between the parties.

Clauses regarding trade secrets and confidentiality include, *inter alia*, definitions on what constitutes confidential information and trade secrets, the duration of the obligation to maintain the confidentiality of the information (depending on the type and importance of the information, the obligation to maintain confidentiality indefinitely is recommended – this should always be the case for trade secrets) and on the use and the extent of its use by the parties.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

The legal and regulatory framework on data protection applies also with regard to data processing when providing technology services. Key data processing obligations laid down by the GDPR and GDPR Greek implementing law (Law 4624/2019) are the obligation to enter into data processing agreements, to adopt adequate technical and organisational measures and to provide notices to data subjects.

It should be noted that specific rules are in place in relation to the confidentiality of electronic communications and telecommunications, including the processing of traffic and location data, and information security requirements are imposed upon certain technology providers (see question 5.3).

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Personal data can be transferred outside Greece; however, restrictions are established under Chapter 5 of the GDPR in relation to the transfer of personal data outside the European Economic Area. In particular, cross-border data transfers are allowed only to countries for which an adequacy decision has been issued by the European Commission, or if one of the safeguards or the derogations of the GDPR applies in the relevant case.

It should be noted that there are no national specific rules restricting data transfers other than those mentioned above.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The European Union has adopted the Cybersecurity Act and the sectoral Digital Operational Resilience Act ("DORA") for the financial sector, which are directly applicable in Greece. The key points of the Cybersecurity Act are the following:

- Strengthened mandate for European Union Agency for Cybersecurity ("ENISA").
- Establishment of an EU Cybersecurity Certification Framework.
- Designation of national cybersecurity certification authorities.

The DORA sets forth uniform criteria for the security of network and information systems essential for the operational functions of financial institutions.

In addition, requirements concerning information security for operators of essential services and digital service providers are set out in Law 4557/2018, which transposes the Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive) into the Greek legal system. Said obligations aim at ensuring a high security level of networks and information and include, among others: (i) the obligation to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems used and to prevent and minimise the impact of security incidents; and (ii) the obligation to notify the National Cybersecurity Authority or the competent CSIRT without undue delay of incidents that have a substantial impact on the provision of its service. The level of security for networks and information systems is expected to increase with the transposition of Directive (EU) 2022/2555 (NIS 2 Directive) by Member States by 17 October 2024, which will replace the current NIS Directive as of 18 October 2024. The NIS 2 Directive provides for the expansion of the scope of the cybersecurity rules to new sectors and entities (and not only operators of essential services and digital service providers), the strengthening of security requirements, and the introduction of more stringent supervisory measures and stricter enforcement requirements. Further, the Cyber Resilience Act (European Commission's proposal) will impose horizontal cybersecurity requirements within the European internal market for hardware and software products with digital elements, while the Critical Entities Resilience Directive ("CERD") mandates critical entities to identify vulnerabilities, develop resilience plans, and collaborate with stakeholders to mitigate risks and enhance continuity and preparedness in vital sectors.

Moreover, Art. 26 of Law 5002/2022 ("Waiving of Communications Secrecy, Cybersecurity, and Data Protection") provides for all public sector bodies, and in particular the

prosecuting authorities, the Hellenic Data Protection Authority, the Hellenic Authority for Communication Security and Privacy, and the Hellenic Telecommunications and Post Commission, that they must inform without delay the General Directorate of Cybersecurity of the General Secretariat of Telecommunications and Post of the Ministry of Digital Governance, the Cyber Defence Directorate of the General Staff of National Defence (designated as the competent Response Team for Computer Security Incidents "CSIRT"), the Cyberspace Directorate of the National Intelligence Service as the National Cyber Attack Response Team (National CERT) and the Hellenic Police as soon as they receive any information about a cyber-attack which is either in progress or which has already taken place. In addition, the aforementioned bodies may request from public authorities and other public and private sector bodies, as well as from private persons, any information, document or evidence, and the latter must respond within 24 hours. Art. 28 thereof also states that the National Cybersecurity Authority (NCA) and the Cyberspace Directorate of the National Intelligence Service (EYP) shall monitor the threats and vulnerabilities of information and communication systems, issue security alerts and recommendations, and provide relevant information to the bodies concerned.

In addition, the following information security requirements are imposed upon electronic communications service/network providers (PECS/PECN):

- Other than GDPR-related security obligations, PECS/PECN providers are under an obligation as per Art. 148, 149 of Law 4727/2020 ("Digital Governance (Transposition to the Greek Legislation of Directive (EE) 2016/2102 and the Directive (EE) 2019/1024)) – Electronic Communications (Transposition to the Greek Law of Directive (EE) 2018/1972) and other provisions") to take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. These measures are defined in the Hellenic Authority for Communication Security and Privacy newly-issued Regulation on the Security of Electronic Communications Networks and Services (Decision No. 28/2024), which repealed the Regulation for the Assurance of Confidentiality in Electronic Communications and the Regulation on the Security and Integrity of Electronic Communications Networks and Services. Having regard to the state of the art, those measures should ensure a level of security appropriate to the risk presented. In particular, measures such as encryption must be taken to prevent and minimise the impact of security incidents on users and on other networks and services. In this respect, it is explicitly provided that PECS must, *inter alia*, adopt a security policy in order to protect the security of services and of the network.
- PECS/PECN are required to take appropriate technical and organisational measures to protect data retained for the purpose of criminal investigation. To that effect, they must draft and implement a specific Security Policy Plan. They must also appoint an Officer responsible for Security of the Data Retention System (i.e., the system on which data retained for the purpose of criminal investigation, detection and prosecution of certain serious crimes are kept), to whom monitoring of the implementation of the dedicated security policy, which aims to ensure security of aforementioned types of data, is assigned. Finally, they must implement measures such as logical separation of data, encryption and access control (Law 3917/2011).
- Under Art. 12 par. 5 of Law 3471/2006, in the event of a personal data breach related to electronic communications services, PECS/PECN providers shall notify without undue delay the Hellenic Authority for Communication Security and Privacy ("ADAE") and the Hellenic Data Protection Authority ("HDPA") and disclose a description of the nature of the personal data breach, the points of contact from which more information can be obtained, the consequences of the personal data breach and the measures proposed or implemented by the entity to address the breach.
- Pursuant to Art. 24 of Law 4961/2022, additional requirements are imposed on PECS/PECN providers, who must develop and annually update a risk assessment plan, taking into account the reliability of suppliers in terms of the confidentiality, integrity and availability of their networks, their supply capacity in terms of products and services, and the overall quality thereof. Further, these providers must establish a procurement plan for all equipment and third-party suppliers involved, which must include any technical security and risk management measures taken, as well as a detailed description of supplies. Moreover, under Art. 85 of Law 4727/2020 as recently amended by Art. 74 of Law 4961/2022, each information systems of public sector entities hosted in the three governmental clouds described in Art. 87 (i.e. G-Cloud, RE-Cloud and H-Cloud), must be accompanied by a data classification study carried out by the competent cloud management entities.

Further, similarly to aforementioned obligation, Arts 18 to 20 of Law 4961/2022 "Emerging information and communication technologies, strengthening digital governance and other provisions", provide for the obligation of Central Government Bodies to appoint an Information and Communication Systems Security Officer who monitors the information security and resilience of the entity and manages its risk analysis plan, as well as to establish and maintain a uniform information and communication systems security policy. Said Law also imposes on Central Government Bodies an obligation to appoint an IT officer as a Security Coordinator for critical digital infrastructure providers (Arts 21–22), to establish an online Registry of DPOs (Art. 25), and a data protection committee for the coordination of DPO activities (Arts 26–27).

Part B, Chapter C of Law 4961/2022 lays down Cybersecurity measures for Internet of Things (IoT) technology devices and related obligations applying to manufacturers, importers and distributors and operators. The National Cybersecurity Authority is the competent authority to monitor the implementation of the abovementioned IoT security framework.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

In Greece, the outsourcing of services does not necessarily result in a transfer of undertaking (TUPE application). The determination of whether an outsourcing arrangement constitutes a transfer of undertaking requires an assessment of the facts of the specific case. More specifically, an outsourcing arrangement might trigger the application of the TUPE rules, for example when an organised grouping of resources which has the objective of pursuing an economic activity is transferred to an external provider.

In practice, the assessment of whether a specific business transaction constitutes a transfer of undertaking, and therefore

triggers the application of the Greek TUPE provisions, depends on various factors that should be examined each time. Such factors include, *inter alia*:

(a) the type of the business to be transferred;
(b) whether or not any tangible assets will be transferred to the transferee;
(c) the intangible assets of the business to be transferred and the value of the same;
(d) whether the employees dedicated to the business will also be transferred to the transferee; and
(e) the degree of similarity between the activities carried on before and after the transfer.

In addition to the above, in case the transferred services constitute an autonomous business unit (i.e., 'an organised grouping with a view to carrying out an economic activity – whether this activity is essential or ancillary', as described above), which will retain its identity and will be continued by the transferee, the Greek TUPE rules will usually apply.

However, the applicability of the Greek TUPE provisions is considered unlikely when there is no transfer of any asset whatsoever (tangible or intangible), and therefore no transfer of an autonomous business unit will take place.

6.2 What employee information should the parties provide to each other?

In case of a transfer of undertaking, the employment agreements of the affected employees are automatically transferred to the new employer (transferee) and the latter undertakes all rights and obligations of the existing employment agreements at the date of the realisation of the transfer (i.e., indefinite term employment contracts, fixed term contracts, part time contracts, contracts of lending of services of employees, etc.), without the obligation to sign new employment agreements.

In case of a business transfer, both employers have an obligation to inform employee representatives (trade union/works council) in writing regarding the exact or the eventual date of the transfer, the reasons of the transfer, the legal, financial, and social consequences of the transfer as far as the employees are concerned, and the measures to be taken regarding the employees (if any). There is no specific time schedule regarding the information process to be followed. In practice, a period of 20 days prior to the actual transfer (closing) is generally considered as reasonable for the information process.

In the absence of employee representation (i.e., when there are no trade unions or works councils in the company), all affected employees need to be informed, individually and in writing, regarding the above.

Consultation with the employee representatives is required only if there will be changes to the employees' employment terms and conditions. The results of said consultation are drafted in minutes, which can either be an agreement or the final position of the two parties involved. Depending on the extent of the measures to be taken, the relative period needs to be readjusted (i.e., 20 days prior to the transfer might be sufficient or not sufficient for the same).

If no changes will be made to employees' terms of employment, no consultation obligation exists (only obligations regarding information).

Therefore, the transferor must provide details to the transferee regarding the above points.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

In case of a business transfer, the law prohibits the implementation of dismissals when the cause of the dismissal is the transfer itself, but also provides for an exception for dismissals that need to take place for technical, financial, and organisational reasons, under the condition, though, that Greek employment law is not violated.

This means, for example, that the transferee may proceed to terminations due to reorganisation (e.g., if it wants to abolish a specific department completely, or because there is more than one employee covering the same position, etc.). On the other hand, the transferor cannot validly dismiss the employees solely because the transferee wants to hire only some of them, and the transferee cannot validly dismiss personnel just because there are a lot of employees.

Such prohibition on dismissing employees because of the actual transfer concerns both the transferor and the transferee. In practice, however, greater importance is placed on terminations before the transfer.

In any case, Greek courts examine the condition of each reorganisation procedure meticulously to ensure the correct application of the legal criteria that determine who will be dismissed first (i.e., an employee's performance, seniority, family status, possibility of finding a new job, etc.), the necessity of the dismissals in relation to other measures that could have been taken instead, etc.

Also, employees protected against dismissal (protected union officials, pregnant employees/new mothers/new fathers, forced hires, etc.) continue to be protected in the case of transfer and when a business is reorganised, such employees would be last to go, unless of course a significant reason exists which could justify the termination of their employment (for example, permanent abolition of their job position or department). It goes without saying that, regarding these employees, a thorough examination of the facts of the case needs to be realised to avoid or reduce the eventual risks. Additionally, specific documentation should be used, and specific procedures followed.

If no transfer exists, dismissal is allowed as long as the provisions of Greek law related to employee dismissal are followed.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

In case of a TUPE transfer, in practice, employers propose to the transferred employees the full or partial harmonisation of salaries and benefits in order to avoid administrating different categories of employees. This harmonisation process needs to be shared and discussed with the employees' representatives, but, given that they constitute mainly individual terms of employment, the consent of each and every employee needs to be granted. If all or some employees refuse the proposal of the transferee, then the latter will have to administrate the specific employees separately.

6.5 Are there any pensions considerations?

As per Greek TUPE provisions, an exception is made for pension schemes, where the new employer is entitled to either continue, amend or terminate the existing scheme following the

specific procedures provided by the law. Therefore, the new employer has three options:

(a) accept the insurance contract under the same terms and conditions;

(b) amend the existing pension plan, in which case the new employer should enter into negotiations with the employee representatives regarding the changes in order to reach an agreement; or

(c) decide not to continue the application of said plan. This must be declared before the transfer date, in which case it will be terminated and liquidated as per its own rules, i.e., each employee will receive what he/she is entitled to at the date of liquidation. In this latter case, neither the transferor (under the condition that it has fulfilled his obligations) nor the transferee will be liable regarding the terminated pension scheme.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

In case the offshore outsourcing meets the above criteria and is therefore characterised as a transfer of business (or business unit) on a local level, then the employees dedicated to the unit shall, by virtue of law, automatically be transferred to the third party (new employer).

Transfer to a company outside Greece, however, may be considered as a detrimental change to the employee's agreed terms of employment.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

The Bank of Greece issued Executive Committee Act no. 178/5/2.10.2020 adopting the guidelines of the European Banking Authority (EBA) on outsourcing arrangements (EBA/GL/2019/02). These guidelines also incorporate EBA recommendations on outsourcing to cloud service providers. The new Act abolishes the existing framework for outsourcing, laid down in Annex 1 to Bank of Greece Governor's Act 2577/9.3.2006.

The aim of the Act is to establish a harmonised framework for the outsourcing of functions by all the institutions supervised by the Bank of Greece. Its scope therefore encompasses not only credit institutions, but also financial institutions, including payment institutions and e-money institutions.

The new outsourcing framework provides a clear definition of outsourcing, as well as of critical or important functions. In addition, it includes specific internal governance requirements and obligations of institutions, both before entering into an outsourcing arrangement and during the term of the arrangement, with a view to the more effective management of the risks entailed by outsourcing. Stricter requirements apply to the outsourcing of critical or important functions, given the higher risk entailed.

Under the new framework, institutions are required to inform the Bank of Greece of their intended arrangements for the outsourcing of critical or important functions before they enter into any outsourcing agreement, but without the need for a relevant approval decision from the Bank of Greece, so as to facilitate and accelerate the outsourcing process. However, where it is judged that the relevant supervisory requirements are not met, the Bank of Greece may decide not to allow the outsourcing of functions, or may request the termination of any outsourcing agreement in force.

In order to ensure adequate and standardised information on outsourcing arrangements by all institutions, the new framework introduces the obligation for institutions to maintain a register of information on all outsourcing agreements, following the template provided in the Annex to the Act. Institutions must make this register available to the Bank of Greece upon request, as well as any other information necessary for the exercise of effective supervision.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

As there is no regulated outsourcing contract under Greek law, the legal and contractual types depend upon the respective outsourcing products and/or services. Therefore, contractual structure and details must be assessed on an individual level, mainly depending on scope, type and circumstances of the planned outsourcing. Due to the legal complexity of outsourcing contracts, the legal classification of the contract types often varies (such as service contract, rental contract, purchase contract and works contract). As a result, explicit contract tailoring is required. Taking the aforementioned into consideration, the most common types of legal or contractual structure used include the below alternatives:

- Direct outsourcing: The simplest outsourcing structure is a direct outsourcing between the customer and the supplier.
- Multi-sourcing: In a multi-sourcing, the customer enters into contracts with different suppliers for separate elements of its requirements.
- Indirect outsourcing: In an indirect outsourcing, the customer appoints a supplier (usually based in Greece) that immediately subcontracts to a different supplier (such subcontractors are usually based outside Greece).

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

When negotiating the contract, the parties usually try together to identify and agree a set of objective, measurable criteria to measure the supplier's performance (key performance indicators (KPIs) or service levels). These service levels need to be combined with:

- a process for recording and reporting on success or failure in achieving the targets; and
- a formula under which financial compensation is paid to the customer if targets are not met. These are referred to as service credits or liquidated damages.

The aim of service credits is to compensate the customer for poor service without the need to pursue a claim for damages or terminate the contract, and to motivate the supplier to meet the performance targets.

The supplier will want to ensure that the stated service credits are the sole remedy of the customer for the particular failure concerned, but this should be without prejudice to the customer's wider rights in relation to more serious breaches of the contract or persistent failures in performance. Service credits are generally enforceable, provided they are a genuine pre-estimate of the customer's loss or can be shown to protect a legitimate commercial interest of the customer and are not a contractual penalty.

For the sake of completeness, it is also noted that, pursuant to Art. 87 of Law 4727/2020 which refers to the government cloud, the competent management entities described therein are obliged to provide agreed service levels (SLAs) to any public sector bodies which are to install their central electronic applications and central information systems in the cloud. Moreover, as per the new addition of para. 9B to the aforementioned Art. 87, by virtue of Law 4961/2022 "Emerging information and communication technologies, strengthening digital governance and other provisions", for SLAs whose object concern electronic applications or IT systems within the competence of multiple public sector bodies, a prior act of approval is issued by the Council of Ministers upon recommendation of the Minister of Digital Governance.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Mostly a basic fee is combined with fees based on usage, also known as "compensation on a time basis". In such cases the works are billed at actual cost, on a *pro rata* basis of the works requested and the volumes dealt with. It is therefore not possible to know in advance the total cost of the outsourcing arrangement. Final costs can only be estimated.

Other alternative charging methods include:

- subscription models;
- cost plus, where the customer pays the supplier both the actual cost of providing the services and an agreed profit margin;
- a true fixed price in cases where there will be a regular and predictable volume and scope of services and the customer wants to have greater certainty over its budget; and
- flat-rate global price, i.e. the price is fixed and includes all the works agreed under the contract. If other works are then carried out, they will be charged additionally.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

The parties should carefully check the terms of such contracts at an early stage in order to ensure that they are able to assign the contract, and if so, if the counterparty's consent is required or not. If the counterparty's consent is required, they must confirm and attempt to obtain such consent if necessary.

Further to complying with assignment requirements and depending on the respective service and the contractual relationship, mainly data protection requirements under the GDPR must be fulfilled. In particular, in the case of a processor/sub-processor relationship, consent of controller for the use of the sub-processor must be obtained and a data protection agreement as per. Art.28 para. 4 GDPR is required.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

There are no specific Greek tax provisions applicable to outsourcing arrangements. Consequently, each outsourcing arrangement will be specific to its own particular facts and will raise different tax issues depending on the type of services being outsourced, the structure of the outsourced transaction and the nature of the parties involved.

In the context of outsourcing arrangements, depending on both the parties involved and the nature of the services/assets supplied, Greek VAT (24%) will usually be applicable.

Moreover, the disposal of assets and/or the supply of services will generate taxable business income subject to corporate income tax of 22% at the level of the supplier. At the level of the recipient entity, the general deductibility criteria should be fulfilled for the expenses occurring in the context of an outsourcing transaction, in order for said expenses to be deducted from the taxable income of the recipient entity. In particular, the deduction of expenses for tax purposes is subject to general conditions, notably: (i) the expenses should be incurred for the benefit of the taxpayer; (ii) they should correspond to real transactions that have been effected in line with the arm's length principle; and (iii) they should be recorded in the taxpayer's accounting books and should be evidenced by appropriate documentation.

In addition, if the parties involved are considered to be related entities for income tax purposes, any outsourcing transaction should be performed at arm's length and be properly documented/reported to the Greek tax authorities (if the relevant Greek TP reporting thresholds are met).

Last but not least, it should be noted that from an indirect tax point of view, if the assets that are transferred constitute a self-standing business from a business perspective, the transaction should be considered as transfer of business of going concern (TOGC) and should not be subject to VAT but instead to stamp duty at 2.4%. Stamp duty is imposed on the higher amount between the actual sales price and the net equity of the business segment transferred.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Some of the key contractual issues for customers to consider in relation to the above-described on-premise solutions are:

- responsibility of the vendor to deliver the product (software);
- the number of users allowed to use the software;
- intragroup use (companies within the same group may not be allowed to use the software unless they are expressly granted a licence as separate entities/users);
- third-party (customer's third-party service providers) access to the software;
- the geographical extent of the licence and/or geographical limitations related to accessing the software;
- license to reproduce/make copies of the software and relevant payment information;
- limits on the number of devices onto which the software can be uploaded;
- a description of the customer's needs and wording regarding modification of the software to meet such needs. Also, regulation of whether additional costs would be incurred and/or not, depending on the modifications and on when those modifications would take place;
- description of all open-source code (OSS) and tools with respective clauses on due use as per the OSS respective licences by the vendor;
- representations and warranties, and relevant indemnity clauses: adequate protection should be sought related to the performance of the software and/or on the infringement of third-party IP rights; and
- clauses/wording related to the vendor securing business continuity for the client in case of termination of the agreement.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Some of the key contractual key issues for customers to consider in relation to support and maintenance services installed on customer's systems are:

- whether the support will take place remotely and/or on site, or a combination of both;
- depending on the business and its needs, ensuring appropriate and accredited (if possible/applicable) level of provision of services;
- categorising the types of services and whether additional costs would be incurred (e.g., ensuring no additional support maintenance costs would be incurred for necessary updates and/or upgrades so as to secure due function of the software, including updates that secure compliance with applicable legal provisions);
- the total number of hours, the timeframe and the respective potential increase in cost depending on the time of provision of the service should be specified;
- matters related to access to commercially sensitive information and/or personal data and/or sensitive information should also be covered; and
- clauses/wording related to the vendor securing business continuity for the client in case of termination of the agreement.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Escrow agreements are still not very widely used in Greece; however, they are starting to be used all the more in transactions related to IT/software/technology development entities where source code and other related rights are involved. In some cases, public procurement-related contracts may provide for the execution of escrow agreements as a prerequisite. Current contractual practice mainly consists of including clauses in software licensing agreements about the delivery from the licensor to the licensee of the source code and any other relevant data and information in cases of liquidation, bankruptcy and/or other similar procedure of the licensor.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

Public law: For the procurement of cloud computing services, the abovementioned Law 4412/2016, as amended and in force, is applicable. The contract notice provisions, the terms of the contract and the provisions of the GCC are also in force and are applied in a supplementary way.

Law 4727/2020 includes a number of provisions relevant to cloud computing services. Specifically, Art. 87 provides for the following three government clouds: the Government Cloud of the Public Sector (G-Cloud); the Government Cloud of the Research and Education Sector (RE-Cloud); and the Governmental Cloud of the Health Sector (H-Cloud), managed by the General Secretariat for Public Administration Information Systems (Γ.Γ.Π.Σ.Δ.Δ.), the National Network of Infrastructures for Research and Technology (Ε.Δ.Υ.Τ.Ε. S.A) and the e-Government of Social Security (Η.ΔΙ.Κ.Α. S.A), respectively.

Pursuant to the recent Law 4961/2022 "Emerging information and communication technologies, strengthening digital governance and other provisions" para. 9A of Art. 87, each entity managing the aforementioned government clouds (i.e., G-Cloud, RE-Cloud and H-Cloud) may grant cloud infrastructure to another management entity, upon request of the latter, documenting the operational need for the concession. The concession is made by decision of the competent body of the Ministry of Digital Governance, which is issued the following:

(a) a recommendation of the entity granting the cloud infrastructure; and

(b) a recommendation of the public sector entity, as defined in point (a) of para. 1 of Art. 14 of Law 4270/2014 (A' 143), whose electronic applications or information systems are to be hosted in the infrastructure under concession.

As of the publication of the aforesaid decision, the above infrastructures shall be part of the government cloud managed by the entity applying for the concession.

As per Art. 85 of Law 4727/2020, the above three management entities procure cloud computing services as a priority for public sector bodies as a whole over any other technological solutions for the purpose of data storage, hosting of information systems and applications of public sector bodies, provision of cloud services to public sector bodies, the performance of their responsibilities, and the design and productive operation of technological infrastructures and information systems. Moreover, in order to promote the use of the Cloud by the Greek public administration, Art. 87 para. 8 stipulates that the Ministry of Digital Governance must design and implement a digital marketplace for Cloud services and applications in which public sector entities and Cloud service providers must register, posting in particular the Cloud services provided, technical details and procurement costs.

Moreover, by virtue of Art. 99 of Law 4961/2022 any public sector body acting as a contracting authority for the award of a public contract for the implementation of an ICT project to be installed in the G-Cloud, RE-Cloud or H-Cloud, is obliged to send to the competent government cloud management body, documented information on the resources required for the implementation of the project managed by the latter, before the publication of the contract notice or call for the expression of interest. The said information is effected via a specific application developed and operated by the Γ.Γ.Π.Σ.Δ.Δ, which, if it concerns RE-Cloud or H-Cloud, must then forward the said information to the respective competent management entity.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions have recently been adopted in the public sector in light of Greece's general efforts to integrate new digital technologies and ensure the interconnection and interoperability of Public Sector Systems. A number of regulatory reforms to increase the reliability and security of cloud critical infrastructures are further included in the country's Recovery and Resilience Plan.

In the private sector, cloud computing solutions have been widely adopted within the past few years, while private investments in cloud-based solutions and applications are steadily increasing.

Further expansion in the use of cloud computing services is expected also in light of the announcements made by Tech companies over the past two years regarding the upcoming creation of cloud regions and the construction of data centres in

Greece, which will allow organisations and businesses in Greece access to digital products and services and critical technologies such as AI and big data computing tools.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Public Law: The provisions of the Greek procurement framework (Law 4412/2016, as amended and in force) aim to serve the public interest and ensure a prevailing position of the contracting authorities/customer with respect to the conclusion and execution of the public contract. The aforementioned principles (public interest and the contracting authority's/customer's prevailing position) constitute fundamental doctrines governing the interpretation and implementation of Greek public tender law.

Contracting authorities shall treat economic operators equally and without discrimination and shall act in a transparent manner, respecting the principles of proportionality and freedom of competition. In addition, the relevant national and EU public procurement legal framework ensures the effectiveness of public procurement procedures and the proper financial management of the public resources allocated for this purpose.

Data Protection: The important issues that should be considered when procuring cloud computing services are:

- Data Privacy and Security (e.g. data breaches). Companies should engage with cloud service providers that would offer the highest level of privacy and security standards.
- Geographical location of the cloud providers' resources (in terms of data transfers). Specifically, customers need to confirm if their data is stored on servers located in countries that provide an adequate level of protection. Companies that use cloud service providers located outside the European Economic Area must make sure that requirements laid down in Chapter V of the GDPR are met and they must enter into adequate Data Processing Agreements with them.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

AI is recognised as one of the key points of Greece's Digital Strategy for 2020–2025, which includes the country's conditions for the development and use of AI-based technologies. Greece is now taking the final steps in developing a National Strategy for the utilisation of AI and working on issues related to data collection and quality, ethical dimensions and skills for AI. The key areas of focus are economic growth, with the use of AI and the application of AI to the public sector. Law 4961/2022 "Emerging information and communication technologies, strengthening digital governance and other provisions" (the "Law") introduced several provisions impacting the use and development of AI in Greece. Said provisions entered into force on 1 January 2023.

This Law constitutes the first attempt of the Greek legislator to regulate the use of AI in both public and private sector, ahead of the highly anticipated Commission's, i.e., the EU Regulation – the Artificial Intelligence Act (the AI Act) which will provide harmonised rules on AI for all Member States. Pursuant to the Explanatory Memorandum, one of the key objectives of the Law is the implementation of a comprehensive national strategy for the development of AI in Greece.

As regards private entities, Art. 9 of the Law imposes, *inter alia*, an information obligation to private entities as long as they use an AI system which affects any decision-making process concerning the entity's employees or prospective employees and which has an impact on their working conditions, their selection, recruitment or evaluation. In addition, according to Art. 10 of the Law, any private sector business, excluding SMEs, must maintain a registry of AI systems used, which must include details on the system's operating parameters, the number of natural persons concerned, technical information on the manufacturer or external partners, the period of operation and any safety measures taken.

Art. 11 of the Law provides for the establishment of a Steering Committee on Artificial Intelligence, with the aim of coordination of the National Strategy for the AI, by virtue of a decision of the Minister of the Digital Governance. Moreover, Art. 13 of the Law provides for the establishment of a Committee for the Supervision of the National Strategy for the utilisation of the AI, as an executive body of the Steering Committee on Artificial Intelligence within the Ministry of Digital Governance.

Art. 14 of the Law sets out the establishment of the AI Observatory within the Ministry of Digital Governance, under the General Secretariat for Digital Governance and Simplification of Procedures, with the main objective of collecting data on the implementation of the National Strategy for the utilisation of AI, reporting on the activities related to AI in Greece, and supporting the relevant stakeholders in setting priorities and identifying opportunities and areas of added value.

Public law: For the procurement of AI-based solutions, the abovementioned law 4412/2016, as amended and in force, is applicable; as well as the contract notice provisions, the terms of the contract and the provisions of the GCC, which are applied in a supplementary way.

Moreover, Art. 7 of the Law provides that, without prejudice to the provisions on the protection of military, commercial and industrial secrecy, any contract notice or call for expressions of interest launching a competitive tendering procedure or any other procedure for the award of a public contract for the design or development of an AI system must include a clause requiring the contractor to provide the public sector entity with information on the operational parameters, capabilities and technical characteristics of the system, the categories of decisions taken or acts adopted involving or supported by the system, as well as the conduction of the algorithmic impact assessment, including, *inter alia*, an obligation to waive any claims which might jeopardise the right of natural or legal persons to be provided with information.

With reference to the use of AI in the public sector, Art. 4 of the Law provides that public sector bodies may use AI systems for the process of making or supporting the process of making a decision or issuing an act, which affect the rights of a natural or legal person, only if such use is expressly provided for in a specific legal provision containing appropriate safeguards for the protection of those rights.

Moreover, Art. 5 of the Law introduces an obligation for the aforementioned public sector bodies using AI systems to conduct an Algorithmic Impact Assessment before the AI system becomes operational, taking into account, among other things: (a) the objective pursued, including the public interest served by the use of the system; (b) the capabilities, technical characteristics and operational parameters of the system; as well as (c) the expected benefit to the public, in relation to the potential risks and impacts that the use of the system may entail.

Furthermore, Art. 6 of the Law imposes a series of obligations on public sector bodies regarding the use of AI systems and the public disclosure on: (a) the operational parameters, capabilities and technical characteristics of the system; (b) the categories of decisions taken or acts adopted involving or supported by the system; and (c) the conduction of the algorithmic impact assessment. It should be noted that the imposition of said obligations are without prejudice to Art. 12 to 14 of the General Data Protection Regulation on the exercise of information rights by natural persons. Per para. 3 of the same article, the National Transparency Authority shall be competent for receiving, processing, evaluating and, where appropriate, investigating or filing complaints or reports related to violations of the above obligations.

In the same context, Art. 8 of the Law stipulates that any public sector entity using AI systems must maintain a registry thereof, which it must update by 1 March each year and, in any case, when a new system becomes operational.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Data used to train machine learning systems could, in some cases, be protected as confidential information and their use by third parties could be provided for under the respective agreement(s).

Under Greek Law 2121/1993 on the protection of intellectual property (Greek IP Law), certain databases (i.e., a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means), as well as Digital Computer Aided Design Files (C.A.D. Files) which contain source code, could be copyright protected and therefore also licensed contractually.

Regarding ownership, under Greek Law, the owner of any copyright work needs to be a natural person, and such person always maintains the moral rights, though such rights can be restricted. For entities-employers of employees that are also creators, Greek IP Law provides that all exploitation/use/economic rights to the works related to computer programs automatically vests with the employer (provided that a written employment agreement has been executed). For works of independent contractors, however, the transfer and assignment of the respective IP rights should take place via written agreements.

It should be highlighted that the anticipated EU AI ACT approved by the European Parliament will introduce requirements for general-purpose AI systems such as transparency obligations; among these requirements is compliance with EU copyright law.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Algorithms cannot be the object of copyright protection, since it is considered that they do not constitute the expression of an original creation. The same applies for the ideas and principles on which any element of a computer program is based, including those on which its interconnection systems are based. The source and machine code (software), Digital Computer Aided Design Files (C.A.D. Files) if they contain source code, the preparatory work to the design and the structure of a computer program can be protected, but not the algorithm, which is considered an idea/principle on which elements of a computer program are based. In matters of ownership of the elements that can be protected under copyright, our "Note on ownership" included in our answer to question 10.2 above also applies in this case. In general, it should be highlighted, that algorithms can be protected as trade secrets via contractual arrangements.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

In Greece Art. 31 of Law 4961/2022 "Emerging information and communication technologies, strengthening digital governance and other provisions" introduces for the first time a definition of the terms "blockchain", "distributed ledger technology" and "distributed ledger technology systems". Chapter E of the said Law on the applications of Distributed Ledger Technology provides that blockchain technologies may be used in data recording and transactions, in smart contracts, where the terms of the contract may be predefined on the blockchain, as well as for the maintenance of the Single Register for Elevators.

Art. 4961/2022 (art. 47 *et seq.*) provides for the validity and enforceability of transactions in the application of DLT, evidentiary matters, smart contracts, etc.

Public law: For the procurement of blockchain-based solutions, the abovementioned Law 4412/2016, as amended and in force, is applicable, as well as the contract notice provisions, the terms of the contract and the provisions of the GCC, which are applied in a supplementary way.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

The Digital Transformation Strategy for 2020-2025 of the Ministry of Digital Governance of Greece provides, *inter alia*, for the use of Distributed Ledger Technologies (DLT) in the public sector, in the public document verification, in the publication of public acts in "Diavgeia" ("Clarity" program on the internet), in the digitisation of public contracts, the management of health data, etc.

While blockchain technology is used to some extent in the public domain, there have not yet been any large-scale applications. Notably, the Hellenic Blockchain Hub (a non-profit organisation of executives from the public and private sector) has recently entered into a memorandum of co-operation with various organisations, including the Supreme Council for Personnel Selection (ASEP). Blockchain-based technologies are most widely being adopted in the IT, financial, fintech and insurance sectors, as well as in public administration, while interest in the energy and maritime industry is also steadily growing. In the financial sector in particular, cryptocurrencies are disrupting traditional banking and payment systems, offering alternatives for peer-to-peer transactions, remittances, and cross-border payments.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Public law: See our answer to question 9.3 above.

Data protection related issues that should be addressed include, among others:

- the decentralised nature of blockchain technology poses ambiguity regarding data controller and processor roles within its distributed peer-to-peer network structure;
- the complexity of determining the applicable jurisdiction and enforcing regulations on decentralised blockchain technologies;
- issues on safe cross-border data transfers; and
- data protection and privacy security issues.

IP-related issues that should be addressed include, *inter alia*:

- IP rights and protections should reflect the regulations of the jurisdictions involved in the transaction;
- whether new works should be owned solely or jointly and how they should be owned;
- licensing of IP and relevant permissions and limits;
- use of open source in blockchain and limitations thereof, as well as liabilities related to potential infringement of the open-source licence terms;
- new technology, new developments: ownership thereof and protection of content and relevant rights (as patents or otherwise); and
- IP infringement indemnification.

Private law: In this case, the party responsible for the state of the product at each stage of its manufacture, storage, transport, sale and delivery to the consumer should be specified in order to distinguish at all times who is liable for any defects or destruction of the product.

Konstantinos Vouterakos leads the firm's TMT practice, advising on communications and information technology law. He represents both national and international clients with respect to regulatory issues under the jurisdiction of the National Telecommunications and Post Commission (EETT), the principal telecommunications regulator in Greece. Konstantinos acts for a variety of TMT clients and handles various information technology matters. He has represented various clients in many projects and aspects related to the above subject-matters, *inter alia*, in the granting of licences for the installation of electronic communication networks and the rendering of relevant services, in public consultations and bidding procedures, and advises on regulatory compliance issues in alignment with the electronic communications framework.

Kyriakides Georgopoulos (KG) Law
28, Dimitriou Soutsou Str.
115 21 Athens
Greece

Tel: +30 210 817 1580
Email: k.vouterakos@kglawfirm.gr
LinkedIn: www.linkedin.com/in/konstantinosvouterakos

Elisabeth Eleftheriades currently leads the firm's Project Development/Startups and Innovation team. Her area of expertise covers Corporate and M&As in the technology, real estate and infrastructure sectors, where she acts for buyers and sellers, private equity investors (VCs and angels) in Greece and other jurisdictions. She also acts for lenders and IFIs as well as private sponsors in PPPs and project finance transactions in energy and infrastructure, with a focus on diligence, and the drafting and negotiation of construction and operation contracts.

Kyriakides Georgopoulos (KG) Law
28, Dimitriou Soutsou Str.
115 21 Athens
Greece

Tel: +30 210 817 1626
Email: e.eleftheriades@kglawfirm.gr
LinkedIn: www.linkedin.com/in/elisabeth-lisa-eleftheriades

Dr. Victoria Mertikopoulou holds an LL.M. from U.C.L. and a Ph.D. on EU Competition Law (U. of Athens). Her practice focuses on EU competition law, the digital economy, regulatory and compliance and consumer protection. She acts for a variety of TMT clients on various information technology projects and matters regarding electronic communications regulation. Prior to joining KG Law Firm, she served as a member of the Directorate General of Competition and, since 2012, as Commissioner – Rapporteur of the HCC; as HCC Commissioner she regularly participated in European and International organisations (European Competition Network, OECD, ICN). She is the scientific expert of the Working Group on Evaluation of Judicial Systems of the Council of Europe. She is also a regular contributor and author for some of the leading industry publications and has given lectures at international conferences and universities on her areas of expertise.

Kyriakides Georgopoulos (KG) Law
28, Dimitriou Soutsou Str.
115 21 Athens
Greece

Tel: +30 210 817 1545
Email: v.mertikopoulou@kglawfirm.gr
LinkedIn: www.linkedin.com/in/victoria-mertikopoulou-9037055

Constantinos Kavadellas heads the firm's Public & Administrative Law department. His practice focuses on public and administrative law litigation. His experience extends to a wide range of public law aspects such as administrative law, public supply and works contracts, pharmaceutical law, environmental law, land and urban planning law, tax law, social security law and financial law. He also provides consulting services to individuals, legal entities and public bodies in many public law issues, participating in numerous due-diligence projects regarding their licensing status from an environmental and urban planning law perspective. Constantinos has 18 years of experience in dispute resolution, both relating to out-of-court and judicial settlements. He has pleaded in numerous public law cases before the Supreme Administrative Court (Council of State), the Administrative Courts of First Instance and Second Instance (Courts of Appeals) and the Court of Auditors.

Kyriakides Georgopoulos (KG) Law
28, Dimitriou Soutsou Str.
115 21 Athens
Greece

Tel: +30 210 817 1624
Email: c.kavadellas@kglawfirm.gr
LinkedIn: www.linkedin.com/in/constantinos-kavadellas-2b7801b8

Kyriakides Georgopoulos (KG) Law Firm is a leading Greek multi-tier business law firm dating back to the 1930s and recognised as one of the most prestigious law firms in Greece. The firm has over 100 highly skilled lawyers actively involved in the provision of legal services to high-profile Greek and international clients in complex and innovative cross-border deals. KG multidisciplinary teams of lawyers are efficient in working closely with clients and in ascertaining innovative and practical solutions to complex problems. KG Law Firm and a significant number of its lawyers are consistently ranked highly by the most prestigious of international directories.

https://kglawfirm.gr

KG
KYRIAKIDES GEORGOPOULOS
Law Firm

Hong Kong

Bird & Bird


Wilfred Ng


Olivia Cheng

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, it is not.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The public procurement regulatory regime, which is regulated under the Stores and Procurement Regulations ("**SPRs**") pursuant to the Public Finance Ordinance (Cap. 2), covers the procurement of goods, all construction services and eight major groups of non-construction services (including computer and telecommunications services) by government entities and five public bodies, if the contract value exceeds certain thresholds. If the requirements are met, the procuring entity must ensure that the procurement is conducted in compliance with the SPRs, which reflect the requirements of the World Trade Organization's Agreement on Government Procurement to which Hong Kong acceded in 1997.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

In general, no. However, in a public sector outsourcing, the term of the contract and any extension may be subject to the SPRs.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, this is left to the parties to negotiate.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

At present, there is no general implied duty of good faith and fair dealings in Hong Kong contract law in all contracts. If the duty is incorporated as a contractual term by the parties, the court would generally apply the typical principles of contractual interpretation to determine the extent and effectiveness of such obligation. It should be noted that recent English case law (which has persuasive authority in Hong Kong) has suggested that in what the courts are increasingly labelling "relational contract", an obligation of good faith may be implied. No one factor is determinative, but a contract is more likely to be considered relational if it involves a mutual intention to establish a long-term relationship, a high degree of communication and collaboration, the parties placing mutual trust and confidence in one another, significant investment and exclusivity. Although there is no direct authority on the point, a technology sourcing contract could well fall within this category. Given the uncertainty in this area, if the parties do not wish a duty of good faith to be implied, they should include an express term to this effect.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The following remedies are available:

- Damages.
- Specific performance/injunction (available at the discretion of the court).
- Termination.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In addition to the remedies available at law, the customer could seek the following protections:

- service credits;
- indemnities from the supplier for loss suffered by the customer in specified circumstances;
- other forms of financial consequences, such as loss of exclusivity, a reduction in the minimum price payable to the supplier or the right to withhold payment;
- warranties;

- step-in rights;
- specific provision for termination in defined circumstances (for example, material breach or insolvency);
- a requirement for the supplier to hold insurance and note the customer's interest on its insurance policy;
- a parent company guarantee; and
- an appropriate governance or escalation structure.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Any termination that occurs in accordance with the terms of the contract would be justified without giving rise to a claim for damages from the terminated party.

In addition, the following events are generally considered sufficiently serious to justify immediate termination, regardless of the terms of the contract:

- a repudiatory breach, i.e. a breach of a condition or contractual term that would deprive the innocent party of "substantially the whole benefit of the contract";
- a breach indicating that the counterparty no longer wishes to continue with the contract;
- if a party is unable to perform its duties under the contract (e.g. through its insolvency); or
- if, through no fault of the parties, the performance of the contract becomes impossible or if external events conspire to make it radically different from what was originally envisaged by the parties (i.e. "discharge by frustration").

2.7 Can the parties exclude or agree additional termination rights?

The parties are free to agree specific termination rights, which can block or extend rights implied by general law (e.g. a party commits a series of minor but persistent breaches, there is a change of control of one of the parties, etc.).

2.8 To what extent can a contracting party limit or exclude its liability under national law?

In general, in a business-to-business contract, the parties are free to exclude liability altogether, put a financial cap on liability, restrict the types of loss recoverable or remedies available and/or impose a short time limit for claims, subject to the following:

- under the Control of Exemption Clauses Ordinance (Cap. 71) ("**CECO**"), it is not possible to exclude or restrict liability for death or personal injury resulting from negligence. In the case of other loss or damage, the exclusion or restriction of liability for negligence must satisfy CECO's reasonableness requirement;
- an exclusion or restriction of liability for fraud or fraudulent misrepresentation is unenforceable and should be carved out from any general exclusion of liability;
- exclusions or restrictions of liability for pre-contractual negligent or innocent misrepresentation must satisfy the requirement of reasonableness under CECO;
- if the parties are dealing on written standard terms of business, any exclusion or restriction of liability for breach of contract must satisfy CECO's reasonableness requirement. Where business parties have a negotiated agreement, CECO does not apply to exclusion/restriction of liability for breach of contract; and
- implied terms as to title to, and quiet possession of, assets cannot be excluded or restricted, while those relating to satisfactory quality, fitness for purpose and certain other matters can only be restricted in business-to-business contracts where this meets CECO's reasonableness requirement.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, subject to the limitations set out in question 2.8 and the reasonableness test under CECO.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, the same principles generally apply across all these types of technology procurement contract.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

The choice for the ultimate determination of a dispute that arises under a contract for the procurement of technology solutions and services is generally between court litigation and arbitration. Court litigation remains the most common mechanism, in part because, unless the parties agree to another approach, they will be obliged to litigate by default. However, arbitration is a popular method, particularly given that the process is confidential.

It is common for technology contracts to include certain levels of "alternative dispute resolution" as preliminary steps to be taken in order to try to resolve a dispute before the final stage of litigation or arbitration. Such steps – which can be agreed to be either mandatory or optional – often include:

- one party giving notice to the other of the nature of the dispute;
- levels of commercial negotiation between the parties about the dispute, first at an operational level with the issue being escalated up to project managers, any relevant steering/project committee and the parties' executives if it cannot be solved within specific periods of time; and
- mediation, being a confidential process under which a neutral third party (who has no binding decision-making power) is appointed to attempt to facilitate the parties in reaching a negotiated settlement.

It is also open for the parties to agree that disputes of a technical nature (or disputes that are particularly industry-specific) can be resolved by expert determination.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The parties will define which intellectual property ("**IP**") rights belong to each party at the start of the transaction ("**Background IP**"). This Background IP will be specifically

ring-fenced to clarify that only prescribed use by the other party will be allowed. This will typically be accomplished by way of an IP licence within the scope of the outsourcing agreement. The intention is that any use outside of those parameters will be prohibited.

The parties will also have to consider what new IP rights may come into existence during the course of the technology sourcing transaction ("**Foreground IP**"). The outsourcing agreement will need to make provision for who will own the Foreground IP and what permission may have to be sought in order to make use of it.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes, any assignment of patents, registered trade marks and registered designs would be void unless they are: (i) in writing and signed by the assignor; and (ii) registered with the Patent Registry, Trade Marks Registry and Designs Registry, respectively. Assignment of copyright must also be in writing and signed by the assignor.

It is also considered best practice to enter into a written agreement to license other types of IP rights. It is also usually advisable (but not a legal requirement) for an exclusive licensee of registered IP rights (such as patents or registered trade marks) to register the exclusive licence with the Hong Kong Intellectual Property Department.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Such information can be protected under Hong Kong common law of breach of confidence or through contractual means. To qualify for protection under Hong Kong common law, the information must have: (a) the necessary quality of confidence; (b) been imparted in circumstances importing an obligation of confidence; and (c) been misused to the detriment of the party communicating it.

That said, parties will typically agree confidentiality provisions in the technology outsourcing agreement rather than relying on confidentiality protection at common law. Confidentiality provisions in the agreement are likely to include: defining the know-how, trade secrets and confidential information of each party; creating a contractual duty to maintain this information in confidence (subject to some typically agreed carve-outs); specifying its use within the scope of the IP licence (see question 4.2 above); and defining the duration of the confidentiality undertakings (for a fixed period or potentially indefinitely depending on the perceived value of the confidential information).

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

In Hong Kong, the processing of personal data is regulated generally under the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"), irrespective of the types of services concerned. In essence, consent from data subjects is generally not required, provided that the data subjects have been properly notified of the prescribed information (e.g. types of data to be transferred, purpose of transfer, classes of transferee, etc.). Consent is only required in specific circumstances where personal data is used for: (1) a new purpose; (2) direct marketing purposes; or (3) matching procedure.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes. While the specific provision governing cross-border transfer of personal data under the PDPO has yet to come into force, such transfer remains subject to the general requirements under the PDPO.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Yes. The PDPO imposes obligations on data users to: (a) comply with security obligations in relation to the personal data held by the data user; and (b) ensure that its data processors (e.g. technology service providers) comply with such security obligations. Depending on the industry concerned, industry-specific rules may also apply (see question 7.1 below).

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

There is no law in Hong Kong providing for the automatic transfer of the employment relationship from one entity to another entity.

Where there is a change of ownership of business and the employee agrees to enter into new employment with the new owner, there are provisions under the Employment Ordinance ("**EO**") preserving employees' continuity of employment and providing for situations where the original employer may be able to avoid liability for severance payments. However, the law has not developed to determine whether outsourcing a part of a business to a third-party service provider (in the absence of a transfer of assets and goodwill on an ongoing concern basis) would constitute a change of ownership of business.

In an outsourcing scenario, where workers are supplied by a service provider to provide services to a customer, the general position is that the employer remains to be the service provider, and not the customer receiving the services. Usually, no change to the employment relationship will be required as the arrangement can be implemented by providing in the workers' employment contract that they are required to perform their services in the customer's premises.

Having said that, employees may also be "transferred" to provide services to the customer by way of secondment or through direct hire by the customer.

6.2 What employee information should the parties provide to each other?

There are no specific requirements in relation to what employee data needs to be transferred.

In practice, it is common for the service provider to provide to the customer information about the workers that are required for the services to be provided under the arrangement. Such information could include the workers' name, payroll details, skills, qualifications and work experience, etc. If any personal data will be transferred, parties should ensure that any transfer of personal data is in compliance with the PDPO (Cap. 486).

In an outsourcing arrangement, it is advisable to obtain the workers' consent before their data is transferred to the other party. Also, the party providing the data should request that the receiving party provide an undertaking to comply with the PDPO and keep such data secure.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

There is no restriction on dismissing employees for a reason connected with the outsourcing arrangement. Employees' employment needs to be terminated on the basis of a valid ground of dismissal under the EO. Employers should also ensure that the employees do not fall under certain categories of employees where termination of employment is prohibited, and the employment is not terminated on discriminatory grounds.

As the customer/end service user should not be the employer of the outsourced workers, they would not have the right to terminate the worker's employment. Generally, the outsourcing agreement would contain provisions regarding the management of outsourced workers, and the customer's rights if it is dissatisfied with a worker's services, or a worker has breached any relevant rules and regulations. However, the decision of whether to discipline or terminate a worker's employment would ultimately be a decision for the service provider, which is the employer.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

There is no legal restriction regarding the harmonisation of employment terms of outsourced workers with those of other employees, and this is a matter of business decision.

As the workers will usually remain employees of the service provider, there are no issues for the terms of employment of these outsourced works to be the same as other employees employed by the service provider.

6.5 Are there any pensions considerations?

As the service provider is likely to remain as the employer of the outsourced workers, it will continue to be responsible for making Mandatory Provident Fund ("**MPF**") contributions for the workers as usual. However, if there is any change in the employment structure, then the new employer will need to enrol the workers into an approved MPF scheme and make monthly contributions.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

If there will be an offshore element to the outsourcing arrangement, the worker may need to apply for necessary immigration approvals prior to commencing work.

Depending on the jurisdiction and the duration of performance of work offshore, there is a risk that the workers may accrue employment law rights and benefits under local law (even though their employment continues to be governed by Hong Kong law).

There may also be permanent establishment and tax equalisation considerations.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Outsourcing transactions are typically regulated by industry authorities. For instance, in the financial services sector, a number of industry authorities regulate outsourcing, including:

- **Banking sector**: the Hong Kong Monetary Authority ("**HKMA**") has issued the Supervisory Policy Manual on Outsourcing, which includes requirements such as risk assessment, ability of service provider, the need to have an outsourcing agreement in place, etc. In May 2022, the HKMA introduced a new Supervisory Policy Manual chapter OR-2 that requires authorised institutions to take into consideration third-party dependency management, including outsourcing, with respect to operational resilience. Further, the Guidance on Cloud Computing published by the HKMA in August 2022 sets out its supervisory expectations of authorised institutions on adopting cloud computing services, covering principles on governance framework, risk management, control and capabilities, and protection of access and legal rights. In December 2023, the HKMA issued a circular on sound practices for managing cyber risks associated with the use of third-party service providers. Authorised institutions are expected to assess their current controls for mitigating cyber risks associated with third parties, taking into account the provided guidance. Where gaps are identified, authorised institutions are expected to consider applying the sound practices in a manner commensurate with their cyber risk exposures and the level of reliance on third parties, including:
  - ensure sufficient emphasis on cyber risk associated with third parties in risk governance framework;
  - holistically identify, assess and mitigate cyber risks through putting in place security measures supported by proper contractual agreements with effectiveness evaluated throughout the third-party management lifecycle;
  - assess supply chain risks associated with third parties supporting critical operations;
  - expand cyber threat intelligence monitoring to cover key third parties and actively share intelligence with peer institutions;
  - strengthen the preparedness for supply chain attacks with scenario-based response strategies and regular drills; and
  - continuously enhance cyber defence capabilities through adopting the latest international standards, practices and technologies.
- **Securities and Futures sector**: the Securities and Futures Commission ("**SFC**") has issued a circular to licensed corporations on the Use of External Electronic Data Storage, which contains requirements when licensed

corporations keep regulatory records exclusively with electronic data storage providers ("**EDSPs**"), including public and private cloud service providers. Pursuant to the licensing regime for Virtual Asset Trading Platforms ("**VATPs**") which took effect on 1 June 2023, the SFC has issued the Guidelines for Virtual Asset Trading Platform Operators ("**VATP Guidelines**"). The VATP Guidelines impose various obligations on a platform operator, including the obligation to ensure that the VATP (including the trading system and custody infrastructure) is properly designed and operated in compliance with all applicable laws and regulations. Where the VATP or any activities associated with the VATP is provided by or outsourced to a third-party service provider, the VATP operator should perform appropriate due diligence, conduct ongoing monitoring, and make appropriate arrangements to ensure that the VATP operator meets the requirements in the VATP Guidelines. In particular, the VATP operator or its associated entity should enter into a formal service-level agreement with the service provider which specifies the terms of services and responsibilities of the provider. This service-level agreement should be regularly reviewed and revised, where appropriate, to reflect any changes to the services provided, outsourcing arrangements or regulatory developments. Whenever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details.

- **Insurance sector**: the Insurance Authority ("**IA**") has also issued the Guidelines on Outsourcing ("**GL14**") and Guidance Note on Outsourcing ("**GN14**"), which, respectively, contain guidance and recommendations on prudent risk management practices for outsourcing, and sets out a number of essential issues that the IA expects an authorised insurer to take into account in formulating and monitoring its outsourcing arrangements.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The simplest outsourcing structure is a direct outsourcing between the customer and the supplier.

In a multi-sourcing, the customer enters into contracts with different suppliers for separate elements of its requirements.

In an indirect outsourcing, the customer appoints a supplier (usually Hong Kong-based) that immediately subcontracts to a different supplier (usually non-Hong Kong-based).

Where a customer desires more "skin in the game", an alternative option is for the customer and supplier to set up a joint venture company, partnership or contractual joint venture, perhaps operating in an offshore jurisdiction. Customers can also adopt "insourcing" models (or captive service models), which are adopted by financial institutions in Hong Kong where group companies "insource" certain functions to an affiliated or a wholly-owned company that is responsible for provision of the services, and the affiliated or wholly owned company then outsources the services to suppliers.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

When negotiating the contract, the parties usually try to identify and agree a set of objectives and measurable criteria to measure the supplier's performance (key performance indicators ("B") or service levels). These service levels need to be combined with a:

- process for recording and reporting on success or failure in achieving the targets; and
- formula under which financial compensation is paid to the customer if targets are not met. These are referred to as service credits or liquidated damages.

The aim of service credits is to compensate the customer for poor service without the need to pursue a claim for damages or terminate the contract, and to motivate the supplier to meet the performance targets.

The supplier will want to ensure that the stated service credits are the sole remedy of the customer for the particular failure concerned, but this should be without prejudice to the customer's wider rights in relation to more serious breaches of the contract or persistent failures in performance. Service credits are generally enforceable, provided they are a genuine pre-estimate of the customer's loss or can be shown to protect a legitimate commercial interest of the customer and are not a contractual penalty.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The method of charging will depend on the type of services being outsourced, the nature of the supplier's appointment and the balance of risk between the parties.

The most common charging methods are as follows:

- Cost plus, where the customer pays the supplier both the actual cost of providing the services and an agreed profit margin.
- Where there will be a regular and predictable volume and scope of services and the customer wants to have greater certainty over its budget, a true fixed price will be a better option for a customer.
- Where the level and volume of service is less predictable, the parties may decide to opt for a pay-as-you-go charging model whereby the customer pays a pre-agreed unit price for specific items of service (such as volumes of calls taken), often based on a rate card.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

The assignment of key contracts must be in writing. The parties should check the terms of such contracts at an early stage to ensure that they are able to assign without the counterparty's consent and attempt to obtain such consent if necessary. Alternatively, if the terms of the contract permit, the customer can retain ownership of the contract and allow the supplier to supply the services to the counterparty as agent of the customer on a "back-to-back" basis. It should also be considered whether the burden of the contract should also transfer to the supplier, either by:

- novation; or
- express indemnity (which leaves some residual risk with the transferor).

The concept of a contract being leased or licensed is not generally recognised under Hong Kong law.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The key tax issues are as follows:

- **Transfer of assets to supplier**: none, save for stamp duty (see below).

- **Transfer of employees to supplier**: none for employee termination or re-engagement in relation to any transfers under outsourcing arrangements.
- **Corporation tax**: the statutory tax rate for corporations is 16.5% for the assessable profit arising in, or derived from, Hong Kong.
- **Stamp duty**: stamp duty is not typically payable for outsourcing agreements, as it is generally only payable in Hong Kong for the sale, transfer or lease of immovable property or transfer of Hong Kong stock.
- **Withholding tax**: payments to the supplier could be subject to withholding taxes, depending on the treatment in the customer's jurisdiction and any tax treaty protection.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Where software applications are installed on a customer's own systems (as opposed to being accessed remotely on a software-as-a-service model), some of the key issues to consider from a contractual perspective include the following:

- **Permitted users**: users will need to be expressly licensed to use the software so a customer should consider whether, for example, other group companies will need to be licensed in addition to the main customer entity. Restrictions will often be placed on the number of individual users who may access or use the software. Care should be taken if software may be accessed directly or indirectly by third parties such as an outsourcing service provider or by the customer's own customers and an analysis undertaken as to whether these entities need to be expressly licensed to use the software.
- **Other restrictions**: a software vendor will often seek to impose restrictions around the geographic locations in or from which the software can be used or accessed, the number of machines onto which it can be loaded, the number of copies that may be taken, the processing volumes that may be handled and/or the nature of the operating environment in which the software is loaded. These should all be checked to ensure they are consistent with a customer's business requirements and intended use of the software.
- **Open-Source Software ("OSS")**: a customer should check whether the software includes any OSS code. A detailed analysis of OSS issues is beyond the scope of this chapter, but in general terms where OSS is present, it will be licensed under its own terms that, while free of many of the use restrictions that apply to proprietary software, will generally contain fewer protections for a customer and be licensed on an "as is" basis. Particular issues can also arise where a customer wishes to modify and adapt and possibly distribute the software and one of the more restrictive OSS licences is used.
- **Warranties**: appropriate warranty protection should be sought in relation to the performance of the software and its conformance to specification; for package software, this is often limited by vendors to an undertaking to rectify faulty software free of charge for a defined period after delivery/installation.
- **IP infringement protection**: indemnities should be sought against the risk of a customer's use of the software infringing a third party's IP rights.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Key issues include:

- ensuring a clear description of the support and maintenance service is set out in the contract, including a clear definition of what constitutes a "fault" or "defect";
- ensuring appropriate service levels (and, where applicable, an associated service credit regime) are included; particular care should be taken around the categorisation of the severity of faults and the service levels that apply to each category;
- understanding whether the provision of upgrades and new versions of the software are included within the service or not and, linked to this, whether the vendor requires the latest version of the software to be run as a condition of providing the support and maintenance service;
- whether the services will be provided remotely or on site (or a mixture of both); and
- understanding whether, in providing the services, the vendor will have access to personal data being processed by the software – where it does, the customer will need to put in place arrangements (including appropriate contractual clauses) to ensure that the personal data is processed in accordance with the PDPO.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes, although software vendors are often reluctant to agree to them.

In broad terms, escrow agreements are generally enforceable from a Hong Kong law point of view, as long as they are not entered into when the insolvency of the vendor is actually in contemplation. From a practical point of view, the utility of an escrow arrangement for a customer will depend on the source code deposits being kept up to date and appropriate documentation being included in the escrow deposit that is sufficient to enable a competent programmer to understand the source code.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

There are no national laws or regulations that apply specifically to cloud computing arrangements *per se*, but the operation of cloud computing solutions in Hong Kong will need to comply with Hong Kong data protection and, in certain industry sectors, cybersecurity requirements. There are also certain industry-specific regulations that affect the way in which cloud computing arrangements are undertaken and operated – for example, in the financial services sector.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions are being adopted widely in Hong Kong, across a wide range of industry sectors.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Many cloud vendors, particularly those offering public cloud services, will insist on contracting on their standard terms and little if any negotiation is possible. For bigger deals or more bespoke arrangements based on private cloud delivery models, more negotiation tends to be possible but, generally speaking, a customer will still need to accept a different balance of risk than it would be used to in more traditional IT contracts.

Other key issues that a customer will need to consider include:

- appropriate licence and usage rights for applications made available via the cloud service;
- appropriate service levels, particularly around service availability;
- ensuring that customer data that will be stored in the cloud is accessible and required to be returned (in a useable format) on termination/expiry;
- as the cloud vendor will normally be a data processor for data protection purposes, ensuring that PDPO-compliant processing provisions are included in the contract (e.g. to ensure that data processors comply with data security and data retention requirements under the PDPO);
- depending on the nature of the services provided by cloud vendors, cloud vendors (whether based in or outside Hong Kong) that process content for Hong Kong customers may be subject to a cessation notice served by the Hong Kong Privacy Commissioner for Personal Data to take down any suspected doxxing content;
- understanding in which territories any personal data will be stored and ensuring that any data export arrangements comply with applicable data protection legislation;
- whether the level of protection afforded by the supplier's business continuity and disaster recovery arrangements is sufficient for the customer's purposes;
- the extent to which the supplier is entitled to use data stored on its systems for data analytics or other purposes; and
- the extent of the indemnity protection offered by the cloud vendor for third-party IP right infringement.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

There is currently no overarching national law or regulation in Hong Kong that specifically regulates the use of Artificial Intelligence-based ("**AI**") solutions. However, the following points should be noted:

- depending on the nature of the AI solution in question, existing laws in areas such as data protection and anti-discrimination may apply to the operation of a particular AI-based solution or software product; and
- the regulatory regime for Autonomous Vehicles ("**AV**") has been recently updated and came into force on 1 March 2024 to provide for the wider trial and pilot use of AVs on Hong Kong roads. The updates encompass amendments to the Road Traffic Ordinance (Cap. 374), the introduction of new subsidiary legislation titled Road Traffic (AVs) Regulations (Cap. 374AA) ("**AV Regulations**"), and the promulgation of the Code of Practice for Trial and Pilot Use of Autonomous Vehicles ("**Code of Practice**"). Under the previous regulatory framework, the Transport Department has been issuing Movement Permits in accordance with the Road Traffic (Registration and Licensing of Vehicles) Regulations (Cap. 374E) to authorise each AV trial while customised conditions are individually imposed on a case-by-case basis. With the rapid development of AVs in recent years, the practice of allowing the testing of AVs through movement permits has limitations under the Road Traffic Ordinance and its subsidiary regulations. The new regulatory regime establishes a clear framework for conducting AV trials in Hong Kong in the form of a pilot scheme through the application and issuance of AV Pilot Licences and AV Certificates. The Code of Practice sets out detailed technical, safety and operational requirements for vehicle design and construction, network security, personnel training and record-keeping, etc., in relation to the AV. Going forward, any person or institution that intends to test and use AVs on the roads in Hong Kong must comply with the updated regulatory regime.

In addition, local regulators such as the Office of the Privacy Commissioner for Personal Data ("**PCPD**") and the HKMA regularly publish guidance, principles and sector-specific guidelines on the use of AI, for instance:

- **Banking Sector**: The HKMA issued a circular to authorised institutions and stored value facility ("SVF") licensees regarding a publication of its Insights for Design, Implementation and Optimisation of Transaction Monitoring ("**TM**") Systems in April 2024 ("**Insights**"). The HKMA has conducted a thematic review examining the end-to-end processes of design, implementation and optimisation of authorised institutions' TM systems, including governance and oversight, data quality, detection scenario, threshold setting and periodic review with a focus on strengthening effectiveness and output into the anti-money laundering and counter-financing of terrorism ("**AML/CFT**") eco-system. The review also looked at how authorised institutions and SVF licensees use artificial intelligence to optimise TM systems and provided AML/CFT specific guidance based on industry best practices. As stated in the Insights and as part of HKMA's regulatory expectations, authorised institutions should take into account the guidance on High-level Principles on Artificial Intelligence ("**AI Principles**") published by the HKMA in November 2019 when deploying AI in their operations. Pursuant to the AI Principles, authorised institutions should, amongst other things:
  - adopt an effective data governance framework to ensure the data used is relevant and of good quality;
  - conduct rigorous validation and testing of trained AI models to ensure the accuracy and appropriateness of the AI models before actual deployment;
  - track the outcome of AI applications on a continuous basis and gather evidence to support investigations when incidents occur;
  - conduct periodic review and on-going monitoring to ensure that the applications perform as intended;
  - comply with data protection requirements under the Personal Data Privacy Ordinance;
  - implement effective cybersecurity measures; and
  - implement risk mitigation and contingency plans.
- **Data Protection**: In February 2024, the PCPD issued a media statement on the 'Implications of the Development or Use of Artificial Intelligence on Personal Data Privacy'. The statement outlined observations from compliance checks conducted on local organisations between August 2023 and February 2024 pursuant to the Personal Data Privacy Ordinance (Cap. 486) ("**PDPO**"). These checks aimed to understand the practices related to the collection,

use, and processing of personal data in the development or use of AI, as well as the AI governance structure within the relevant organisations. As part of the media statement, the PCPD referenced the non-binding Guidance on Ethical Development and Use of AI ("**AI Guidance**") in August 2021 to help organisations understand and comply with the relevant requirements of the PDPO when developing or using AI. The AI Guidance encourages organisations to adopt several ethical principles for deploying AI: accountability; human oversight; transparency and interpretability; data privacy; fairness; beneficial AI; and reliability, robustness, and security. The guidance includes a practice guide which provides practical examples of how organisations should approach AI governance when implementing AI in their operations, from inception to implementation and ongoing risk-based management, covering the following areas:

- AI strategy and governance;
- risk assessment and human oversight;
- development of AI models and management of AI systems; and
- communication and engagement with stakeholders.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Under Hong Kong law, there is no single property right that applies to data *per se*. Depending on its nature and/or source, the use and/or disclosure of certain data may be regulated by the law of confidential information. In addition, certain data may qualify for copyright protection or, where the data has been aggregated with other data and compiled into a database, separate copyright may exist in the database.

Where these IP rights exist in the relevant training data, an appropriate IP or know-how licence can be granted. Given the findings of the English courts (which have persuasive authority on Hong Kong courts), it is arguable that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights under Hong Kong law. Accordingly, training data can be licensed on a purely contractual basis under Hong Kong law.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Under Hong Kong law, algorithms are potentially protectable by copyright as original literary works. Where an algorithm is written by a human, the author of that work is the person who creates it (Section 11(3) Copyright Ordinance (Cap. 528) ("**CO**")). This is taken to be the person responsible for the protectable elements of the work, being those elements that make the work "original" (i.e. those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using machine learning without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e. there is no human author such that the work qualifies as "computer generated" under Section 198 CO. In these circumstances, Section 11(3) CO deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under Section 17(6), the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created. While the test set out in Section 11(3) CO determines the identity of the author of a computer-generated work, it is not currently clear as a matter of Hong Kong law whether such work will actually qualify as copyright work. Under Section 2(1) CO, copyright only subsists in original literary works, which requires an intellectual creation by the author that reflects an expression of their personality. It is questionable whether an algorithm developed by machine learning without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation. As a result, such an algorithm may not qualify for copyright protection under Hong Kong law. An alternative view is that Section 11(3) CO in fact creates its own *sui generis* right for computer-generated works that is not subject to the usual requirement for originality. These issues have not thus far been addressed by the Hong Kong courts, and claims to copyright (or an absence of rights) in algorithms developed by machine learning without human intervention must therefore be treated with caution in Hong Kong.

Given the uncertainty of the law in this area, the issue of ownership of copyright should be clearly dealt with in the customer contracts.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there are not.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain-based technologies are being adopted in a variety of sectors, including the financial services, life sciences and media sectors.

The most common use case relates to using blockchain-based technologies to better record and share data between disparate and unconnected parties, taking advantage of some of the technology's benefits such as:

- **immutability**: once data is added to a blockchain database, it is very hard to interfere with it without the change being obvious to all parties and therefore rejected (this can help combat fraud);
- **security**: cryptography (including "hashing") is used to secure the data held on the blockchain database, making it very secure; and
- **peer-to-peer**: because the blockchain network is peer-to-peer, it can continue to function even if some of the nodes in the blockchain network become unavailable. This makes the blockchain network more robust than networks reliant on a central server where the network could go down if the central server is unavailable.

In the financial services sector, blockchain-based technologies have been used to enable different entities in the syndicated loans market (agent banks, syndicates of lenders, borrowers) to share data relating to loans more efficiently. Historically, this data has been manually communicated between these parties by phone, fax and email. As a result, this data can be lost, miscommunicated or falsified. In addition, there are significant

administrative costs incurred by these parties having to manage their own databases and reconciling the data they hold with each other. A blockchain-based database enables these parties to publish and securely record data relating to their syndicated loans onto a private blockchain network and then securely share that data in real-time with others. This makes the process more efficient and less costly as the parties are sharing data via one (albeit distributed) database. In addition, once data is published to the blockchain database, it is very difficult for it to be tampered with, which helps reduce fraud.

In the life sciences sector, electronic health records could be securely operated on a private blockchain network, protecting patient data and privacy while allowing doctors to access their patients' medical histories and empowering researchers to use shared data to further scientific research. Blockchain-based technologies enable permission layers to be built into the system. So, while patients are unable to change or delete medical information inputted by their doctors, they can control access to their profiles by granting full or partial visibility to different stakeholders.

More recently, for example, in the media sector, non-fungible tokens ("**NFTs**") have been created or minted on blockchain networks and then bought and sold on NFT marketplaces that are integrated with the blockchain network: end users purchase an NFT on the market place and then the purchase history is tracked on the associated blockchain database, providing an immutable proof of ownership. Advocates claim that NFTs are the next generation in digital collectibles (the electronic version of the Panini trading cards that have been widely traded in school playgrounds since the 1970s).

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Private blockchain contracting

Organisations looking to exploit blockchain-based technologies are often attracted to private blockchain networks (as opposed to public blockchain networks) because of the greater certainty as to the rules governing how the blockchain network operates and the opportunity to build in protection through contracting. Typically, an organisation will use proprietary software owned by a blockchain developer to set up a private blockchain network. In such circumstances, the organisation can engage the blockchain developer to run the blockchain network (including all the nodes) on its behalf as its subcontractor on the basis that the blockchain network is made available by the organisation to its customers (let us call the organisation running the blockchain network the "**trusted intermediary**" and its customers the "**participants**"). In such circumstances, the key contracts governing the use of a private blockchain network would typically comprise:

- a **blockchain developer contract**, which is between the blockchain developer and the trusted intermediary operating the blockchain network. The trusted intermediary will license the right to use the blockchain developer's software and will engage the blockchain developer to provide it with ancillary services related to the launch, operation, support and development of the network, as the trusted intermediary's subcontractor;
- a **participation contract or charter**, which is the multi-lateral contract between the trusted intermediary and all the participants that want to gain access to the blockchain network. This contract governs the "rules" of the network. In this agreement, the trusted intermediary will include obligations on participants relating to acceptable use of the network (e.g. not uploading infringing material);
- a **blockchain services contract**, which is a bilateral contract between the trusted intermediary and each participant governing the provision of access to any technology by the participant so it can access the blockchain network. In addition to IP licensing, this contract will deal with issues such as availability of the network and liability.

Key legal and practical issues that come up include liability (what happens if data is lost or corrupted), security (what security measures does the trusted intermediary have in place to ensure the integrity of the network), service levels (uptime of the network) and IP (who owns the IP in any bespoke developments made by the blockchain developer). In addition, it is important that any commitments the trusted intermediary provides to a participant (for example, under the blockchain services contract) are, where applicable, flowed down to the blockchain developer under the blockchain developer contract.

IP in the blockchain – who owns it?

The blockchain network will comprise two key elements: the back-end blockchain software that determines how data is recorded on the blockchain database; and the user-facing app. The back-end blockchain software will often be pre-existing software that is utilised by the blockchain developer to service multiple clients. In contrast, the user-facing app may be bespoke software created by the blockchain developer for the trusted intermediary to solve its particular use case.

The user-facing app is what each participant accesses and will interoperate with the back-end blockchain software via an application programming interface ("**API**"). One of the key IP battlegrounds between the blockchain developer and trusted intermediary is who owns the IP in the user-facing app; this is most likely to be decided by the needs and bargaining positions of the parties.

Irrespective of ownership, the user-facing app should, where possible, be developed in such a way that it is able to interoperate with other blockchain solutions. Otherwise, the trusted intermediary will be "locked in" to the blockchain developer's solution.

Are there legal challenges with blockchain?

Although no specific privacy regulation exists for the technology in Hong Kong, any processing of personal data remains governed under the PDPO. Accordingly, when dealing with blockchain, organisations must consider different issues relating to data protection when implementing a blockchain network, such as:

- the roles played by the different parties in the transaction and what data protection obligations are attached to such roles (e.g. the role of a miner against the role of a transaction creator or a validator); and
- compliance with security requirements and the data minimisation principle (e.g. whether it is really necessary to use a blockchain network).

Prior to implementing a blockchain network, organisations should carry out a detailed analysis of what kind of information is going to be collected and shared on the network, how it is going to be processed and stored, and what the risks are. Proper contractual arrangements between all the parties involved should also be put in place.

Wilfred Ng is a Partner in our Corporate and Commercial Department based in Hong Kong. He is a bilingual (Chinese and English) technology, media, telecoms and data protection lawyer experienced in all areas of commercial, transactional, and regulatory work in the TMT sector.
Wilfred has more than 10 years' experience advising clients on a variety of commercial and transactional matters in the sectors of cloud services, financial services, media, telecommunications, retail, healthcare and public institutions. These include negotiating and preparing complex technology contracts, licensing and development arrangements, collaboration, integration and managed services agreements, as well as advising on regulatory considerations arising from the adoption, integration and transfer of technology solutions such as data privacy issues.
Prior to re-joining the firm, Wilfred was a Senior Legal Counsel with a PRC-based technology conglomerate and assisted in co-founding its International Privacy and Data Protection Team. He advised on all aspects of international data protection and privacy issues arising from the company's international, ex-PRC presence. Before the in-house role, he was part of Bird & Bird's Commercial team in Hong Kong, having spent time on secondment to the London office's Commercial team.

Bird & Bird
6/F, The Annex
Central Plaza, 18 Harbour Road
Hong Kong

Tel: +852 2248 6000
Email: wilfred.ng@twobirds.com
LinkedIn: www.linkedin.com/in/wilfred-ng-179a58144

Olivia Cheng is an Associate in our Corporate and Commercial Department based in Hong Kong. Her practice involves advising local and multinational clients in the TMT space on a broad spectrum of commercial, regulatory and transactional matters, including data protection and privacy issues. She also has experience in advising institutional clients in the payment industry on payment licensing obligations, AML regulations and outsourcing issues.
Olivia takes an avid interest in cutting edge technology which lies at the heart of Bird & Bird's ethos – supporting organisations being changed by the digital world or those leading that change. She prides herself in transferring this passion into her practice of assisting clients in the technology, healthcare, cloud services and consumer industries on a range of commercial law and data protection matters. These include negotiating transactional agreements, coordinating and implementing all stages of data protection compliance and risk analysis projects, and advising on data sharing and cross-jurisdictional transfer arrangements.

Bird & Bird
6/F, The Annex
Central Plaza, 18 Harbour Road
Hong Kong

Tel: +852 2248 6000
Email: olivia.cheng@twobirds.com
LinkedIn: www.linkedin.com/in/olivia-cheng-51971913b

Bird & Bird has more than 1,600 lawyers in 31 offices across Europe, the Middle East, Asia-Pacific and North America and clients based in 118 countries worldwide. We specialise in combining leading expertise across a full range of legal services and aim to deliver tailored local advice and seamless cross-border services.
Our technology sourcing practice is widely recognised as having a leading reputation in the field and enjoys top-tier international rankings in the *Chambers* and *The Legal 500* guides to legal profession. We advise on the full range of technology transactions, including complex outsourcings and managed services deals, system implementation projects, telecoms infrastructure and regulatory matters, strategic alliances and collaboration agreements, cloud computing deals and contracts for the deployment of AI and blockchain-based solutions.

www.twobirds.com

Bird & Bird

India

Kaizen Law


Harsh Kumar


Indraneel Chakraborty

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

There is no special law in India to expressly regulate the procurement of technology products and services by entities in the private sector. Accordingly, such procurement by private sector entities in India is governed by the contractual terms agreed between the contracting parties. These contractual arrangements must follow the principles specified under the Indian Contract Act of 1872 and the Sale of Goods Act of 1930 (for movable products). Accordingly, such contracts must fulfil the essential elements of a valid and enforceable agreement, including that the contracts are entered into freely, fairly, and with the mutual consent of the parties involved, who have the legal capacity and are not disqualified under laws, and that the contracts are for a lawful consideration and intended to serve lawful purposes.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

India has no specific laws that create an overarching framework to regulate the procurement of technology products and services by public authorities. In the absence of a comprehensive central law, procurement of technology products is governed by the General Financial Rules, 2017 ("**GFR 2017**") promulgated by the Ministry of Finance. GFR 2017 applies to all central ministries, their attached and subordinate bodies, and autonomous bodies. The GFR 2017 includes detailed procedures for procurement, bidding, contract management, and disposal of goods for use in the public service. It encourages the use of electronic means for procurement to enhance transparency and efficiency. It mandates that all Ministries/Departments publish and receive bids through e-procurement using the Central Public Procurement Portal or their e-procurement portals.

Additionally, the Department for Promotion of Industry and Internal Trade, under the Ministry of Commerce and Industry, has issued the Public Procurement (Preference to Make in India) Order in 2017 ("**PPPMI Order**"). This order promotes local manufacturing and the Make in India initiative. It provides preference to domestically manufactured goods and services in public procurement, classifies local suppliers based on local content, specifies minimum local content requirements for goods, fixed margins for purchase preferences, and basic specifications in tender-related and procurement solicitations.

Further, the Ministry of Electronics and Information Technology ("**MeitY**") also regulates the public procurement of electronic and information technology products and services in India. It has issued several notifications pursuant to the PPPMI Order, which cover a wide range of products and services including computer monitors, cellular mobile phones, cloud computing services, cyber security products, contact and contactless smart cards, etc. These notifications not only ensure that products and services procured meet prescribed cybersecurity standards, but also provide a regime to encourage the procurement of innovative technology solutions.

Various state governments in India have also initiated several state-specific regulations for their procurement activities.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

There is no statutory minimum or maximum term of a contract concerning technology-related solutions and services, and the tenure of such contracts remains entirely subject to the parties' discretion depending on the nature, scope, and complexity of the transaction.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

While there is no law regulating the length of the notice period *vis-à-vis* technology contracts, judicial precedents have established that that a "*reasonable*" notice period must be served to the other party in good faith, prior to termination of a service contract. The length of notice period for terminating such contracts in India is dependent on the parties to the transaction and typically ranges from 30 days to 90 days.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

The doctrine of good faith serves as the guiding principle

throughout the Indian Contract Act, 1872 ("**ICA**") and although not stipulated explicitly, the provisions of the ICA aim to ensure fairness, equity, and honesty in contractual relationships. Section 23 of the ICA in particular, embodies the doctrine of good faith and entails what contractual considerations and objects are lawful/unlawful.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The following remedies would be generally available to a customer under Indian law for a contractual breach by a supplier:

- **Damages (Section 73, ICA):** The customer shall be entitled to claim damages against the losses sustained. Parties may also agree to an indemnity under Section 124 of the ICA.
- **Specific performance:** The customer may be entitled to claim specific relief under the Specific Relief Act, 1963 wherein the supplier would be required to fulfil its contractual obligations.
- **Injunction:** Generally, in cases where the breach of the contract threatens irreparable harm, the customer may seek an injunction order from the court to prohibit the commission or continuation of the breach by the supplier.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In addition to the standard clauses of a technology services contract, the customer may incorporate additional provisions to its benefit, such as: (i) indemnity against any claims and losses arising out of the contract; (ii) confidentiality and data protection clauses; (iii) penalties for non-performance such as service credits; (iv) warranties against the quality and reliability of services; and (v) escrow arrangements to ensure that the source code or critical data can continue to be accessed by the customer in case the supplier goes bankrupt or there is an interruption of services to the customer.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Any termination of the contract without attracting a claim for damages shall rely on the provisions in the termination clause of the contract between the parties. Typically, a non-defaulting party is entitled to forthwith terminate the contract without serving notice to the defaulting party in the event of repudiatory breaches.

2.7 Can the parties exclude or agree additional termination rights?

Yes, while parties are at their discretion to include additional termination rights, any exclusion of rights shall be subject to the scope of the law and any such terms that are or may be contrary to the ICA are void *ab initio*.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Fundamentally, a contracting party is free to limit or exclude its liability subject to the exclusions being sound in law. While contracting parties often limit their liability with respect to indirect, special, and threatened losses; exclusions such as the duty of good faith, gross negligence, wilful misconduct, or a fraudulent intent are exclusions that may be considered unlawful and unjust.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, it is common practice for the parties to a contract to mutually agree on a financial cap on their respective liabilities arising under the contract. The liability can be limited as a fixed amount or a percentage of the transaction value or as the parties may deem fit.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

The principles stipulated in the responses to questions 2.1–2.9 are applicable to all of the aforementioned types of contracts.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

For commercial transactions including the procurement of technology solutions and services, parties generally prefer alternative dispute resolution mechanisms as compared to conventional court-driven litigation, which is treated as the ultimate legal recourse. Popular alternative dispute resolution frameworks in India for procurement of technology solutions and services include: (i) arbitration; (ii) mediation; (iii) conciliation; and (iv) negotiation, out of which arbitration is generally the preferred route.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In the context of a technology sourcing transaction, the pre-existing intellectual property rights of a party will be subject to protection under the intellectual property laws of India, briefly: the Copyright Act, 1957; the Patents Act, 1970; and the Trade Marks Act, 1999, as may be applicable. Any intellectual property ("**IP**") that is created pursuant to a contract between the parties in a sourcing transaction will also be subject to protection under the appropriate intellectual property laws and the detailed contractual provisions shall govern all aspects concerning such IP *vis-a-vis* the ownership, assignment, transfer, registration and exclusivity of such IP arising out of the contract.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Any assignment of IP shall conform to the requirements as laid down under the respective contract between the parties, and in line with the intellectual property laws in India. The statutory requirements under the aforementioned regulations in question 4.1 are briefly illustrated hereunder:

- **the Copyright Act, 1957**: Section 18 allows the first owner and the original creator of the copyrightable work to assign the copyright to an individual either wholly or partially when such copyrightable work comes into existence;
- **the Patents Act, 1970**: As per Section 68, it is mandatory for the assignment of a patent to be in writing, and the parties concerned shall ensure to embody all terms and conditions governing the rights and obligations arising from such assignment; and
- **the Trade Marks Act, 1999**: A trademark can be assigned irrespective of whether it is registered. Further, a trademark can be either assigned completely or partially and also with or without the goodwill associated with such mark. Sections 37 and 38 regulate the assignment of trademarks and provide for the use of the registered goods and services by the assignee once the payment for considerations is duly received.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Presently, India does not have any specific central law to protect trade secrets, know-how, and any related confidential business information. In the absence of such laws, courts often rely on common law principles and the terms in the contract executed between the parties to uphold and adjudicate upon any requisite protections in the interest of the aggrieved party. The courts are empowered to enforce any confidentiality/non-disclosure provisions in the contract to cease any unauthorised use or disclosure of confidential information and to ensure the same, courts may issue injunctions, specific performance orders, and other equitable remedies to that effect such as a declaratory judgment for the rescission of the contract and awarding damages to the aggrieved party.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

In August 2023, India notified the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), which is India's first legislation comprehensively governing the aspect of data protection and data processing. However, the DPDP Act is yet to be implemented and is awaiting notification from the Central Government. Until the DPDP Act is enforced, the extant laws governing the processing of personal data remain the Information Technology Act, 2000, and its rules, specifically the Information Technology (Reasonable Security Practices and Procedures and Sensitive Data or Information) Rules, 2011 ("**SPDI Rules**"). Rule 5 of the SPDI Rules sets out specific requirements governing the collection, processing, and storage of sensitive personal data by business entities. Further, sectoral regulators such as the Reserve Bank of India ("**RBI**") and the Insurance Regulatory and Development Authority of India ("**IRDAI**") have issued express guidelines governing the processing of personal data in the sectors concerned.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside India subject to compliance with the SPDI Rules. Rule 7 of the SPDI Rules allows business entities to transfer personal data outside the Indian jurisdiction given when: (i) it is in furtherance of a lawful contract between the data receiver and the data provider; and (ii) the data provider has expressly consented to such data transfer, under the condition that the data receiver must ensure the same levels of data protection as stipulated under the SPDI Rules.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The SPDI Rules touches upon the aspect of information security in Rule 8, wherein certain '*reasonable security practices and procedures*' are to be followed by a corporate body to ensure stringent information security practices are set out. Briefly, these practices include obtaining an *'IS/ISO/IEC 27001' certification on "Information Technology – Security Techniques – Information Security Management System – Requirements"*, getting the codes and practices on information security approved and audited by an auditor approved by the Central Government, etc.

Additionally, once the DPDP Act is enforced, data fiduciaries (equivalent to data controllers under the GDPR) would be mandated to implement "*appropriate technical and organisational measures*", as well as "*reasonable security safeguards*" to reinforce information security practices and minimise the occurrences of potential data breaches.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Indian laws do not permit the transfer of employees as part of an outsourcing transaction or other technology-related service. That said, Section 25 FF of the Industrial Disputes Act, 1947 ("ID Act") provides for the transfer of employment of "workmen", typically including blue-collar workers (*defined under Section 2(s) of the ID Act*),[1] upon the transfer of ownership or management of an industrial undertaking if the following conditions are met:

- service of the workmen are not interrupted by the transfer;
- the terms of service are no less favourable than prior to the transfer; and
- the new employer ensures continuity of service is uninterrupted by the transfer for the purposes of computing retrenchment compensation in the event of termination of the workman.

Therefore, even if the contract between the parties in a technology-related outsourcing transaction includes a provision concerning the transfer of employees, it shall not be treated as a *per se* right and will be subject to the discretion of the

employees and their consent to such transfer, in addition to the aforementioned requirements under the ID Act, as the case may be. In the case of non-workmen employees typically including white-collar employees, the new employer must also consider any collective bargaining agreements that may be established with these employees in relation to their employment transfer.

6.2 What employee information should the parties provide to each other?

There are no specific laws or regulations in India that govern specific employee information for parties to shares under a commercial arrangement. Typically, only such employee information that is essential for the performance of a service under a contract such as educational credentials, identification proof, training qualifications, etc., is ideally provided by a party to the service provider. If such information is required to be transferred electronically, then the parties must ensure compliance with the requirements of data transfer as regulated by the Information Technology Act, 2000 (*and the SPDI Rules*), and the DPDP Act (*once enforced*).

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Termination of employees by the service provider or the customer in an outsourcing transaction is generally governed in accordance with the terms of the contract between the parties. From the lens of the service provider, reasonable reasons for the termination or dismissal of employees may include termination on grounds of role redundancies, financial constraints, or acts of fraud, misconduct, wilful negligence, or any material breach of the terms of employment by the employees. Whereas, from the customer's perspective, the customer may be entitled to terminate the employees in accordance with the contract executed by the customer with the service provider or in accordance with the general statutory principles of Indian employment laws as discussed hereunder.

Concerning the termination of workmen under the ID Act, the service provider must adhere to the conditions under Section 25 FF of the ID Act and shall ensure to pay all accrued statutory entitlements to the workmen along with adequate retrenchment compensation upon dismissal (*as applicable*). Termination of non-workmen employees and cases where a formal contract of employment may not be in existence are governed under the state-specific shops and establishment regulations ("**S&E Regulations**") that generally provide for the requirement of serving a one-month prior notice to the employee being terminated or providing compensation *in lieu* of the notice. In the context of employee termination, Indian courts have consistently upheld that the contract between the parties shall supersede the S&E Regulations if it accommodates more beneficial provisions in the interest of the employee.

Further, arrangements where contract workers are outsourced may trigger the applicability of the provisions of the Contract Labour (Regulation & Abolition) Act, 1970 ("**CLRA Act**") that may impose specific registration and filing requirements on both the service provider (*as the contractor*) and the customer (*as the principal employer*). The CLRA Act places the burden of meeting all contract worker-related compliances on the contractor's shoulders; however, judicial precedents indicate that in cases where the contractor fails to comply with its obligations under the CLRA Act, the principal employer may be held vicariously liable for the contractor's inaction.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Indian labour courts have held that employees who consent to their transfer of employment shall be entitled to better or at least equal terms of service compared to their employment in their former establishment. While any enhancement or harmonisation of the terms of employment is welcome, any unreasonable cutbacks are often prohibited.

Moreover, as indicated in our response to question 6.1 above, for any harmonisation of the terms of employment in relation to the transfer of employment of an individual classified as a 'workman' under the ID Act, the service provider should ensure compliance with the requirements specified under Section 25FF of the ID Act. Therefore, no synchronisation of employment terms during the transfer of workmen shall impair or adversely affect their terms of employment hitherto the transfer.

6.5 Are there any pensions considerations?

There are several regulations in India governing the payment of pension and annuity benefits to former employees, such as: the Employees' Provident Funds and Miscellaneous Provisions Act, 1952; the Pension Fund Regulatory and Development Authority Act, 2013 (*governing NPS – the National Pension System*); and several employee welfare schemes concerning pension and annuity benefits issued by the Central Government and the respective state governments. Employment laws in India generally require employers and employees jointly and severally liable for making any statutory/voluntary pension contribution, as applicable. In the context of an employee being transferred, the new employer shall be responsible for liaising with the former employer/employee to effectively reassign the credentials of the pension fund account of such employer to ensure a seamless transition and the continuance of pension contributions.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Like as indicated in the aforementioned responses, there are no employment regulations in India governing the transfer of employment in offshore outsourcing transactions. All outshore employee transfers in connection with an outsourcing transaction shall solely be subject to the discretion of the transferring employees, and the employers shall be responsible for ensuring all labour-law-related compliances in both jurisdictions. A key consideration regarding offshore employee transfers is to ensure that the labour laws of both jurisdictions are in parity or are inclined towards the benefit of the transferred employees.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

While there are no overarching laws or regulations specifically regulating outsourcing transactions in India, sector-specific regulators like the RBI have issued directions regulating outsourcing transactions by regulated entities ("**REs**") in the information technology sector and the financial services sector.

The RBI issued the "*Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023*" in April 2023 and subsequently, the "*Draft Master Direction – Reserve Bank of India | Managing Risks and Code of Conduct in Outsourcing of Financial Services) Directions, 2023*" in October 2023. Both of these directions aim to regulate the framework of outsourcing transactions by REs that include commercial banks, non-banking financial companies ("**NBFCs**"), credit information companies ("**CICs**") and specified cooperative banks. The underlying principle behind both of these directions was to regulate REs in a manner that allows them to fulfil their contractual obligations in the aforementioned sectors without impeding the supervision of the RBI.

Akin to RBI, other sectoral regulators have also established specific norms and regulations for regulating outsourcing transactions in their respective sectors. Illustratively, IRDAI has established the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 and the Securities Exchange Board of India ("**SEBI**") has issued a circular on "*Guidelines on Outsourcing of Activities by Intermediaries*" in 2011; these regulate outsourcing transactions in the insurance and securities market sector respectively.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Typical structures observed in outsourcing transactions in India include as follows:

(i) **Turnkey contracts**: Contracts where the contractors are responsible for the entire project including the designing, building, and delivering of a fully operational system or service to the client. These contracts minimise the client's involvement in the execution process and shift the liability to the shoulders of the contractor.

(ii) **Third-party outsourcing**: Similar to turnkey outsourcing, third-party outsourcing involves getting into a contractual arrangement with an external organisation to perform specific services or business functions. This arrangement benefits the client company by leveraging the requisite expertise, efficiency, and resources of the third-party provider while maintaining broader project oversight. Contrary to turnkey outsourcing which offers an end-to-end solution, third-party outsourcing involves delegating specific tasks that are generally performed in-house, thereby allowing the client to focus on the core activities. Third-party outsourcing is generally executed via the following contractual arrangements:

  (a) *Service Level Agreements* ("**SLAs**"): Detailed contracts that specify the exact nature of services to be provided and often include performance metrics, quality standards, and fixed timelines. SLAs generally include milestone-based incentives and penalties for non-compliance to ensure the consistent expectations of the client.

  (b) *Master Service Agreements* ("**MSAs**"): Comprehensive legal contracts that outline the overarching terms and conditions of the outsourcing relationship between the parties. MSAs include detailed aspects including, without limitation, the scope of services, payment terms, confidentiality obligations, intellectual property rights, liability limitations, dispute resolution frameworks, etc. MSAs serve as the bedrock of individual service orders or statements of work that detail specific project requirements of the client.

  (c) *Subcontracting agreements*: These are used when a portion of the contracted services are outsourced to another vendor by the primary service provider. These agreements frequently delineate the specific duties, performance standards, and responsibilities of the subcontractor, as well as the primary contractor's obligations in connection to the subcontracted services.

(iii) **Outsourcing Framework Agreements**: Umbrella agreements that lay down the general principles and guidelines governing the outsourcing relationship between the parties. These agreements are fundamentally designed to cater to multiple outsourcing arrangements and the specific terms and conditions of each project are listed in separate task orders/project agreements issued under the broader framework, thereby allowing flexibility and scalability in the outsourcing engagement.

(iv) **Build-Operate-Transfer ("BOT") Agreements**: These are best suited for commercial arrangements where the service provider is responsible for building a facility or developing a service, subsequently operating it for a predetermined period, and eventually transferring it to the client. BOT Agreements incorporate provisions relating to the construction and operational levels, performance benchmarks and the conditions for the transfer to allow a seamless transfer of ownership and operational responsibility.

(v) **Joint Ventures ("JVs")**: JVs involve the creation of a new corporate entity by two or more parties to provide outsourcing services. JVs allow leverage to the parties involved in such JV in sharing risks, investments, and profits arising out of the outsourcing transaction. A JV structure fosters collaboration and joint management of the outsourced functions and typically enshrines the contributions of each party, governance structures, profit-sharing mechanisms, and exit strategies.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Service levels and service credits are essential components of an SLA in any technology outsourcing arrangement. Service levels indicate the key performance indicators that providers are reasonably expected to adhere to in achieving or exceeding the levels specified in the contract. The common metrics that often form part of service levels in a technology outsourcing transaction may include the availability or uptime of the service, the incident response time for addressing issues, the complete resolution time from the commencement of the issue, and other throughput and performance metrics such as processing speed, data handling capacity, user load management, etc.

Regarding service credits, they are a form of monetary penalty on the service provider for its failure to achieve the specified service levels. While service credits can be offset against any contractual damages upon the client initiating any proceedings resulting in the award of damages, optimally, service credits shall be defined independently in the SLA and should not be clubbed together with other penalties or liquidated damages. SLAs also oftentimes incorporate variable fee component provisions concerning service credits.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Mainstream charging mechanisms in technology outsourcing transactions include:

(i) **Fixed price ("FP") model**: As the term suggests, in this model, the customer pays a fixed fee for a specified amount of IT services utilised. The FP model is frequently observed in outsourcing transactions where companies execute contracts with external vendors to provide specific IT services over a long-term period.

(ii) **Cost-plus pricing model**: In this model, the end customer is charged for the actual cost of the IT services in addition to a profit margin or a markup percentage comprising any additional labour, materials, and other overhead expenses involved.

(iii) **On-demand pricing model**: A model wherein the customer pays for the IT services on an '*as-required*' basis *in lieu* of paying a predetermined fee on the set amount of services. This model is cost-effective and optimal for enterprises that require IT services irregularly or contingently. Cloud service providers often utilise the on-demand pricing model for their services.

(iv) **Time and materials ("T&M") model**: This charging framework relies on billing the end user based on the actual time and materials (e.g. hardware, software licences, etc.) that were required to complete a particular project. This arrangement is oftentimes observed in long-term IT projects, executed vide a BOT agreement.

(v) **Shared risk-reward pricing model**: A model that allows the customer and the vendor to share the risks and the rewards associated with the IT services concerned. This model can be further amalgamated with the T&M, FP, and other profit/revenue sharing-based models.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

All formalities involved in the transfer of third-party contracts to a service provider in an outsourcing transaction would originate from the terms of the contract executed between the parties concerned. If the contract expressly allows for its assignment, then the transfer of the contract would be permissible, subject to any prior approval of the parties for such assignment, as required. In most cases, the transfer of certain rights often results in the execution of a tripartite arrangement between the parties to the original arrangement and the third-party service provider.

In addition to an assignment clause, creatively drafted contracts can impose further formalities administering the transfer such as prior notification for assignment, conducting due diligence, documentation and record-keeping requirements, etc. It is also pertinent to note here that in some cases, the assignment may be substituted with a 'novation' clause that requires all parties to enter into and execute a new contract altogether wherein the third-party service provider will assume full responsibility for the contractual obligations emanating from the prior contract.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

To accurately assess the tax implications arising out of an outsourcing transaction, there should be a thorough evaluation of the transaction structure and the characteristics of the assets involved in the transaction. A few legal issues that may arise in an outsourcing transaction in India include: (i) determining the applicability of Goods and Services Tax ("**GST**") on the services provided by the service provider and identifying the place of supply to determine the appropriate GST jurisdiction and compliance requirements; (ii) carefully examining and availing the provisions of Double Taxation Avoidance Agreements ("**DTAAs**") if the service provider is a non-resident and is based out a country with whom India has entered into a DTAA; (iii) assessing whether the activities of a foreign service provider in India constitute a permanent establishment ("**PE**") under the Income Tax Act, 1961 ("**ITA**"); (iv) ensuring that the pricing of inter-company transactions between any related entities adheres to the arm's length principles under Section 92 of the ITA; (v) certifying withholding tax deductions when employees are involved as part of the outsourcing transaction; and (vi) streamlining the perplexing tax compliance and reporting requirements to ensure prompt regulatory compliance and avoiding any unwarranted penalties and interest.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Some key issues worth considering when licensing software for installation and use on on-premise solutions include: (i) evaluating the extent of usage rights, timelines for use, and usage restrictions; (ii) cost and licence fee considerations; (iii) complying with data handling and data security practices to ensure compliance with the Information Technology Act and the SPDI Rules; (iv) ensuring that customers are indemnified against claims of intellectual property infringement; (v) validating the credibility of technical support including prompt response times and service levels; and (vi) determining the requirement of a source code escrow provision in the licensing agreement to safeguard the customer's access to the software in critical situations.

In addition to the above, another crucial consideration for the customers is to ensure that the software vendor possesses the necessary intellectual property rights and registrations in India to license the software. Albeit Indian laws offer protection to IP irrespective of its registration (excluding designs), registration is recommended to enforce the IP as *prima facie* evidence of goodwill in court and forms a crucial element in passing off.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Some key issues worth considering when procuring support and maintenance services for software installed on customer systems include: (i) ensuring that the contract (SLA) clearly specifies the availability of the service and the mode of service delivery (remote/on-site/both); (ii) ensuring the contract lays down a clear definition of 'fault'/'defect' in the relevant software; (iii) ensuring the contract stipulates appropriate service levels and a service credit framework, as applicable, along with a categorisation of the severity of the faults; (iv) ensuring if local support is available to facilitate prompt and effective service; and (v) determining whether the vendor will have access to personal data processed by the software during the tenure of the services and whether the instant contractual arrangement conforms with the data protection laws including

the Information Technology Act, 2000 (*read with the SPDI Rules*) and the DPDP Act (*once enforced*).

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Software escrow arrangements are not generally the norm in India. Having said that, it has been observed that large organisations do tend to enter into such arrangements with foreign organisations where the size of the business is considerable. Software escrow arrangements are gaining traction in India since they offer licensees the opportunity to protect their interests and rights accruing out of the software licensing agreement while simultaneously allowing the licensor (vendor) to market its software products and services.

One of the primary objectives of a software escrow arrangement is to ensure that licensees can maintain and support the software in case the licensor is unable to do so, generally due to bankruptcy, discontinuation of support, or breach of the contract. Therefore, the very purpose of an escrow arrangement in the first place is to ensure protection against any unforeseeable risks of bankruptcy/insolvency of the licensor. An event of bankruptcy/insolvency of the vendor may trigger the release of the escrowed source code, which may be contested by the licensor. Therefore, in order to ensure any revenue losses or a loss of customer confidence due to interruption of services arising from a disputed software escrow arrangement, parties shall clearly establish the jurisdiction and dispute resolution framework in the contract along with adequate considerations concerning the bankruptcy statutes in the jurisdiction where the vendor is situated.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

In 2014, MeitY introduced "*MeghRaj*", which is national government cloud initiative portal to promote the benefits of cloud computing and streamline cloud computing processes. Further, MeitY has also empanelled the cloud service offerings of prominent cloud service providers ("**CSPs**") to facilitate cloud procurement for governmental departments. In connection with procurement of cloud computing services, MeitY subsequently released: (i) "*Guidelines for Procurement of Cloud Services*" to highlight the key responsibilities of governmental departments and empanelled CSPs, managed service providers ("**MSPs**"), and system integrators ("**SIs**"); and (ii) a template of the master service agreement on the procurement of cloud services to enshrine an effective contractual structure to deal with the risks and challenges associated with the public procurement and consumption of third party cloud services.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

As per NASSCOM, the Indian tech industry currently employs approximately 5.43 million people and therefore, the scope of the use of optimal computing technologies like cloud computing is of paramount significance in the Indian technological landscape.[2] Despite the arduous economic conditions, the Indian cloud market has positively witnessed leading cloud service providers like Amazon Web Services and Google Cloud investing extensively into the Indian market. The International Data Corporation ("**IDC**") reports that the Indian public cloud services market has a combined revenue of approximately USD 3.8 billion. Further, IDC estimates that the Indian public cloud services market could grow to USD 17.8 billion by 2027, with a CAGR of 22.9% for 2022-27.[3]

9.3 What are the key legal issues to consider when procuring cloud computing services?

There exist several challenges from a legal perspective that affect the procurement of cloud computing services in India. The fundamental challenge arises due to the lack of any explicit norms and regulations governing private sector procurement in cloud computing and other similar services and products. Some other key issues include: (i) the diverse Indian procurement landscape that ranges from small-scale local suppliers to multinational vendors; (ii) operational complexities for transitioning from legacy procurement systems and processes; (iii) data privacy and security considerations affecting cloud management systems upon the enforcement of the DPDP Act; (iv) scalability issues for increasing data volumes and transactions on the cloud; and (v) sector-specific data localisation norms for financial data, health data, etc.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

Barring the Indian state of Tamil Nadu which released the "*Safe & Ethical Artificial Intelligence Policy*" in 2020 wherein the State Government briefly touched upon the aspect of procurement related to AI solutions/systems for government procuring agencies in Tamil Nadu, as of today, India does not have any national laws or regulations regulating the procurement or use of AI-based technologies.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

In the absence of the enforcement of the DPDP Act, the regulation and processing of any form of digital personal data (including any digital personal data used to train machine learning-based systems) are governed under the extant provisions of the Information Technology Act, 2000, read with the SPDI Rules. As both legislations specifically govern 'personal data', Indian regulations remain silent on regulation of any 'non-personal' data, including any non-personal data involved in the training of machine learning technologies in India. Notwithstanding the aforementioned, MeitY released the "*India Data Accessibility and Use Policy*" in 2022 to regulate non-personal data available in the public sector for all data and information created/generated/collected/archived by the Central Government and allowing the respective State Governments to freely adopt the policy and protocols enshrined under the 2022 policy.

Further, the ownership of such data remains unclear and should ideally depend on several factors including the nature, source, usage and disclosure of such data, and its conformity with any confidentiality or intellectual property protections under the Copyright Act, 1957 (as Indian law recognised

copyright protection for databases) and other applicable laws, or any specific contractual provisions governing the ownership of such data. Likewise, the renewal of any such data used for training any machine learning-based systems could be licensed contractually.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Algorithms under the Indian patent law, governed by the Patents Act, 1970 are excluded from the purview of being patentable by virtue of Section 3(k) of the Patents Act, unless any algorithm is inherently attached to a patentable invention. So far as the Copyright Act, 1957 is concerned, the act intends to protect the expression of an idea and not the idea itself and it specifically excludes ideas, procedures, processes, systems, method of operations, concepts etc., from the purview of Copyright law. Since an 'algorithm' can be generally categorised as a set of rules or procedures, it cannot be granted protection under Indian copyright law.

In addition to the aforementioned considerations, originality and novelty are some of the fundamental tenets of Indian intellectual property laws and as of now, Indian law does not recognise artificial intelligence as a rightful author for vesting it with the protections available under Indian intellectual property laws. Therefore, the question regarding the ownership of algorithms and IP created by generative artificial intelligence technologies such as large language models ("**LLMs**", e.g.: ChatGPT, Google Gemini), text-to-image models (e.g.: DALL-E) and other similar AI technologies, without any form of human intervention, remains largely unsettled until any further developments are incorporated in the extant intellectual property laws of India.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

As of now, and as indicated in our earlier responses to questions 1.1 and 1.2, there are no specific laws or regulations in India that govern the procurement of blockchain-based technologies in India. That said, India is actively recognising the role of blockchain technologies including cryptocurrencies and virtual digital assets ("**VDAs**") in particular. In January 2020, NITI Aayog (*the National Institution for Transforming India, a policy think tank of the Indian government which provides inputs on implementing national programmes and policies in India)* released a discussion paper titled "*Blockchain: The India Strategy, Part 1*", wherein it discussed how government institutions can effectively leverage blockchain-based technologies. NITI Aayog's discussion paper also mentioned that the subsequent editions would include suggestions on the procurement of blockchain technologies but to no avail.

MeitY followed in the footsteps of NITI Aayog and released the "*National Strategy on Blockchain*" in January 2021, later revising it in December 2021. In this strategy paper, MeitY identified 44 potential areas of utilising blockchain solutions and laid out the fundamental contours of how the technology could be leveraged across the various sectors. Unfortunately, however, the MeitY's strategy paper remains silent on the aspect of the procurement of blockchain-based technologies and solutions in India.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

India has shifted from a flat-out antagonistic approach in the past to more of an implicitly hostile regulatory shift towards blockchain technologies, particularly concerning blockchain technologies including cryptocurrencies, non-fungible tokens ("**NFTs**"), and VDAs. While no standalone regulations have been formulated yet, the national tax regime was amended in 2022 and tax laws witnessed the introduction and taxation of VDAs. Furthermore, the recent amendments to the Prevention of Money Laundering Act, 2002, to bring cryptocurrency under the purview of India's anti-corruption and money laundering laws signify the Indian government's vision to regulate the blockchain.

So far as the adoption of blockchain technology in India is concerned, some states have meticulously integrated blockchain technologies in an array of diverse sectors. For instance, the West Bengal government has adopted NFTs for the representation of land mutation purposes. Likewise, Uttar Pradesh has launched a public grievance management system in association with Polygon that allows users to transparently file and track complaints against corrupt public officials. Furthermore, key sectoral regulators like SEBI and the Telecom Regulatory Authority of India ("**TRAI**") have instructed their subordinate regulated entities to commence incorporating blockchain technology into their existing infrastructure.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Some of the fundamental legal issues that may arise during the procurement of blockchain-based technologies may include, without limitation: (i) recognising the exigency for actionable regulatory mechanisms to enable the deployment of scalable blockchain technologies in both the public and private sectors; (ii) tackling the issues of jurisdiction and liability, given the anonymity of parties engaged in a blockchain transaction due to the decentralised nature of the technology; (iii) assessing the legal recognition and enforceability of smart contracts for procurement, which are self-executing contracts coded on the blockchain; (iv) enforcing standardised contractual considerations while drafting and negotiating contracts dealing with the procurement of blockchain technology by blockchain technology vendors/service providers; and (v) harmonising the procurement of blockchain technologies with the competition/antitrust regulatory regime in India due to the fact that the availability of a colossal amount of information on a blockchain network may facilitate the exchange of commercially sensitive information, thereby abetting the adoption of anti-competitive practices prohibited under the Competition Act, 2002.

Endnotes

1 The test under Indian law to ascertain if an employee is a workman or non-workman is that if an employee is employed in a managerial or administrative or supervisory capacity drawing remuneration exceeding INR 10,000 per month, such employee would be a non-workman, otherwise he would be a workman. Whether an employee is a workman or non-workman is a matter of fact which can be determined on the basis of the nature of duties of the employee and his job description.

2 "Technology Sector in India: Strategic Review – 2024", National Association of Software and Service Companies ("**NASSCOM**") (February 2024).

3 "Worldwide Semi-annual Public Cloud Services Tracker", International Data Corporation (14 December 2023).

Harsh Kumar is the Founding and Managing Partner of Kaizen Law. He is a seasoned transactional lawyer with over 19 years of experience in complex, high-value transactions involving domestic and cross-border investments and acquisitions. His area of expertise lies in mergers and acquisitions of listed and unlisted companies, and private equity and venture capital transactions. He has served diverse clients, including top Indian corporates, MNCs, start-ups, and unicorns across various industries, including manufacturing, healthcare, pharmaceuticals, e-commerce, logistics, IT services, and new-age sunrise sectors. He also provides external advisory services to companies on commercial and contractual matters. Harsh has previously worked as a partner in Cyril Amarchand Mangaldas and Shardul Amarchand Mangaldas.
Harsh's legal prowess has been acknowledged by Indian and international publications, solidifying his position as a leading lawyer. His professional journey also took him to the London office of Herbert Smith Freehills LLP, where he worked on international corporate law transactions. *Legal500.com* named Harsh a prominent lawyer in the corporate practice of M/s Shardul Amarchand Mangaldas in 2019 and 2020, further highlighting his expertise in the field.

Kaizen Law
4th Floor, Spring House Plot No. 2
Golf Course Road Sector 43
Gurugram, Haryana, 122011
India

Tel: +91 9999 1916 20
Email: harsh.kumar@kaizenlaw.in
LinkedIn: www.linkedin.com/in/harsh-kumar-62a6b38

Indraneel Chakraborty is an Associate and part of the dynamic team at the Gurgaon office of Kaizen Law. He is a prominent representative of the Technology and Data Protection team at Kaizen Law, with his expertise rooted in niche subject areas such as artificial intelligence, big data, blockchain, and cloud computing. Indraneel also specialises in providing counsel on issues related to the information technology, data breaches, data transfers, use of cookies and online tracking, privacy policies, and the terms of use.

Kaizen Law
4th Floor, Spring House Plot No. 2
Golf Course Road Sector 43
Gurugram, Haryana, 122011
India

Tel: +91 8406 9497 76
Email: indraneel.chakraborty@kaizenlaw.in
LinkedIn: www.linkedin.com/in/indra-neel

Founded in 2022, Kaizen Law is an independent law firm based in Gurgaon, India, offering comprehensive legal advisory services on transactional matters and technology law. Kaizen Law has recently set-up another office in Bangalore, India. Our expertise encompasses private equity, early-stage and late-stage venture capital, mergers and acquisitions, and exit financing transactions. We pride ourselves on providing legal advice on complex to routine matters with utmost efficiency and timeliness. Our clientele spans large Indian conglomerates, blue-chip Indian and global companies, multinational corporations, regulated institutions, investment funds, and entities functioning in the new age and technology services sector. In the past year alone, we have played a pivotal role as legal advisors in more than 20 transactions, collectively valued at approximately USD 2 billion.
Rooted in the Japanese philosophy of kai 改 and zen 善, signifying "change for the better" or "continuous improvement", Kaizen Law distinguishes itself from its competitors through personalised service and an unwavering commitment to understanding our clients' deal drivers. Clients have applauded us for our industry-focused competencies, comprehensive understanding of Indian technology laws, including entities functioning in regulated sectors, and our dedicated emphasis on continuous training of our legal team. Our goal remains to offer quality legal advice while responding with the legal creativity and agility expected by sophisticated clients. With over 12 team members having a rich experience working with leading Indian firms, we are committed to delivering pragmatic, business-oriented solutions that clients can trust.

https://kaizenlaw.in/

Kaizen Law

Japan


Yuko Tashiro


Kenji Sugiura


Naotaka Yamashiro


Kosuke Sakata

STORIA Law Office

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

There are no specific regulations for the private sector procurement of technology products and services in Japan. However, on September 13, 2022, the Japanese government publicly released the "Guidelines on Respecting Human Rights in Responsible Supply Chains" to encourage companies' initiatives to respect human rights. Although these Guidelines are not legally binding, they cover all business entities engaging in business activities in Japan and the Guidelines' scope includes both upstream and downstream supply chains and is not limited to direct business entities. Business entities are required to avoid causing or contributing to any negative impact on human rights arising from their business activities and to prevent or mitigate any negative impact by formulating their human rights policies and conducting human rights due diligence.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Government procurement in Japan is regulated for the purpose of ensuring transparency and competitiveness in government procurement by the Public Accounting Act (Act No. 35 of 1947), the Cabinet Order on Budgets, the Settlement of Accounts, and Accounting (Imperial Order No. 165 of 1947), and the Regulations for Contractual Business Transactions (Ministry of Finance Ordinance No. 52 of 1962), among others, with respect to the procurement procedures of governmental bodies. For procurement to which the WTO's Agreement on Government Procurement applies, the procurement procedures under the WTO Agreement on Government Procurement and other international agreements are ensured under Japan's domestic laws and regulations through the establishment of cabinet orders and ministerial orders. In addition, procurement by bodies other than governmental bodies is regulated by the Local Autonomy Act, the Act on Special Corporations, and the Act on Regional Incorporated Administrative Agencies, and their respective related cabinet orders.

For reasons such as safety and reliability in governmental bodies, there are procurement guidelines for each government body that specify a list of requirements that target specific products or services in the following fields: IT products; cloud services; telecommunications products and services; and medical technology products and services. In addition, as a cyber security measure for national administrative agencies, the Manual for the Formulation of Security Requirements in the Government Procurement of Information Systems has been created and procured products and services must meet certain technical requirements and supply chain risk assessments.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

There are no particular Japanese laws or regulations imposing any minimum or maximum term for a contract for the supply of technology-related solutions and services.

However, if such technology-related solutions and services are provided in the form of worker dispatching services, the term for dispatch of a worker in the same workplace cannot exceed more than three years in principle (Act on Securing the Proper Operation of Worker Dispatching Businesses and Protecting Dispatched Workers Articles (**AWDB**) 35-2, 40-2). After that period, the operator of the worker dispatching the services must take measures to stabilise the employment of dispatched workers, including offering a labour contract (AWDB, Article 30).

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

In general, a contract can be terminated by giving notice within a reasonable period to cure the breach (Civil Code, Article 541).

However, a party can terminate a contract without giving any advance notice if (Civil Code, Article 542):

(a) the performance of the entire contract by the breaching party is impossible;

(b) the breaching party unequivocally manifests its intention to refuse performance of the entire contract;

(c) (i) performance of a part of the contract by the breaching party is impossible or the breaching party unequivocally manifests its intention to refuse performance of a part of the contract, and (ii) the performance of the remaining part of the contract does not satisfy the purpose of the contract;

(d) one of the purposes of the contract is frustrated due to late performance by the breaching party, considering the nature of the contract or the manifestation of the parties; or

(e) any party breaches the contract and it is obvious that performance satisfying a purpose of the contract is unlikely to be rendered by the breaching party, even if the other party provides advance notice.

Furthermore, a party can terminate a contract without any advance notice if it is agreed in the contract.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

There are general rules requiring that rights and duties must be exercised or performed in good faith (Civil Code, Article 1(2)) and that no rights can be abused (Civil Code, Article 1(3)).

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

If one party breaches a contract, the non-breaching party can terminate the contract (Civil Code, Article 541 or 542) and/or claim compensation for damages (Civil Code, Article 415).

Furthermore, if the contract is a sales contract or contract for work, and goods or services that are delivered are non-conforming in terms of their nature, quality or quantity, in addition to the remedies described above, a customer may also demand:

(a) full performance of the obligations, such as repair, replacement or filling the shortage (Civil Code, Articles 562 and 559); or

(b) a reduction of the consideration in proportion to the value of the non-conformity (Civil Code, Articles 563 and 559).

However, these supplier responsibilities are often limited, as permitted by law, in contracts related to technology-related solutions or services.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

As mentioned above, contracts for technology-related solutions or services often have a provision limiting the supplier's obligation, as permitted by law, because of the higher bargaining power of suppliers. However, some contracts provide the following remedies:

(a) indemnity for infringement of a third party's rights;

(b) termination rights without notice or the customer in cases of material breach by the supplier or the supplier's insolvency; or

(c) service credits for the customer for a breach of a "service-level agreement".

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

In a case of termination due to breach of contract, it is unlikely that the party terminating the contract will be responsible for any damages incurred by the party that has breached the contract, since the termination of the contract will be attributable to the breaching party. However, it is common to clarify that the terminating party has no responsibility for exercising its termination right due to the counter party breaching the contract.

2.7 Can the parties exclude or agree to additional termination rights?

Yes. It is common that parties specify the grounds for termination in the contract, such as a change of control, insolvency or *force majeure*.

In some cases, parties can also exclude termination rights in principle. In business-to-consumer (**B2C**) contracts, however, waiving consumer termination rights and providing that a business has sole discretion over termination are invalid (Consumer Contract Act (**CCA**), Article 8-2).

2.8 To what extent can a contracting party limit or exclude its liability under national law?

As mentioned above, in technology-related contracts, it is common to limit or exclude suppliers' responsibility. However, in B2C contracts, a provision is invalid if it (i) wholly exempts the business from its responsibility for damages incurred by consumers, (ii) partially exempts the business from its responsibility for damages incurred by consumers due to the business's gross negligence or wilful misconduct, whether the claim is based in contract or on tort (CCA, Article 8), or (iii) is ambiguous as to whether it applies only to the business's ordinary fault, not to its gross negligence or wilful misconduct (CCA, Article 8-3).

Even in business-to-business (**B2B**) contracts, some courts find that a provision limiting or excluding a party's liability for damages caused by the party's gross negligence or wilful misconduct is invalid.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

In general, parties agree to a financial cap on their respective liabilities under a contract.

However, as mentioned above, in the case of B2C contracts, any provision partially exempting a business from responsibility for damages incurred by consumers due to the business's gross negligence or wilful misconduct is invalid (CCA, Article 8). Similarly, in B2B contracts, some courts have ruled to invalidate a provision setting a financial cap on either party's liability for its gross negligence or wilful misconduct.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

Mostly, no. The answers to questions 2.1–2.9 are general and may equally apply to items (a)–(e) above.

Exceptionally, some contracts for the procurement of AI-based solutions are regarded as Quasi-Mandate contracts (Civil Code, Article 656) and therefore the provisions regarding sales contracts or contracts for work (e.g., Civil Code, Articles 562, 563, 559) do not apply.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

In Japan, the most common method of dispute resolution for technology solutions and services contracts is litigation. In such litigation, in addition to the judges, expert advisors with expertise in related areas of technology may also participate.

In addition, alternative dispute resolution (**ADR**) may be selected as a method of out-of-court dispute resolution. However, in Japan, parties usually opt for litigation in court, with ADR opted for less frequently.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In Japan, the intellectual property rights in technology sourcing transactions are generally protected legally by contractual provisions and as patent rights, copyrights, trademarks and trade secrets.

Although the copyright of the source code in a development contract belongs to the creator under Japan's Copyright Act, the copyright can be transferred to the user by contractual agreement, or, if not transferred, a licence is generally granted to the extent necessary to use the developed software in question. In joint development, the contract grants a licence to each party to use the counterparty's existing intellectual property rights only for the purpose of joint development and stipulates the ownership of the intellectual property of the deliverables obtained during joint research. In supply contracts (hardware, services), the customer generally gets a licence to use the supplier's intellectual property rights to the extent necessary for the use of the products or services.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Registration procedures for the transfer of a patent are a requirement for such transfer to be effective (Patent Act, Article 98, Paragraph 1, Item 1). In the case of general succession, the transfer becomes effective simultaneously with the inheritance or merger; however, notification of the general succession event must be made to the Commissioner of the Japan Patent Office without delay. In this case, the notification of the succession is not a prerequisite for the succession to take effect. In the case of a jointly owned patent, none of the joint owners may transfer its share without the other joint owners' consent (Patent Act, Article 73, Paragraph 1).

Although a copyright is transferable by agreement, it must be registered in order to assert it against a third party. Moreover, the moral rights of the author are not transferable.

The effective transfer of a trademark requires both the agreement of the concerned parties to the transfer and transfer registration procedures.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

In Japan, know-how, trade secrets, and other business-critical confidential information are protected under the Unfair Competition Prevention Act (**UCPA**). The UCPA defines a trade secret as "technical or business information useful for business activities, such as manufacturing or marketing methods, that is kept secret, and is not publicly known". The unlawful acquisition or unauthorised use of this information is defined as unfair competition, which is subject to injunction and compensation for damages. Criminal penalties of up to 10 years in prison or fines of up to 30 million yen may be imposed on natural persons for trade secret infringement or up to 1 billion yen for companies.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Under the Act on the Protection of Personal Information (**APPI**), businesses mainly have the following obligations.

(i) Notification or publication after specifying the purpose of use of personal information in advance (APPI, Article 17, Article 21). Personal information can only be handled within the scope of the notified or announced purpose of use (APPI, Article 18).

(ii) In principle, consent must be obtained from the data subject when providing personal data to a third party (APPI, Article 27, Article 28).

(iii) The business must respond appropriately to requests for disclosure or correction of personal data from data subjects (APPI Articles 33–35).

Although the GDPR requires that one of six legally required criteria be met for processing personal data (GDPR, Article 6), the APPI does not have such a requirement. However, the APPI prohibits any use of personal information in a way that may encourage or induce illegal or unjustifiable conducts (APPI, April 19).

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, under certain conditions.

Under the APPI, before transferring personal data to third parties in foreign countries, consent must be obtained from the data subject (APPI, Article 28), except when the transfer of personal data is either (i) to a destination country that is recognised as having the same level as Japan in protecting individuals' rights and interests (e.g., EU or the UK as of 2023), or (ii) to a person or entity that has a system in place that meets the APPI standards (i.e., a person that establishes a system that conforms to standards prescribed by the Order of the Personal Information Protection Commission as necessary for continuously taking measures equivalent to those that a business handling personal information must take concerning the handling of personal data pursuant).

In this way, the APPI regulates the transfer of personal data to third parties in foreign countries by monitoring: (i) the country to which the personal data will be transferred; (ii) the level of the

system of the recipient of the personal data; and (iii) the level of consent from the data subject.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The APPI requires businesses to take necessary and appropriate measures to manage the security of personal data, including the prevention of leakage, loss, or damage of, or to, personal data (APPI, Article 23). The APPI clarifies in its guidelines the details of these security management measures, including taking the institutional security management measures, personnel security management measures, physical security management measures, and technological security management measures, as well as understanding the external environment. As for understanding the external environment, the guidelines require a business, when handling personal data in a foreign country, to understand the system for personal information protection in that foreign country and to take necessary and appropriate measures for managing the security of personal data.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

No. Please see below for a discussion on (a) worker dispatching, and (b) outsourcing separately.

(a) Worker dispatching refers to an arrangement where a licensed dispatch company sends its own employees to work for a client under the client's supervision and instructions. Although a dispatched worker works at the client's place of business under its supervision and instructions, the dispatching company remains the dispatched worker's employer.

(b) Outsourcing refers to a transaction where a subcontractor performs work that it accepts from the outsourcing party. There is no change in the employment relationship between the subcontractor's employees and the outsourcing party; nor is the subcontractor's employees subject to the supervision and instructions of the outsourcing party. If, for any reason, a supervision and instruction relationship is deemed to exist between the subcontractor's employees and the outsourcing party, it would amount to an illegal, unauthorised dispatch business (disguised contracting).

6.2 What employee information should the parties provide to each other?

(a) The AWDB, which was mentioned in Section 2 "General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services" above, requires the dispatching company to notify the client company of (i) a worker's name and gender, (ii) whether the dispatched worker is subject to any agreement, (iii) whether the term of employment is fixed or indefinite, (iv) whether the dispatched worker is 60+ years, and (v) a worker's enrolment status for the purpose of labour and social insurance.

(b) There is no legal obligation to provide employee information in an outsourcing transaction. However, the contract may specify the identity of each party's person-in-charge.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

The employment dismissal restrictions in Japan are extremely strict, even from a global perspective. Dismissals that lack objectively reasonable grounds are invalid and courts are extremely vigilant when determining whether dismissal grounds exist. The treatment of dismissals in (a) worker dispatching, and (b) outsourcing is discussed below.

(a) Worker dispatching: As explained in the answer to question 6.1, an employment relationship is created between the dispatching company and its employee. Whether the dispatching company can dismiss its employee is determined by the strict standard mentioned above. On the other hand, the client company is not in a position to dismiss a dispatching company employee.

(b) Outsourcing: As explained in the answer to question 6.1, an employment relationship is created between the outsourcing party and its employee. Whether the outsourcing party can dismiss its employee is determined by the strict standard mentioned above. On the other hand, the subcontractor is not in a position to dismiss an outsourcing party employee.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

(a) In worker dispatching, the workplace of an employee of the dispatching company is that of the client company. The dispatching company has an obligation to ensure that the treatment of its employees is equal and fair to that of the client company's regular employees.

(b) Unlike with worker dispatching, there are no special legal rules for outsourcing transactions. However, of course, the general rules of the Labor Contracts Act apply and any unilateral changes in employment conditions that are disadvantageous to employees are invalid unless such changes are reasonable.

6.5 Are there any pension considerations?

There is no specific consideration of pensions in relation to outsourcing transactions or other contracts for the provision of technology-related services.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

There are no special offshore outsourcing rules for outsourcing transactions or other contracts for the provision of technology-related services. The explanations in this section also apply to offshore outsourcing.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

The AWDB, which was mentioned in Section 2 "General Contracting Issues Applicable to the Procurement of

Technology-Related Solutions and Services" above, and closely related Employment Security Act are introduced as laws and regulations that regulate outsourcing transactions.

If the outsourcing party is in a superior position to the subcontractor, the regulations concerning abuse of a superior position under the Antimonopoly Act will apply. In addition, the Subcontract Act specifically regulates subcontracting transactions, while the Construction Business Act regulates construction work transactions.

From a similar perspective, the so-called "New Freelance Law", which established rules for placing orders associated with freelance workers who do not belong to any organisation, is set to be enforced on November 1, 2024.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

There are several major legal frameworks and the applicable framework will depend on the nature of the outsourcing. Please see the different categories below.

For outsourcing of personnel, worker dispatching (as described in Section 6 "Employment Law" above) is used.

For outsourcing of work, either a contract agreeing on completion of certain deliverables ("contract for work") or a time-and-material contract under the Civil Code is concluded. In a "contract for work", one party is responsible for a "result" of completing work, such as the production of illustrations, while, on the other hand, in a time-and-material contract, one party is responsible for a "process" of work.

In the outsourcing of software and services, a licence agreement with the program developer and a contract with the service provider (based on the terms of service) are concluded.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

One approach is that the service levels are guaranteed by how the servicers set their Service Level Agreements (**SLAs**) for their users.

The SLAs are expected to include matters such as service availability and response times, notification when a system failure occurs, time required for failure recovery and data backup.

Service credits are compensation for services provided below what is agreed upon in the SLA. Compensation can take the form of a refund or a reduced usage fee in the following month, in an amount commensurate with the lower degree of agreed upon performance.

In addition, there are SLAs that merely impose an obligation to make efforts to meet the Service Level Objective (**SLO**).

7.4 What are the most common charging methods used in a technology outsourcing transaction?

To consider this issue, it is helpful to approach it from the same angle as discussed in the answer to question 7.2.

For personnel outsourcing, a dispatch fee will be charged when a technician is sent through worker dispatching.

For work outsourcing, when content creation or program development is outsourced, fees are often charged for the cost of work on deliverables or based on the amount of time necessary to create deliverables.

Software outsourcing involves software package fees, while service outsourcing involves service usage fees. Service usage fees can take the form of a monthly or annual fee (subscription) or a pay-as-you-go fee based on usage volume.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Under Japan's Civil Code, when one party to a contract wants to transfer its status as a party to the contract to a third party, the consent of the other party to the contract is required.

Many contracts incorporate this Civil Code provision and it is common practice to require written consent from the counterparty prior to a party transferring its status as a party to a contract to a third party.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

In addition to the corporate income taxes and consumption taxes that generally arise in intercompany transactions, the following taxes should also be noted:

(a) Withholding taxes: If the counterparty in an outsourcing transaction is a sole proprietor, such as a freelancer, and if the transaction involves fees specifically stipulated by law (such as manuscripts fees, intellectual property royalties, attorneys' fees, and performers' fees), the outsourcing party is required to withhold taxes from the remuneration paid to the counterparty.

(b) Stamp duty: In the answer to question 7.2 above, we explained that there are two types of outsourcing contracts – contracts for work and time-and-material contracts. In principle, stamp duty is imposed on contracts for works and must be affixed to the contract itself, while stamp duty is not imposed on time-and-material contracts. There are other rules, such as differing tax amounts, depending on whether or not the contract is based on a continuing contract.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

The basic element of a software licence is the grant of the right to use the target software in exchange for the payment of consideration for its use.

As such, the key point is whether the target software meets the needs of the licensee and whether the consideration is appropriate.

It is also necessary to confirm whether it is possible to comply with the conditions set by the developer, such as licence conditions and covenants about the use of the software.

Finally, it is essential to confirm that the software conforms to the licensee's security protocols.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

For on-premises software, unlike cloud services, it is necessary to understand the environment and other aspects of the operating system in which the software is installed.

As such, it is important to consider the following points when procuring software support and maintenance services.

- Whether the customer's environment can be verified (i.e., whether on-site support is available or whether secure remote access to the customer's environment is possible).
- Available days and hours for support.
- Whether there is a clear distinction between free and fee-based support.
- Whether service usage fees are reasonable.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

A third-party organisation called the Software Information Center (**SOFTIC**) in Japan has been providing escrow services since 1997. Nowadays, this system is attracting renewed attention from the perspective of open innovation. In other words, a certain number of large companies use SOFTIC's escrow service to license software from start-ups and other companies to prepare for the risk of bankruptcy of the start-up and other companies.

Similarly, from the perspective of protecting the licensee, the 2020 Copyright Act amendments should also be mentioned. Under the 2020 amendments to the Copyright Act, when the former licensor transfers a licensed work to a third party (the new licensor), the licensee may naturally assert its licensee status under the licence agreement against the new licensor.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

In Japan, there is no law that specifically regulates cloud computing services. However, there are separate guidelines and certification and evaluation systems for cloud computing services.

For example, the Ministry of Internal Affairs and Communications (**MIAC**) has published "Guidelines for Appropriate Settings in Using and Providing Cloud Services". These guidelines describe matters of which users and businesses involved in cloud services should be aware, as well as specific countermeasures for risks and flaws in cloud services. It is advisable for cloud service providers to implement measures that are consistent with these guidelines.

Another example is "ISMS Cloud Security Certification", which is a mechanism to certify a system based on the acquisition of ISMS certification, based on ISO/IEC 27001, to ensure that the cloud service-specific control measures specified in ISO/IEC 27017 are implemented for the provision or use of cloud services included within the scope of ISMS certification. In addition, there is the "Information System Security Management and Assessment Program (ISMAP)", which is a security assessment system for government information systems. Generally, government agencies are required to procure cloud services from among the services listed on the "ISMAP Cloud Services List".

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

In Japan, cloud computing solutions have been widely adopted. According to data from the MIAC, more than 70% of Japanese businesses are already using cloud computing solutions. The purposes of such use include file storage, data sharing, e-mail and internal information sharing.

9.3 What are the key legal issues to consider when procuring cloud computing services?

One of the key legal issues is the cross-border transfer of personal data. Generally, consent must be obtained from the data subject, as mentioned in the answer to question 5.2 (APPI, Article 28), when a cloud computing service provider in a foreign country handles (i.e., processes) personal data.

The second issue is when a cloud computing service provider in a foreign country does not handle personal data. If a contractual clause, for example, stipulates that the cloud computing service provider does not handle personal data and the provider provides appropriate access control, there is no need to obtain consent from the data subject, even when using cloud computing services, but "understanding the external environment" is necessary.

"Understanding the external environment" means that when a company handles personal data in a foreign country, it takes necessary and appropriate measures for the secure management of personal data after becoming familiar with the personal information protection system of the foreign country. This has been newly incorporated into the revised APPI Guidelines.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

In Japan, there are no laws or regulations for the procurement or use of AI-based solutions.

However, various guidelines relating to AI have been published by several ministries and other authorities. For example, MIAC issued two guidelines: "The Draft AI R&D GUIDELINES for International Discussions"; and "AI Utilization Guidelines – Practical Reference for AI utilization". The Ministry of Economy, Trade and Industry (**METI**) released the templates for AI contracts between startup companies and business entities, or between universities and startups from university, in 2020–2021, and "AI company guidelines" in 2024. The latter guidelines indicate the desirable direction for developing and using AI in business situations.

Also, Japan Deep Learning Association (**JDLA**) published a model contract for deep-learning and a guideline for using a generative AI including Large Language Model (**LLM**).

These guidelines are not legally binding, but these are practical resources when drafting contracts or terms and conditions related to data usage in AI and AI development arrangements.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

With respect to copyright issues, using copyrighted data and works for machine learning is acceptable without permission of the copyright holder (Copyright Act, Article 30-4). Holding and collecting data for machine learning is also legal. However, this does not apply if the action would unreasonably prejudice the interests of the copyright owner in light of the nature or purpose of the work or the circumstances of its use: for example, datasets sold in marketplaces shall not be used without payment.

Some data are considered to be "trade secrets" (UCPA, Article 2 (6)) or "shared data with limited access" (UCPA, Article 2 (7)). "Trade secret" is technical or business information useful for a

business and kept secret in one company, and "Shared data with limited access" are provided only to licensees, so other people cannot use such data. If this data is used, a licence contract is needed. The holder of such data can prevent other businesses from using the data for machine learning-based systems if it is set out in the licence contract.

If the data is personal information, the data cannot be used for any purpose other than the purpose set out in the acquisition process (APPI, Article 21(1), 18), and cannot be used in a way that may cause fomenting or inducing an unlawful or unjust act (APPI, Article 19).

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

If works are developed by machine learning techniques without any human involvement, these works are not protected by patent. In the Japanese Patent Act, "invention" is defined as "highly advanced creation of technical ideas utilising the laws of nature" (Patent Act, Article 2 (1)), and "ideas" refers to a human idea.

The source code describing algorithms may be protected by copyright; however, any source code generated without any human involvement is not protected by copyright because it is not a "work". "Work" means a creatively produced expression of thoughts or sentiments by human beings (Copyright Act, Article 2 (1)(i)), so codes generated without any human involvement do not constitute a "work".

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

Generally, no. However, depending on the nature of blockchain-based solutions, there are various laws and regulations in Japan.

If tokens provide revenue sharing with the holder of tokens, these tokens may be subject to Financial Instruments and Exchange Act and other financial regulations. If tokens are issued as a means of payment, the Payment Services Act may apply.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain-based technologies are widely adopted in the financial industry and entertainment industry.

In the financial area, blockchain-based technology is used for sharing identity verification (Know Your Customer), security token offerings, and crypto assets.

In the entertainment sector, Non-Fungible Tokens (**NFTs**) have emerged in sports, music, art and some entertainment industries. People say "NFTs keep the originality of data"; however, in most cases, NFTs only have a URL of the data, called "Off-chain NFT", so it is not an accurate sentence from a legal perspective. Users should pay attention to the actual content of NFTs and to what users can do when they have an NFT.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

The key legal issue is what is represented on the blockchain-based technologies.

As mentioned above, if tokens provide revenue sharing with the holder of tokens, these tokens may be subject to Financial Instruments, the Exchange Act and financial regulation. If tokens are used as a means of payment, the Payment Services Act may apply to them.

If you manage an NFT marketplace, an appropriate Terms of Use showing what is exchanged in this marketplace is needed.

Yuko Tashiro is a partner at STORIA Law Office and specialises in corporate matters including M&A, JV, and financial transactions and other corporate reorganisations and finance matters. She also advises IT, financial, chemical, medical, energy companies and also startup companies.

STORIA Law Office
Otemachi Bldg. 6F, 1-6-1 Otemachi
Chiyoda-ku
Tokyo 100-0004
Japan

Tel: +81 3 6711 5160
Email: yuko-tashiro@storialaw.jp
URL: www.storialaw.jp

Kenji Sugiura is a partner at STORIA Law Office who mainly handles matters involving software app development, platform business, data business and entertainment. Kenji has particular expertise in internet law and the APPI and related laws. Kenji is passionate about promoting new technology and entrepreneurial efforts as a backbone to the new Japanese economy. Kenji is the legal counsel for digital platform consultation desk (for app developers) at METI.

STORIA Law Office
Otemachi Bldg. 6F, 1-6-1 Otemachi
Chiyoda-ku
Tokyo 100-0004
Japan

Tel: +81 3 6711 5160
Email: k-sugiura@storialaw.jp
LinkedIn: www.linkedin.com/in/kenjisugiura

Naotaka Yamashiro is a senior associate lawyer at STORIA Law Office. With his in-depth knowledge and experience regarding intellectual property law, data protection law, e-commerce law, and music and entertainment law, he provides legal advice to numerous companies and independent artists, especially AI vendors, web service providers, and entertainment companies.

STORIA Law Office
Boeki Bldg. 3F, 123-1, Higashimachi
Chuo-ku, Kobe
Hyogo 650-0031
Japan

Tel: +81 78 391 0232
Email: yamashiro@storialaw.jp
LinkedIn: www.linkedin.com/in/naotaka-yamashiro

Kosuke Sakata, a mid-level associate lawyer at STORIA Law Office, possesses a remarkable depth of knowledge in the intricate realms of entertainment, AI technology, and startup investments. Renowned for his meticulous approach, this seasoned practitioner has honed his skills in drafting contracts, including English contracts. His exceptional aptitude extends beyond the mere drafting of legal documents; he possesses profound insights into the practical situations that may arise within these practice areas, thereby offering invaluable perspectives from a legal standpoint.

STORIA Law Office
Boeki Bldg. 3F, 123-1, Higashimachi
Chuo-ku, Kobe
Hyogo 650-0031
Japan

Tel: +81 78 391 0232
Email: k-sakata@storialaw.jp
URL: www.storialaw.jp

STORIA Law Office is a law office that mainly serves clients that use intellectual property and IT as their means to compete in the corporate world. More specifically, we provide legal support for corporations that use intellectual property rights, such as copyright and patent rights as their means of competition (technological intellectual property and entertainment related intellectual property), manufacturing/medical/healthcare/university-launched venture businesses, AI-related business, and IT companies engaged in system development and the provision of web services, and corporations engaged in international activities.

www.storialaw.jp

Madagascar


Hoby Rakotoniary


Fabiola Andriamalala


Hariliva Andriamahefa

John W Ffooks & Co

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, it is not regulated. However, it should be noted that all products and services provided within Malagasy territory must comply with a non-exhaustive list of applicable laws and regulations, in particular Law No. 2015-014 on guarantees and consumer protection (the "Consumer Protection Law), Law No. 2014-038 on the protection of personal data (the "Personal Data Protection Law"), Law No. 2014-006 on combating cybercrime (the "Cybercrime Law), and Law No. 2018-020 amending the competition law (the "Competition Law").

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The public procurement regime of Madagascar does not prohibit the use of innovative and comprehensive contractual techniques whereby the private sector can finance, design, build and operate a public interest infrastructure on behalf of the public entity, the government or public interest infrastructure on behalf of the public entity. The government and public sector bodies tend to resort, however, to public-private partnership contracts or *contrat de Partenariat Public Privé* governed by Law No. 2015-039 on Public Private Partnerships. This means that the main objective of the partnership contract is to combine the resources, skills, and expertise of the public and private sectors to carry out a project or provide a public service. Nevertheless, access to cutting-edge technologies may still be restricted in the public sector, which further encourages the use of such contracts to benefit from the private sector's expertise in the provision of technological goods and services.

Contracts between government entities and suppliers of technology products and services are governed by the law of contracts to ensure the delivery, quality and performance of the products and services.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, Malagasy law does not provide for a minimum or maximum term for contracts for the supply of technology-related solutions and services. The terms of such contracts are generally subject to negotiation between the parties involved and the applicable consumer protection laws can provide additional layers of protection to ensure that consumers receive what they are promised and are not subject to unfair practices, as well as having freedom to negotiate and agree upon the terms and duration of their contracts.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, Malagasy law does not provide for specific regulations governing the length of the notice period required to terminate a contract for the supply of technology-related services.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

No, there are no legal requirements under Malagasy law for a customer and/or supplier of technology-related solutions or services to act fairly or in good faith. However, the Consumer Protection Law may provide additional provisions for protection to ensure that consumers receive what they are promised and are not subject to unfair practices. Furthermore, Article 123 of the General Theory of Obligations or *La Théorie Générale des Obligations* ("LTGO") stipulates that agreements formed in accordance with the law are legally binding. Therefore, the contractors must carry out the agreement in good faith. This

also involves a general duty of fairness and good faith in the performance and enforcement of contractual obligations.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Malagasy law stipulates a range of remedies available to customers when a supplier breaches a contract. Such remedies aim to either enforce the contract or compensate the customer for their losses:

- Compensation for damage: LTGO stipulates that in the event of total or partial non-performance of a contractual obligation or of late performance, the debtor (supplier) must compensate the creditor (customer) for the damage caused as a result of contract breach.
- Compulsory execution: LTGO stipulates that where the debtor (supplier) fails to perform an obligation under the contract, the creditor (customer) may pursue them by any legal means. This may be a court order requiring the supplier to fulfil their contractual obligations or a court order preventing the supplier from certain actions or compelling them to act.
- Termination of contract: LTGO stipulates the injured party may request resolution by mutual agreement or judicial termination of the contract. This gives the injured party the ability to end the contractual relationship as a result of the breach.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In addition to the general legal remedies, additional remedies or protections typically include:

- Warranties and guarantees.
- Indemnification clauses.
- Limitation of liability.
- Data protection and security.
- Dispute resolution.
- *Force majeure*.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

A party can terminate a contract without giving rise to a claim for damages in the following circumstances:

1) Mutual agreement of the parties: a contract may be terminated without invoking a claim for damages if the contract includes an express termination clause. This clause must set out specific circumstances that allow for immediate termination. In such cases, damages are generally not payable, unless the contract specifies that compensation will be due upon termination.
2) *Force majeure*: under provisions of the LTGO, the debtor is released from their obligations if all the required performances become impossible due to *force majeure*.
3) Relative nullity of the contract: Article 101 of LTGO stipulates that a contract may be subject to relative nullity when it sanctions the violation of rules intended to protect a private interest. The injured party may rely on the relative nullity of a contract, which is prescribed five years after the formation of the contract.

Moreover, certain events are typically considered serious enough to justify immediate termination, including instances of a significant breach of contract, situations where performance of the contract becomes impossible, such as *force majeure,* and other limited circumstances.

2.7 Can the parties exclude or agree additional termination rights?

Yes, they can. Parties can exclude or agree additional termination rights based on the principle of freedom of contract. Unless prohibited by law, the parties to a contract can freely agree to exclude certain termination rights. These rights can be interpreted as limiting the liability of the debtor. Article 180 of LTGO stipulates that the parties can expand or limit their contractual liability in advance. They can, for example, limit the cases where the debtor is liable, agree that the debtor will bear the consequences of *force majeure* and acts of third parties, whether or not they constitute *force majeure*, or reduce the amount of damages for which the debtor may be held liable.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Contracting parties generally have some flexibility to limit or exclude their liability, but this must be subject to certain legal principles and limitations and under the condition that the provision is fair, reasonable, and compliant with applicable legal requirements. Indeed, the extent to which a contracting party can limit or exclude its liability is governed by LTGO and other relevant laws. In this regard, LTGO allows parties to limit their liability by agreement unless this limit is not prohibited by the laws of Madagascar. However, there is an exception regarding this limit – the party cannot exempt themselves in advance from all liability or from the consequences of gross negligence or fraud, whether committed by themselves or by the persons for whom they are responsible. It also cannot apply to intentional misconduct or gross negligence.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, under Malagasy Law, parties generally have the freedom to agree on a financial cap on their respective liabilities under a contract on the condition that the cap provision is reasonable, fair and compliant with applicable legal requirements.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

The general principles governing contracts relating to liability, termination, and consumer protection, are applicable across all types of technology procurement contracts, although specific considerations may arise depending on the nature and specific circumstances of each contract.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

In contracts for the procurement of technology solutions and services under Malagasy law, disputes may be resolved using the following main methods of dispute resolution:

1) **Negotiation**
   This is the simplest form of dispute resolution, where the parties attempt to resolve the issue directly between themselves without involving third parties. Negotiation can be informal or structured, depending on the complexity of the dispute.
2) **Mediation**
   Mediation involves a neutral third party, the mediator, who facilitates discussions between the parties to help them reach a mutually acceptable resolution. The mediator does not impose a decision but assists in finding common ground. Mediation is voluntary, and the outcome is non-binding, unless a settlement agreement is reached and signed by the parties.
3) **Arbitration**
   Arbitration is a more formal process where the dispute is submitted to one or more arbitrators who make a binding decision on the matter. Arbitration can be chosen by the parties as the method of resolving disputes in their contract, and the decision of the arbitrator(s) is usually final and enforceable. When a definitive judgement or arbitral award (as the case may be) is pronounced by a competent foreign court or arbitral tribunal and the enforcement of such foreign law, definitive judgment or arbitral award (as the case may be) in Madagascar is sanctioned by an exequatur order by the competent Malagasy court.
4) **Litigation**
   This is the process of resolving disputes through the court system. If the parties cannot agree on another method of dispute resolution or if the chosen method is unsuccessful, they may take their dispute to court. The court will then make a decision based on the evidence and arguments presented by both parties.

In Madagascar, the choice of dispute resolution method can depend on the preferences of the parties involved and the specific terms outlined in the contract. It is common for contracts to specify a preferred method of dispute resolution, such as arbitration, and the details of how disputes are to be resolved, including the selection of an arbitrator or arbitration body.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The intellectual property rights related to technology are mainly protected by Law No. 2017-049 pertaining to the rule of industrial protection in Madagascar. This means that any invention focused on technological fields within the Madagascar territory is protected by this said law. It should be clarified that this law is based on both the Paris Convention of 1883 and the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") signed in Marrakech, Morocco on 15 April 1994. Thus, Madagascar ratified the Marrakech Agreement in 1995 and is required to align its national legislation with the provisions of the TRIPS Agreement relating to industrial property.

Given the territorial jurisdiction of Malagasy law that governs technological inventions, it must be inferred that Malagasy law does not protect the inventions of the other party in a technology sourcing transaction. In addition, it is governed by the principle of the patent of the invention, which allows the declared owner to create, import and offer for trade, sell, or use their invention. All activities that involve the invention but do not have the consent of the registered owner fall into the category of unfair trading and/or piracy and can be punished by the law. Usually, licensing is used in technology sourcing instead of artistic and literary (intellectual) property rights. Hence, the terms of the technology sourcing transaction (period, guarantee of use) must be clear. The provider is bound to provide a working technology but can deliver a licence to other clients. The exception to this is where an exclusive licence is granted. Customers must comply with the normal usage terms in a technology sourcing contract.

The protection benefits both the technology provider and the technology user as it ascertains the authenticity of technology sources and enforces trust in their trade relationship. Madagascar also ratified the "cooperation treaty". The *Office Malgache de la Propriété Industrielle* ("OMAPI") can intervene in case of litigation, or any international matter related to intellectual property.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes. Intellectual property rights are protected by the "patent" of invention. Patent requests must be registered at the relevant office (usually OMAPI). A patent of invention and a certificate of addition are then delivered to the claimant to confirm the ownership of the technology. The finalised patent gives the owner full rights to the invention and prohibits all activities that have not first been approved by the owner (i.e. an unauthorised sublicense contract made by the licensed user, for example).

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Know-how is protected under intellectual property law and under the patent mechanism. In addition, there are some legal provisions that recognise the concept of trade secrets, commercial and professional secrets provided by competition law, and personal data protection law. However, explicit protection other than loyalty and honour is lacking. Otherwise, parties are generally free to insert a confidential clause that will engage both parties for loyalty and confidentiality.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes. As most of the African countries, Madagascar also adopted its own legal framework on the processing of personal data. The Personal Data Protection Law establishes the scope of personal data processing, its limitations, liabilities and enforces protection of the very data subjects. The relevant Malagasy

law also recognises the concept of data processor (*sous-traitant*) and data controller (*responsable de traitement*). Data processing activities are regulated by the consent of the person, moral rules (i.e. dignity and human rights…) and mostly for the protection of the source of the personal data. There are specific provisions relating to the protection of sensitive data.

The *Commission Malagasy de l'Informatique et des Libertés* ("CMIL") is the entity in charge of overseeing, monitoring and approving personal data-related matters. Nevertheless, CMIL has not yet been put in place. Despite initial plans and discussions within the relevant authority, CMIL has not yet been implemented. Several key steps remain incomplete, including the establishment of the necessary infrastructure, allocation of resources, and finalisation of regulatory frameworks. Until these foundational elements are fully addressed, CMIL cannot be considered operational. Therefore, any reliance on its functionality at this stage would be premature.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes. Under the Personal Data Protection Law, it is possible to transfer personal data outside the jurisdiction of Madagascar. However, the transfer is subject to the following conditions:

- the data subject has given their express consent to the proposed transfer, being duly informed of the absence of a similar level of protection;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the execution of pre-contractual measures taken at the request of the data subject;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded, in the interest of the data subject, between the data controller and a third party;
- the transfer is necessary or legally required for the safeguarding of an important public interest, or for the establishment, exercise, or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject; or
- the transfer is made from a public register that, by legislative or regulatory provisions, is intended to provide information to the public and is open to public consultation or any person demonstrating a legitimate interest, provided that the legal conditions for consultation are met in the specific case.

To operate the transfer of data, the country receiving the personal data must yield a similar level of legal protection to – or greater than – that of Madagascar. The legal protection level can be determined based on the nature and duration of processing, the reason for collecting the data and assessing any other processing operations that will be used in connection with the data.

The Personal Data Protection Law stipulates that in the absence of the required legal provisions, the CMIL has the power to deliver authorisation to the recipient country if it grants necessary insurance with regard to the protection of privacy, freedom and fundamental rights. However, this provision presents an issue. Due to the current position of the CMIL, data transactions are limited.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Yes. Article 15 of the Personal Data Protection Law sets out the information security "obligation", which obliges the data controller to ensure the security of personal data under his responsibility by all means necessary in terms of the nature of the data and the risks involved.

This includes protecting the data and processing activities against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access. The data processor is also under the obligation to provide a sufficient guarantee of security and confidentiality. However, with a contract, they can set up an agreement to establish the proportion of liability that each party should assume.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Under the Malagasy Labour Code, employees can indeed be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services. The transfer is subject to conditions that ensure the continuity of employment terms and protect employee rights. Indeed, pursuant to Article 12 of the Malagasy Labour Code, in the event of a change in the legal status of the employer, in particular by succession, sale, merger, conversion of the business, incorporation, concession or lease, all employment contracts in force on the date of the change shall remain in force between the new employer and the employees of the company. In other words, this article stipulates that in the event of a change in the legal status of the employer, such as a transfer, merger, or any other operation including outsourcing transaction, or other contract for the provision of technology-related services, the employment contracts in existence at the time of the change continue with the new employer under the same terms and conditions.

The terms under which the transfer takes place may include:

- Automatic transfer: As said above, the employment contracts of the affected employees are automatically transferred to the new employer. This means the employees become part of the new entity without the need for new employment contracts or renegotiation of terms.
- Preservation of employment terms: The new employer is obliged to maintain the same terms and conditions of employment that the employees had with the previous employer. This may include job roles, salary, benefits, seniority and other contractual terms.
- Employee notification: Prior to the transfer, the current employer must inform and, if necessary, consult with the employees and their representatives about the transfer. This ensures transparency and allows employees to be aware of any changes or implications.
- Protection against unjustified dismissal: Employees cannot be dismissed solely because of the transfer. Any termination of employment must be for valid reasons unrelated to the transfer, such as economic reasons or performance issues.

6.2 What employee information should the parties provide to each other?

In the context of an outsourcing transaction or other contract for the provision of technology-related services under the Malagasy Labour Code, certain employee information must be

exchanged between the parties involved to ensure compliance with legal requirements and the smooth transfer of employees.

Here is a non-exhaustive list of the necessary information:

1) **Employee data**
   - Personal information: The current employer must provide the names, contact details, job titles and roles of the employees being transferred to the new employer.
   - Employment terms: Details of employment contracts, including duration, working hours, salary, benefits, and any other relevant terms and conditions, should be shared to maintain the continuity of employment and uphold the employees' current work agreements.
   - Accrued rights: Information regarding accrued rights such as leave entitlements, pension contributions, and other benefits must be provided to ensure that these are maintained post-transfer by the new employer.
2) **Legal and financial information**
   - Outstanding liabilities: Any outstanding payments or liabilities owed to the employees, including bonuses, unpaid wages, and pending reimbursements, should be disclosed to ensure that the new employer can honour these obligations.
   - Compliance records: Records of compliance with labour laws, including any past disputes, claims, or ongoing legal matters involving the employees, should be shared to provide the new employer with a complete understanding of any legal issues that may need to be addressed.
3) **Consultation and Notification**
   - Employee notification: Employees should be informed about the transfer, the reasons for the transfer, the date it will take effect and the implications for their employment. This will ensure transparency and prepare them for the transition.
   - Consultation with employee representatives: If there are employee representatives or a works council, they must be consulted about the transfer and any planned changes that may affect the employees. The representatives must be given the opportunity to raise any concerns.

In all cases, the transfer of employees in connection with an outsourcing transaction requires maintaining the continuity of employment contracts, meaning all existing rights and obligations of the employees must be honoured by the new employer according to the Malagasy Labour Code. The new employer must provide the same or equivalent working conditions, and any detrimental changes to the employees' terms and conditions are generally prohibited without their consent.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

No, under the Malagasy Labour Code, a customer or service provider is not allowed to dismiss an employee solely for reasons connected with an outsourcing or other services contract. Dismissals must be based on valid and legitimate reasons that are not related to the outsourcing process. Indeed, employees cannot be dismissed solely because of the transfer of an undertaking or an outsourcing transaction. The provisions of the Malagasy Labour Code protects employees from being terminated due to changes in the structure or ownership of the business. Furthermore, while the transfer itself cannot be a valid reason for dismissal, employees may still be dismissed for valid reasons unrelated to the transfer. This includes reasons such as misconduct, incapacity, or other legitimate business needs not connected to the outsourcing process.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

The service provider must adhere to specific legal requirements regarding the employment terms of transferring employees. Indeed, while a service provider can seek to harmonise the employment terms of transferring employees with those of its existing workforce, this process must respect the protections provided under the Malagasy Labour Code. The new employer must maintain the continuity of the existing employment contracts and cannot impose detrimental changes without the employees' consent. Harmonisation efforts must be conducted through proper negotiation and agreement to ensure compliance with legal obligations and the protection of employee rights. It is worth noting that the Malagasy Labour Code stipulates that the amendment of the substantive clauses of an individual contract of employment, such as occupational classification, remuneration and position held, is no less favourable.

6.5 Are there any pensions considerations?

Yes, in the case of an outsourcing transaction or services contract, it is crucial to ensure the protection of employees' pension rights. The new employer must maintain the continuity of pension benefits and safeguard accrued pension rights. Any changes to the pension scheme should be negotiated with the employees and agreed upon, ensuring full compliance with legal requirements and the protection of employees' interests.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

If an employee is transferred due to offshore outsourcing, there are certain considerations that need to be addressed to ensure compliance:

1) **Transfer of employment contracts**
   The transfer of employment contracts is governed by the Malagasy Labour Code. When a business function is outsourced offshore, the employment contract of the affected employees may be transferred to the new employer (the offshore outsourcing company). This transfer should be carried out in compliance with the Labor Code and should not result in any loss of rights or benefits for the employees.
2) **Notification and consultation of employees**
   Before any transfer occurs, there should be a notification and consultation of employees affected. This ensures that they are informed about the transfer, their rights, and any implications for their employment.
3) **Social security rights and benefits**
   The social security rights and benefits of the employees should be protected. The new employer (offshore outsourcing company) should ensure that these benefits are continued or equivalent benefits are provided.
4) **Notification to Labour Authorities**
   In some cases, depending on the scale of the transfer, it might be necessary to notify the Labour Authorities about the transfer. This ensures transparency and compliance with labour regulations.
5) **Redundancy and retrenchment rules**
   If the outsourcing leads to redundancies or retrenchment, there are specific rules under Malagasy labour law that must be followed. This includes providing adequate notice periods, severance pay and other benefits.

6) **Employee consent**
Employees should not be transferred to the offshore outsourcing company without their consent. This consent should ideally be obtained after consultation and discussion with the employees.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Outsourcing transactions, including offshore outsourcing, are generally governed by the Malagasy Labour Code and other relevant laws and regulations. However, there are no specific laws or regulations that exclusively regulate outsourcing transactions in a detailed manner.

1) **Labour Code**
The Labour Code governs employment relationships, ensuring rights protection for employees during outsourcing, covering aspects such as contracts, working conditions and social security.
2) **Commercial Code**
The Commercial Code regulates commercial activities and contracts and applies to outsourcing agreements by governing contract formation, obligations and dispute resolution.
3) **Tax and customs regulations**
Tax and customs regulations apply to outsourcing, particularly international services, specifying tax application and customs duties.
4) **Data protection and privacy laws**
Data protection laws apply to personal data handling in outsourcing, ensuring compliance with regulations protecting individual privacy.
5) **Financial services laws**
The Banking Law and Insurance Code regulate outsourcing in banking and insurance, respectively, ensuring compliance and protecting customer interests, etc.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The legal classification of a contract used for an outsourcing transaction depends mainly on the scope, type and circumstances of the planned outsourcing (e.g., service contracts, rental contracts, purchase contracts and works contracts, for example).

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

In technology outsourcing agreements, particularly in the context of Service Level Agreements ("SLAs"), service levels and service credits are crucial components that ensure the service provider meets the client's expectations and maintains service quality. By defining clear metrics, establishing reasonable penalties for underperformance and incorporating mechanisms for continuous improvement and dispute resolution, both parties can effectively manage the outsourcing relationship and maintain mutual accountability.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods include (i) time and materials ("T&M"), (ii) fixed price, (iii) cost-plus pricing, (iv) subscription-based pricing, (v) outcome-based pricing, and (vi) the retainer model. These methods are chosen based on the project's complexity and scope, offering flexibility, predictability, and alignment with performance goals. It is essential to consider the specific requirements of the project, risk allocation, and compliance with local laws to ensure a successful outsourcing arrangement in Madagascar.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

When transferring third-party contracts as part of an outsourcing transaction, it is typically necessary to have agreements in writing. This ensures clarity, formalises the transfer process, and protects the interests of all parties involved. If these third-party contracts lead to changes in the content of the outsourcing transaction, the consent of the service provider is required. Then, novation is generally necessary because the assignment of a contract only transfers the benefits of the contract and not the burdens.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

In the context of an outsourcing transaction under Malagasy law, parties should be aware of the following key tax issues can arise:

- Value-added tax ("VAT").
- Withholding tax.
- Corporate income tax.
- Transfer pricing.
- Employment taxes.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Malagasy Law does not provide for provisions relating to licensing software for installation and use on a customer's own system.

However, in practice, when licensing software for installation and use on its own systems (on-premise solutions), customers should consider the following key issues:

- Licence scope and restrictions.
- Licence term and renewal.
- Intellectual property and ownership.
- Data security and privacy.
- Costs and payment terms.
- Updates and upgrades.
- Dispute resolution.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

The procuring support and maintenance services for software installed on customer systems is not yet regulated in Madagascar. However, the same list above applies to the subject.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Malagasy law does not provide for provisions relating to software escrow arrangements.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No. There is no such law that specifically regulates the procurement of cloud computing services. However, the personal data aspect and any associated cybercriminal acts (i.e. data uploading and data processing on the cloud computing services) can still be covered by the Cybercrime Law, the Personal Data Protection Law and ultimately the Criminal Code.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Madagascar's advances in technology do not correspond to its economic growth. Cloud computing is not yet widely adopted in Madagascar; it is not a foreign concept, however, especially to the working population, such as companies, small businesses and freelancers. In general, Malagasy people partly rely on cloud computing services in the administrative services and as simple citizens. There are only few identified companies that have integrated cloud computing as whole part of their functioning system.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The lack of specific legal provision covering cloud computing services, a weakness in the technology legal framework and the failing of the implementation of the CMIL are major challenges for Madagascar. In a near-future that presents an increase in the use of technology, such as cloud computing services, the enforceable law will fail to hold an effective grip on technology providers. In case of data incidents or liabilities, Madagascar lacks empowered authority representatives to protect its people's data, personal data and cyberreality.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No, there are none.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Yes, while it is generally possible to legally own and license data used to train machine learning-based systems, the Malagasy legal framework requires compliance with the Personal Data Protection Law and contractual agreements. Data ownership typically remains with the original data owner, with licences granted for specific uses under pre-agreed terms. Then, intellectual property rights in the trained machine learning models may be also governed by Madagascar's laws and require clarity in contractual agreements.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

The position on this issue is unclear under Malagasy law. It is difficult to determine who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer and can depend on various factors. For example, if the algorithm is purely generated or improved by machine learning techniques without any human intervention, it may not qualify for traditional intellectual property protection like copyright or patent rights. Otherwise, the author is the natural person who created the work.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

Malagasy laws do not provide for any provisions relating to the procurement of blockchain-based solutions.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Malagasy laws do not provide for any provision relating to procuring blockchain-based technology. Nevertheless, the implementation of blockchain technology may require substantial infrastructure which Madagascar is still developing.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Malagasy law does not provide for any provision relating to procuring blockchain-based technology.

Hoby Rakotoniary is a partner at John W Ffooks & Co, where she leads the corporate and Telco/IT teams. With a keen focus on technology law and practice in Madagascar, she brings extensive expertise in corporate finance and telecommunications, including licensing requirements, landing station regulations, privacy requirements, encryption and interception issues. Hoby advises a diverse range of institutions, including domestic and international banks and financial institutions, supporting investments in key sectors of development across French-speaking Africa. Recognised as a Rising Star Partner by *IFLR1000*, Hoby is the firm's representative to the International Bar Association (IBA) and an active member of its Women in Law Section. Her academic background includes a Law degree from the University of Antananarivo and a Master of Laws from the Institute of Judicial Studies in Madagascar. Fluent in both French and English, Hoby is well-equipped to navigate complex legal landscapes and deliver insightful, strategic advice to her clients.

John W Ffooks & Co
Immeuble Assist - 1st Floor
Ivandry Antananarivo 101
Madagascar

Tel: +261 20 224 3247
Email: Hoby@JWFLegal.com
LinkedIn: www.linkedin.com/in/hoby-rakotoniary-9281b973

Fabiola Andriamalala is a junior associate at John W Ffooks & Co, where she specialises in technology law, providing expert advice on regulatory compliance and legal strategies for technology procurement in Madagascar. With extensive experience of local and international regulatory frameworks, she advises clients on telecommunications, information technology and project finance, ensuring that they adapt effectively to the complexities of the sector. Her expertise extends to dealing with commercial and regulatory issues in the legal systems of Madagascar and OHADA, demonstrating a nuanced understanding of the regional legal landscape. Fabiola frequently works with senior partners on domestic and cross-border transactions, providing valuable insight and support for multi-jurisdictional OHADA cases. Fluent in French and English, Fabiola's language skills enhance her ability to serve a diverse client base, ensuring clear and effective communication in all legal proceedings. Her extensive practice and in-depth knowledge of technology law make her a valuable asset to the firm and its clients.

John W Ffooks & Co
Immeuble Assist - 1st Floor
Ivandry Antananarivo 101
Madagascar

Tel: +261 20 224 3247
Email: Fabiola@JWFLegal.com
LinkedIn: www.linkedin.com/in/fabiola-andriamalala-954b7b22a

Hariliva Andriamahefa is a junior associate at John W Ffooks & Co, specialising in technology law and general corporate matters in Madagascar. With her in-depth knowledge of the local legal landscape, she advises clients on a wide range of matters, including general corporate, telecommunications and regulatory matters. Her in-depth knowledge of technology procurement has proved invaluable to clients navigating the complexities of the technology industry in the region. Hariliva has consistently demonstrated her expertise by playing a key role in advising and assisting large companies seeking local legal advice for their commercial activities throughout French-speaking Africa. Fluent in French and English, she is a remarkable asset to the firm, bridging the gap between international clients and the local regulatory environment.

John W Ffooks & Co
Immeuble Assist - 1st Floor
Ivandry Antananarivo 101
Madagascar

Tel: +261 20 224 3247
Email: Hariliva@JWFlegal.com
LinkedIn: www.linkedin.com/in/hariliva-sandra-andriamahefa-086b41266

John W Ffooks & Co is a full-service corporate & commercial law firm providing exclusively local counsel advice, providing support to business and industry across French-speaking Africa. Our fully bilingual legal team, comprised of 11 partners and 40 lawyers, is the only legal practice in the region supplying Napoleonic advice with a Common Law understanding of client imperatives. This unique mix makes us the obvious choice when it comes to international transactions in Francophone Africa.

From our head offices in Madagascar, Senegal, Guinea, Togo and Mauritius, (as well as lawyer-led bureaux in every country across the region), we advise on a full range of commercial legal issues in French-speaking Africa, including Benin, Burkina Faso, Burundi, Cameroon, Central African Republic, Chad, Comoros, Democratic Republic of Congo, Gabon, Guinea-Conakry, Ivory Coast, Mali, Niger, Republic of Congo, Rwanda, Senegal and Togo.

Our firm has had the privilege of representing a diverse range of clients within the Technology, Media, and Telecommunications (TMT) sector. This includes private organisations, state-owned enterprises, and various government agencies. Our extensive experience in this domain has allowed us to build a deep understanding of the unique challenges and opportunities that clients in the TMT sector face. As a result, we are well-equipped to provide tailored legal and advisory services to cater to their specific needs and requirements.

www.jwflegal.com

JOHN W FFOOKS & CO

Nigeria

Ikeyi Shittu & Co.

Josephine Tite-Onnoghen

Destiny Chukwuemeka

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, it is not regulated. Private sector procurement of technology products and services is subject to the general laws of contract. However, the National Office for Technology Acquisition and Promotion ("NOTAP") Act ("NOTAP Act") provides that all contracts for the transfer of foreign technology to Nigerian parties should be registered with NOTAP; and NOTAP guidelines include some "local content" requirements in respect of software licensing contracts, amongst other mandatory contract terms. Failure to register the contract would prevent payment due to the foreign party under the contract through, or on the authority of, the Central Bank of Nigeria, or a licensed bank in Nigeria (section 8 of NOTAP Act).

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes. The procurement of technology products and services by government or public sector bodies is regulated by the Public Procurement Act 2007 ("PPA"), which covers the procurement of all goods, works, and services carried out by (i) the Federal Government of Nigeria and all procurement entities, and (ii) all entities outside the foregoing description which derive at least 35% of the funds appropriated for any type of procurement described in the PPA from the Federation share of the Consolidated Revenue Fund (section 15 of the PPA). A procuring entity under the PPA is defined as a public body such as a Ministry, extra-ministerial office, government agency, parastatal, or corporation (section 60 of the PPA) that is engaged in procurement. The basic features of the PPA regime include: (i) ensuring accountability and transparency in the procurement process; (ii) establishing pricing standards for procurement; and (iii) ensuring the application of competitive and transparent procurement of services. The provisions of the PPA do not apply to the procurement of special goods, works and services involving national defence or national security, unless the President's express approval has first been sought and obtained.

Furthermore, whilst the Public Procurement (Goods and Works) Regulations 2007 ("Regulation for Goods and Works") applies to procuring entities and participants in public contracts and to all public procurements of goods and works, the Public Procurement (Consultancy Services) Regulations 2007 ("Consultancy Service Regulation") applies to all procurement of consulting services by all procuring entities, except where a waiver is first obtained under the PPA. The Consultancy Service Regulation does not apply to contracts for physical services such as exploratory drilling, surveys, aerial photography, transportation installation and maintenance services or services that are provided by a contractor as a complement to a goods and works contract. The Regulations for Goods and Works apply in such cases. The Guidelines for Nigerian Content Development in Information and Communication Technology ("Guidelines") issued by the National Information Technology Development Agency ("NITDA") specifically regulate the procurement of technology products and services by government or public sector bodies. The Guidelines require indigenous original equipment manufacturers ("OEM") and indigenous design manufacturers ("ODM") to obtain a licence from NITDA. Such licence must be renewed every two years. It also requires that manufacturers, either directly or through outsourcing, ensure local value and skills are added in terms of the quality and quantity of products they produce. Hardware multinational companies/OEMs are required to provide a local content development plan that they will follow in the course of their operations in the country. On their part, government and public sector bodies are obligated to source and procure locally 40% of computer hardware and associated devices from NITDA-approved ODMs or OEMs.

International software vendors, software development firms and indigenous software-enabled product firms must register their products, capabilities and organisation on the NITDA portal. In addition, multinational software companies/OEMs must provide verifiable information and sign affidavits about the origin, safety and workings of software being sold and deployed in Nigeria. They are also required to have a local content development plan for their platforms and products.

Government and public sector bodies are obligated to source locally all software and software-enabled products and services for which there is indigenous capacity to design, develop, compile, test, troubleshoot, launch, maintain and improve. In addition, government and public sector bodies must only source and procure software from indigenous software development companies. Where the capacity for developing such software does not exist locally, procurement, installation and support will be provided by a Nigerian company. It is also necessary to obtain evidence of the origin and workings of all software being used, including adequate assurance of the full security of the source code.

However, the Guidelines prohibit the procurement of bespoke enterprise software from non-indigenous developers for the following categories:

(a) Enterprise Resource Planning ("ERP").

(b) Human Resource Management.
(c) Enterprise Internet/Intranet/Extranet Portals.
(d) Education Content and School Management Systems.
(e) Learning Management and/or Learning Content Management Systems.
(f) Training Systems.
(g) Document Management Systems.
(h) E-commerce Systems.
(i) Payment Systems.
(j) Invoicing and Accounting Systems.

Similarly, the Guidelines require telecommunication companies to be registered with the NCC and to have a local content development plan, whilst networking service companies must register their products, capabilities and organisations on the NITDA portal.

Furthermore, all government ICT service providers are required to be registered with NITDA as ICT service providers before they can provide services to any government ministry, department, or agency. The registration process is governed by the NITDA-issued Guidelines for the Registration of ICT Service Providers/Contractors for the Delivery of IT Services to MDAs.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

Although parties are at liberty to agree on the terms of a contract for the supply of technology-related solutions, NOTAP will usually not approve a contract (which is subject to its regulatory oversight) for a term longer than three years in the first instance. NOTAP may, however, also approve renewed terms for the contract upon application.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, it does not. Parties are free to negotiate and agree on notice periods, as may be appropriate.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

No, there is not. There are no overriding legal requirements under Nigerian law for a customer and/or supplier of technology-related solutions or services to act fairly or in good faith.

However, the Federal Competition and Consumer Protection Act 2018 ("FCCPA"), which applies to all undertakings and all commercial activities within, or having effect within, Nigeria, prohibits unfair, unreasonable, or unjust contract terms in the supply of goods and services generally. For instance, section 131 thereof stipulates that every consumer has a right to receive goods that are reasonably suitable for the purposes for which they are generally intended, of good quality, in good working order and free of defects, usable and durable for a reasonable period of time (having regard to the normal use of such goods and all the surrounding circumstances of the supply) and comply with any applicable standards set by industry sector regulators.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The remedies depend on the nature of the breach. They may include compensatory damages, specific performance, injunctions, and/or recission of the contract.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

There should be provision for a testing period before acceptance of technology solutions. Further, acceptable service levels should be described in the agreement for the provision of technology services, and the customer should be indemnified by the vendor in the event of a breach of third-party copyright or patent by the vendor. There should also be provisions for the ownership of data generated from the contractual relationship and how it may be dealt with in the event of the cessation of the relationship.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Ordinarily, contracts for the procurement of technology-related products or services have termination provisions. Once a party terminates the contract in accordance with the termination provisions, it is unlikely that the counterparty would have a successful claim for damages.

2.7 Can the parties exclude or agree additional termination rights?

Yes, they can. Parties can exclude or agree additional termination rights based on the principle of freedom of contract.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Generally, parties are allowed to limit or exclude their liability contractually. However, neither party is allowed to contract out of a mandatory statutory duty or obligation, though it may transfer the burden of its performance to the other party by contract. However, exclusion or limitation of liability for fraud or fraudulent misrepresentation is usually unenforceable. A Nigerian court will also not enforce an exclusion of liability clause if the effect of the exclusion is to defeat the essence of the contract. The FCCPA also prohibits an undertaking from requiring a consumer to waive any rights, assume any obligation or waive any liability of the undertaking on terms that are unfair, unreasonable or unjust. The terms are unfair, unreasonable and unjust if, amongst others, the result makes the transaction so adverse to the consumer as to be inequitable or if the exclusion is not properly brought to the attention of the consumer (see sections 127(1)(c) and 127(2) of the FCCPA).

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, subject to the details set out in question 2.8 above.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, they do not. All the general principles identified in our responses to questions 2.1 to 2.9 apply to all the stated types of technology procurement contract. The effect of the application may, however, vary in accordance with industry standards in respect of each specific type of contract.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Contracts for the procurement of technology solutions and services usually provide for confidential consultations by the parties' management to resolve any dispute, failing which they resort to mediation, and failing mediation, the dispute would be resolved by arbitration. Although the choice of arbitration would preclude the courts from determining a dispute in respect of which parties have agreed to arbitrate, it operates without prejudice to the parties' rights to apply to the court for urgent interim relief(s).

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

Existing intellectual property ("IP") of either party is usually declared to belong to the relevant party, though it is made available to the other party in the course of, or for the purpose of, fulfilling the contract. Accordingly, the other party is licensed to use such IP to the extent necessary for the performance or receipt (as the case may be) of the services. Also, in contemplation of improvements to the existing IP, parties provide that developments to their respective existing IP would belong to them. The supplier must agree, however, to transfer to the customer rights related to new developments to the supplier's IP, created exclusively for the particular customer, provided that the supplier can continue to perform similar services for other customers after such transfer. Where absolute transfer of such rights would impede the continued performance of similar services by the supplier to other customers, then the supplier would insist on merely licensing the customer to use the development non-exclusively. Permission for customers to continue to use suppliers' IP at the end of a contract term is usually to the extent that such IP is incorporated in the deliverables to the customer under the contract, and only in connection with the customer's normal use of the deliverables.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes, there are. The assignment of an intellectual property right is required to be in writing, signed by the parties, and registered with the relevant authority upon payment of the prescribed fee. The assignment of a trademark and patent right is required to be registered at the Trade Marks, Patents and Designs Registry, whilst the assignment of a copyright may be registered at the Nigerian Copyrights Commission ("Commission"). Registration of a copyright at the Commission is not mandatory but it is advised because the notification database maintained by the Commission is a public source for verifying an author's work.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

No, they are not specifically protected by national law. They are rather protected under the general principles of common law – under contracts, torts and other basic legal principles. Additionally, they are better protected by including non-compete and/or non-disclosure clauses in the agreement.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes, it is. It is regulated by the Nigeria Data Protection Act 2023 ("NDPA"). The Nigeria Data Protection Regulation 2019 ("NDPR") and the NDPR Implementation Framework 2019 ("Implementation Framework") continue to apply as subsidiary legislation pursuant to section 64(2)(f) of the NDPA. The NDPA is administered by the Nigeria Data Protection Commission ("NDPC").

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside the jurisdiction.

Pursuant to section 41(1) of the NDPA, a data controller or data processor can only transfer or permit personal data to be transferred from Nigeria to another country if the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that afford an adequate level of protection with respect to the personal data in accordance with the NDPA; or one of the following conditions have been satisfied: (a) the data subject has provided and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections; (b) the transfer is necessary for the performance of a contract to which a data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract; (c) the transfer is for the sole benefit of a data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such consent, the data subject would likely give it; (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; or (f) the transfer is necessary to protect the vital interests of a data subject or of other persons, where a data subject is physically or legally incapable of giving consent.

A data controller or data processor shall record the basis for the transfer of personal data to another country and the adequacy of protection (section 42 of the NDPA).

Also, the Implementation Framework includes a "Whitelist", which contains the names of countries that have been determined to have an adequate level of data protection. Pursuant to article 14.3 of the Implementation Framework, personal data may be transferred to organisations in countries on the Whitelist, provided the organisation complies with other provisions of the NDPR. For countries that are not on the Whitelist, a level of protection is adequate if principles comprised therein are substantially similar to the conditions for the processing of personal data provided for in the NDPA. The adequacy of protection shall therefore be assessed taking into account: (a) the availability of enforceable data subject rights, the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law; (b) the existence of any appropriate instrument between the NDPC and a competent authority in the recipient jurisdiction that ensures adequate data protection; (c) the access of a public authority to personal data; (d) the existence of an effective data protection law; (e) the existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and (f) international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

Further, under the "Nigerian Communications Commission (Registration of Telephone Subscribers) Regulation 2011" ("NCC Regulation"), information shall not be released to a third party and/or transferred outside Nigeria without the prior written consent of the subscriber and the Nigerian Communications Commission ("NCC") (see Article 10 thereof).

5.3 Are there any legal and/or regulatory requirements concerning information security?

Yes, there are. Section 39 of NDPA provides that a data controller and data processor shall implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access, taking into account: (a) the amount and sensitivity of the personal data; (b) the nature, degree and likelihood of harm to a data subject that could result from the loss, disclosure, or other misuse of the personal data; (c) the extent of the processing; (d) the period of data retention; and (e) the availability and cost of any technologies, tools, or other measures to be implemented relative to the size of the data controller or data processor in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach. Additionally, Article 2.6 of the NDPR also provides that anyone involved in data processing or storage of data shall take adequate measures, such as setting up firewalls and encrypting data for the protection of personal information.

Also, the Cybercrime (Prohibition, Prevention, Etc.) Act 2015 ("Cybercrime Act") provides that service providers shall keep all traffic data and subscriber information as may be required by the NCC for a period of two years and shall implement adequate measures to safeguard the confidentiality of the data retained or processed (section 38 (1) and (5) of the Cybercrime Act). The Cybercrime Act also criminalises the intentional interception of non-public transmissions of computer data without requisite authorisation. Further, the NCC Regulations provide that subscriber information contained in the central database shall be held in strict confidentiality, and that no person or entity shall be allowed access to any subscriber information from the database, except as provided by the NCC Regulations (section 9(2) thereof).

The Central Bank of Nigeria ("CBN") Consumer Protection Framework 2016 also directs financial institutions to take adequate measures to safeguard the data of consumers.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Nigerian law does not recognise the transfer of employees by operation of law [Re Bendel Line Co. Ltd (1979) 5 FRCLR 19]. Specifically, for employment contracts governed by the Labour Act, section 10 thereof subjects the transfer of employment from one employer to another to the consent of the worker and the endorsement of the transfer by an authorised labour officer. Thus, the transfer of employment would only be effective when the employee consents to it. However, the facts and decision in each of *Madam Oyesola Ogunleye v. Sterling Bank Plc.* (unreported judgment of the NICN in Suit No. NICN/LA/430/2014 delivered on 24 May 2018), and *Kefre Ekpo Inyang v. Alphabeta Consulting LLP* (unreported judgment of the NICN in Suit No. NICN/LA/550/2016 delivered on 4 June 2018), suggest that where consent is not expressly given by the employee, it could be implied from the conduct of the parties.

6.2 What employee information should the parties provide to each other?

For outsourcing transactions involving the provision of technology-related services, there is no statute detailing specific employee information to be provided by: (a) the supplier to the customer; or (b) the customer to the employer. Generally, either party would require sufficient information on the relevant employee to enable them to determine the suitability of the employee. Thus, the transferee may request detailed employee records (i.e., a copy of the employment contract, copies of applicable collective bargaining agreements and the curriculum vitae of the relevant employee).

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Yes, but the laws applicable to the termination of employment must be observed. Where an employer plans to terminate the employment of an employee due to redundancy occasioned by an outsourcing arrangement, the employer, in case of an employment contract governed by the Labour Act, would comply with the requirements of laying off a worker for redundancy under section 20 of the Labour Act. For employment not governed by the Labour Act, the employer is required to comply with any redundancy provision in the employee's contract of employment and/or applicable collective bargaining agreement.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, it is. The requirement to obtain an employee's consent to

a transfer of employment in Nigeria provides the parties the chance to negotiate the terms upon which the transfer would be implemented. Such terms may include the harmonisation of the employment terms of the transferring employee with those of the suppliers' existing workforce.

6.5 Are there any pensions considerations?

Yes. Generally, Nigeria operates a mandatory contributory pension scheme in which monthly contributions of the employer and employee are remitted to a pension fund administrator ("PFA") chosen by the employee. The mandatory scheme came into force in 2004 pursuant to the Pension Reform Act ("PRA"). The PRA was subsequently repealed and replaced by the Pension Reform Act 2014 ("PRA 2014"). Although the PRA 2014 sets minimum rates of contribution for both the employee and the employer, the law nevertheless permits the employer to assume a higher percentage of the total contribution. It would therefore be necessary to confirm (a) the rate of contribution assumed by the previous employer, and (b) the previous employer's compliance with its deduction and remittance obligations.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Yes, there are. Parties should adhere to local laws and the laws of the foreign party before, during and after the outsourcing contract to ensure that the outsourced business is not subject to any legal restrictions in any of the jurisdictions. Special consideration should be given to local laws relating to the employment of expatriate staff, and the remittance of money paid to expatriate staff where the transaction contemplates the engagement of expatriate personnel. It is also possible that an outsourcing transaction that involves an offshore supplier and a Nigerian resident customer may create a business activity in Nigeria to the extent that the offshore supplier might be considered to be carrying on business in Nigeria. In this circumstance, the offshore supplier would be required to establish a local subsidiary in Nigeria as prescribed by section 78 of the Companies and Allied Matters Act 2020.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

There are no national laws generally regulating outsourcing. However, the "Guidelines on Labour Administration: Issues in Contract Staffing/Outsourcing in the Oil and Gas Sector" ("O&G Guidelines"), issued by the Federal Ministry of Labour and Productivity in 2011, regulates outsourcing in the oil and gas sector. The O&G Guidelines, amongst others, provide that the jobs in the main organisational structure of companies in the sector must be occupied by permanent employees and restrict outsourcing to the non-core business, except for proven short-term projects. Also relevant are the "Guidelines on Labour Administration Issues in Contract Staffing/Outsourcing, Non-permanent Workers in Banks, Insurance and Financial Institutions" ("Financial Sector Guidelines") issued on 8 September 2022. There also exists a "Code of Conduct for Private Employment Agencies 2012", which was developed jointly by the Human Capital Providers Association of Nigeria, an association of private employment agencies in Nigeria, Nigeria Employers' Consultative Association, the Federal Ministry of Labour and Productivity and the International Labour Organisation. Further, the National Industrial Court, which has exclusive jurisdiction to hear and determine labour- and employment-related disputes, has in recent case law begun to develop some principles of law applicable to outsourcing and other "disguised employment relationships".

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The most common structure in Nigeria is direct outsourcing in which the customer directly engages the supplier under a service agreement. Such service agreements usually have elaborate schedules detailing the scope of the business outsourced, standards against which performances will be assessed, prices, transfer of personnel and equipment, etc.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

The usual approach in a technology outsourcing contract is to include in the contract in sufficient detail and clarity the standard of performance or service level standards expected from the supplier. Each of these service levels should be capable of being objectively measured and focused on the elements of the service that directly impact the customer. The contract should also require that a service level report should be given by the supplier at agreed intervals. Where the supplier fails to meet the contracted service level standards, the customer is entitled to deduct an amount (either already agreed or calculated at an agreed rate) from the amount to be paid under the contract as service credits. The threshold trigger for a service credit is typically set at a reasonable level such that service credits will apply only in circumstances where all parties can agree that the standard of the service provided by the supplier was inadequate.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods are (a) the fixed charging method, (b) the cost-plus charging method, and (c) the pay-as-you-go charging method. If the level and volume of service that would be required by the customer during the contract period is predictable and the customer wants to have certainty over its budget, the fixed charge approach is ideal. However, if the level and volume of service that would be required is not predictable, the cost-plus charging method (where the customer pays the actual cost of providing the service, plus an agreed profit margin to the supplier) would be the preferred method. Where the deliverables under the contract have standard units, the parties may adopt the pay-as-you-go charging model, whereby the customer pays a pre-agreed unit price for each deliverable received.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Generally, the transfer of third-party contracts to a service provider can be achieved by the assignment by a customer of

the customer's existing obligations/proprietary rights under a third-party contract to the service provider, or by entering into a novation agreement with the service provider with respect to the third-party contract. These modes of transfer of third-party contracts are to be incorporated in the outsourcing contract.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Once a service provider receives payments of over N25 million in a year, it must include value added tax ("VAT") – currently assessed at 7.5% – in its invoice to the customer for the service fee arising from the outsourcing transaction. The VAT is to be remitted by the service provider to the Federal Inland Revenue Service ("FIRS") not later than the 21st day of the subsequent month. A foreign service provider is also required to include VAT on its invoice to the Nigerian customer, but the Nigeria customer is required to deduct the VAT at source and remit to the FIRS. VAT leakage on the supply of services under the outsourcing transaction can be an issue as VAT paid on the procurement of services is not recoverable in Nigeria.

Regarding income tax, the customer is required to deduct withholding tax ("WHT") at the rate of 10% (for a corporate service provider) and 5% (in the case of an individual service provider). The WHT so deducted, which represents an advance payment of the income tax liability of the service provider, can be utilised as an offset against the eventual income tax liability of the service provider. Meanwhile, the companies' income tax ("CIT") rate varies between 0% and 30% depending on the annual turnover of the company. Where a company's turnover is not more than N25 million, the CIT rate is 0%, whilst the CIT rate for a company with turnover of between N25m and N100m is 20% and for a company with a turnover above N100m, the rate is 30%. In Nigeria, the WHT deducted from the income earned by a foreign company (which provides the outsourced services outside Nigeria to a resident in Nigeria and earns up to N25 million therefrom) is the final tax on such income. However, a foreign service provider, which has (a) an employee in Nigeria through which it performs the outsourced services in Nigeria, or (b) significant economic presence in Nigeria, will be affixed with tax presence in Nigeria. The foreign service provider will therefore be required to file CIT returns in Nigeria (in which case the WHT will not be the final tax). Accordingly, an outsourcing transaction between a Nigerian resident and a non-resident may be subject to "double taxation" of the income of the non-resident supplier from the transaction.

The service provider is also required to account for personal income tax due on the salaries paid to its employees working on the outsourcing transaction. Every employer is required under the Pay-As-You-Earn ("PAYE") tax scheme to (on a monthly basis) deduct the income tax due from the salaries paid to its employees and remit such deducted PAYE tax to the relevant tax authority for each of the states in Nigeria and the Federal Capital Territory.

An outsourcing transaction which involves the transfer of assets may have capital gains tax implications, and thus may raise the issue of the value at which the transferred assets are brought onto the books of the supplier to whom the assets have been transferred. Transfer pricing issues may also arise where the parties to the transaction are related entities.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

There will be both legal and technical issues to consider. The primary technical issue to be considered is the seamless integration and compatibility with the customer's system of the software about to be procured. Another issue is ensuring the competence of the customer's staff in the use of the solution. The customer may therefore consider having the supplier provide initial training for its staff in the use of the software post integration.

For legal issues, the first issue for a customer to consider is clarity on what constitutes a "fault" or "defect" in the software being licensed, so as to create an obligation for the software supplier to fix problems if they arise. The second legal issue to consider is the issue of warranty. The supplier should generally provide an undertaking to repair or replace the defective software when notified of the defect by the customer. The period of the warranty will vary depending on the type of software being licensed and the bargaining power of the parties.

Further, the customer may have concerns on confidentiality and data privacy, since the supplier would have access to the customer's IT systems and data about its business, products, employees and customers. However, mutual provisions on confidentiality and compliance with the NDPA will protect any such information that is accessed by the supplier in the process.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

One issue that should be considered is the issue of response time to customer complaints. The agreement should classify usual customer complaints according to their level of severity and pre-agreed supplier response time to them. The customer should also agree the terms for on-site support where remote support is unable to resolve a complaint. The agreement should also provide for training upon request by the customer of its staff in the use of the software in the event that those initially trained are unable to train successors before leaving the customer's employment or for any other reason as the customer may deem necessary.

The customer should also impose data protection compliance obligations on the supplier of the support and/or maintenance service that, in the minimum, meets the data protection obligations imposed on a data controller by the NDPA.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes. Software escrow arrangements are commonly used. They are also enforceable in the case of insolvency, provided the escrow agreement so provides.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No, there are not. However, NITDA issued the Nigerian Cloud Computing Policy ("NCCP") 2019, which requires Nigerian public sector entities to prioritise the procurement of cloud-based information and communication technologies whenever possible.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

The adoption of cloud computing solutions is growing rapidly in Nigeria. To encourage the adoption of such solutions, the NCCP 2019 was formulated and issued by NITDA. The objectives of the NCCP 2019 are to create a drive for "cloud first" policies in the country and ensure that ministries, departments and agencies ("MDA") and public sector entities migrate completely to the cloud. Also, major cloud providers such as Microsoft, IBM, Google and Amazon have begun providing cloud computing services directly to organisations or in partnership with local IT firms for better integration and penetration into the Nigerian market.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The first issue is the non-negotiable contracts in procuring cloud computing services. Cloud computing services, particularly those procured by SME companies, are available mostly through non-negotiable clickwrap agreements, where the customer can simply click an "I agree" button to accept the terms and receive the services. In these situations, the customer has little or no opportunity to negotiate the terms of procurement or to conduct extensive due diligence on the vendor. The customer should therefore review the terms of the clickwrap agreement to ensure that it is protected and that the vendor does not limit liability for failure to provide adequate services.

The second issue is subcontracting. A vendor may rely on other cloud vendors to provide data storage services for it where it is cost-efficient to do so. This raises data privacy concerns. Also, there is a likelihood that in the event of a dispute, the vendor will seek to transfer liability to the third party – an entity with whom the customer has no privity of contract.

Where personal information is stored in the cloud, valid concerns may arise as to the protection of such data on the cloud. This will include providing security and notifying customers in the event that their personal information has been compromised. It is therefore necessary that a customer should properly review the applicable agreement to ensure that the vendor is still able to comply with its data privacy and protection obligations under the NDPA if it procures cloud computing services under the agreement.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No, there are none.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Generally, companies looking to obtain data to train machine learning-based systems look to five sources: (i) data sets sold through data brokers; (ii) batch uploaded data from software installed on-premises for customers; (iii) ongoing customer data collection from network-connected software as a service offering; (iv) open public data sets; and (v) data obtained directly from customers. The data obtained from sources (i) – (v) can be legally owned. The licence of any of the data depends on the agreement governing the acquisition and use of the data. However, where regulated data (i.e., data that contains personally identifiable information) is input into the machine learning algorithm, then the output is also likely to be regulated by the NDPA.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

There is no national law regulating the intellectual property rights of algorithms that are improved by machine learning techniques. However, under general copyright law, the copyright in such algorithms should arguably belong to the person who made the data input on which the machine acted to develop the algorithms or improve existing algorithms, unless there is express agreement to the contrary. This is because the algorithm qualifies as literary work under the Copyright Act; and section 28 of the Copyright Act 2022 vests the copyright of literary works in the author, except where there is an agreement to the contrary (the author being the person that created it). In this case, since the machine is not recognised as a person, it will only be regarded as a tool used by the person that made the data input to create the algorithm that resulted therefrom.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there are none. However, where the blockchain-based solution that is procured qualifies as a securities transaction, it will be regulated by the Investment and Securities Act 2007. Further cryptocurrency exchanges, which are conducted within the banking system, are regulated by the CBN.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain-based technologies are mostly used in the fintech sector where companies utilise blockchain solutions to provide efficient financial services to customers in Nigeria, including facilitating payments by means of cryptocurrencies.

The CBN issued a circular in February 2021 directing banks and other financial institutions immediately to close the accounts of persons and/or entities transacting in, or operating cryptocurrency exchanges within, their systems. On 22 December 2023, the CBN issued a guideline ("Guideline") to financial institutions under its regulatory purview with respect

to their banking relationship with virtual assets service providers ("VASPs") which include cryptocurrencies and crypto assets in Nigeria. The primary objectives of the Guidelines are to (a) prescribe the minimum standards for banking relationships with VASPs in Nigeria, (b) monitor financial institutions providing services to Securities and Exchange Commission's licensed eligible entities, (c) offer guidance on eligible entities' account operations, and (d) ensure robust risk management practices in the sector. The Guidelines extended the activities permitted by the eligible stakeholder financial institutions to include (i) opening of designated accounts, (ii) providing non-interest-bearing designated settlement accounts and settlement services, (iii) acting as channels for foreign exchange flows and trade, and (iv) any other activity that may be permitted by the CBN from time to time. Also, section 30 of the Money Laundering (Prevention and Prohibition) Act, 2022 recognises VASPs as part of the definition of a financial institution. In addition, the Securities and Exchange Commission (SEC) in May 2022 issued Rules on the issuance, offering, and custody of digital assets and VASPs to provide a regulatory framework for their operations in Nigeria.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

In Nigeria, procurement of blockchain-based technology is not yet regulated specifically by law. However, to the extent that personal data is exchanged or collected, parties must comply with the provisions of the NDPA in their processing of personal data.

Josephine Tite-Onnoghen is a senior associate at Ikeyi Shittu & Co. and a member of the firm's corporate and investment practice, as well as the firm's technology (including data privacy) practice. Josephine provides transactional support services to businesses including technology companies operating in diverse sectors of the Nigerian economy and she routinely provides general regulatory compliance advisory and compliance services to businesses.

Josephine graduated from the University of Lagos in 2013 with a upper second-class degree and was called to the Nigerian Bar in 2014. She also obtained a Master of Laws (in International Commercial Law with International Law) with distinction from the University of Kent in the United Kingdom in 2017.

Ikeyi Shittu & Co.
Suite 7, Moz Mall
No.19 Durban Street
Off Ademola Adetokunbo Crescent
Federal Capital Territory, Abuja
Nigeria

Tel: +234 703 780 5423
Email: jadeyele@ikeyishittuco.com
LinkedIn: www.linkedin.com/in/josephine-tite-onnoghen-30367aaa

Destiny Chukwuemeka is an associate at Ikeyi Shittu & Co. and a member of the firm's energy, maritime, tax, and technology (including data privacy) practice team. In addition to advising clients on power projects, he also advises technology companies, such as co-location service providers and payment solution providers, on issues relating to fintech regulation, and general regulatory compliance.

Ikeyi Shittu & Co.
Plot 50, Liberty Estate
Independence Layout
Enugu
Nigeria

Tel: +234 803 385 3171
Email: dchukwu@ikeyishittuco.com
LinkedIn: www.linkedin.com/in/destiny-chukwuemeka-cdc-a0908a138

Ikeyi Shittu & Co. (the "firm") is a full-service law firm with international business experience. The firm provides its clients with a full range of legal, business advisory and transaction support services with a guarantee of skill, knowledge and professionalism.

Whether engaged to advise on new investments or relationships, or to resolve issues arising from existing transactions, the firm creates value by providing innovative and practical business solutions. We start by understanding the industries in which our clients operate, the peculiarities of each client's business and the clients' expectations, as the bases for identifying the solutions that optimise the client's position within the framework of the law and the operating environment.

We place strong emphasis on business ethics.

www.ikeyishittuco.com

IKEYI SHITTU & CO.
Barristers and Solicitors

Philippines


Leland R. Villadolid, Jr.


Chrysilla Carissa P. Bautista


John Paul M. Gaba


Erwin Jay V. Filio

Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW)

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

Generally, private sector technology procurement is not regulated. The law on obligations and contracts therefore governs.

However, the Intellectual Property Code ("IP Code") and the Intellectual Property Office of the Philippines' ("IPOPHL") 2020 Revised Rules & Regulations on Voluntary Licensing ("IPOPHL Rules") provide prohibited and mandatory clauses and/or grounds for cancellation of a "Technology Transfer Arrangement" ("TTA"), i.e., contracts or agreements involving the transfer of systematic knowledge or the manufacture of a product, the application of a process, or rendering of a service which may cover management contracts, and the transfer, assignment or licensing of all forms of intellectual property ("IP") rights, including licensing of computer software, except computer software developed for mass market.

While a TTA need not be registered, non-conformance shall automatically result in unenforceability, unless an application for exemption has been granted by the IPOPHL's Documentation, Information, and Technology Transfer Bureau.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes, Republic Act No. ("RA") 9184, known as the Government Procurement Reform Act ("GPRA") governs public sector technology procurement.

As a general rule, competitive public bidding is mandatory and is guided by the principles of: (a) an offer to the public; (b) an opportunity for competition; and (c) a basis for the exact comparison of bids (*Capalla v. Commission on Elections*, G.R. Nos 201112, 201121, 201127 and 201413, 13 June 2012).

Those dealing with the government are mandated to register with the Philippine Government Electronic Procurement System. The bidding process undergoes eight stages: (a) preparation of bidding documents; (b) pre-procurement conference; (c) advertisement; (d) pre-bid conference; (e) eligibility screening of bids; (f) evaluations of bids; (g) post-qualification; and (h) award of contract (RA 9184 (2003), Sec. 5(e)). The contract is awarded to the lowest qualified bid. However, Senate Bill No. 2593 seeks to amend the lowest bid standard to the most economically advantageous bid standard, determined through a quality-price ratio.

There are also rules on warranties, minimum rates for liquidated damages, maximum allowable advance payments, and progress payments, etc. (RA 9184 (2003), Arts XIX and XXII).

The Philippine Innovation Act created the National Innovation Council, which is empowered to initiate a technology procurement process to promote technology diffusion and market transformation for the benefit and on behalf of end-users (RA 11293 (2019), Secs 3(u) and 26(c)).

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, parties are free to establish such stipulations, clauses, terms, and conditions as they may deem convenient (Civil Code ("CC"), Art. 1306).

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, parties are free to establish such stipulations, clauses, terms, and conditions as they may deem convenient (CC, Art. 1306).

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes, parties must act with justice, give everyone his due, and observe honesty and good faith, including in the performance of contractual obligations (CC, Art. 19 and 1159). The Consumer Act provides a legal guarantee of product or service adequacy, regardless of an express instrument or contractual exoneration of the supplier (RA 7394, Art.105).

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

If the supplier provides goods, the remedies are specific, substitute, or equivalent performance, and/or damages (CC,

Art. 1191). If the supplier provides services, the remedies are substitute or equivalent performance, and/or damages (CC, Art. 1167 and 1191).

Under the Consumer Act, product and service suppliers may be liable for: (a) replacement of the product by another of the same kind in a perfect state of use, and/or performance of the service without any additional cost, if applicable; (b) immediate reimbursement of the amount paid, with monetary updating, without prejudice to any losses and damages; or (c) proportionate price reduction (RA 7394 (1992), Art. 100 and 102).

If the customer is the Philippine government, it is allowed to terminate the contract if: (a) the supplier fails to deliver or perform the supplies or services within the period in the contract; or (b) the supplier fails to perform any obligation under the contract (GPRA IRR, Annex I).

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Aside from implied warranties under the CC, parties may stipulate additional protections, e.g., liquidated damages, express warranties, or arbitration clauses. Governmental procurement contracts require stipulations concerning: (a) liquidated damages in favour of the government; and (b) the power of the government to rescind the contract once the liquidated damages exceed 10%.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Parties may include provisions on termination without cause, and/or free and harmless clauses. However, damages arising from law and/or quasi-delict cannot be stipulated away.

A contract may be extinguished without the right to damages when: (1) there is loss or destruction of the thing without fault or delay from the obligor (CC, Art. 1262); (2) the service becomes legally or physically impossible to perform (*Id.*, at Art. 1266); (3) the service has become so difficult as to be manifestly beyond the contemplation of the parties (*Id.*, at Art. 1267); or (4) if non-compliance is due to a fortuitous event (*Id.*, at Art. 1174).

2.7 Can the parties exclude or agree additional termination rights?

Yes; however, the courts may equitably reduce liquidated damages stipulated in a contract if they are iniquitous or unconscionable (CC, Art. 2227).

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Parties are free to establish such limits or exclusions provided they are not contrary to law, morals, good customs, public order, or public policy (CC, Art. 1306).

For the supply of consumer products and services, stipulations preventing, exonerating, or reducing the obligation to indemnify for damages effected are prohibited (RA 7394, Art. 106). Stipulations that exempt the licensor from liability for non-fulfilment of his responsibilities under the TTA and/or liability arising from third-party suits brought about by the use of the licensed product or technology, are likewise prohibited (IPOPHL Memo. Cir. No. 2020-002, Rule 2.14).

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, however, it should not be contrary to law, morals, public order, or public policy (CC, Art. 1306).

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

While the same general principles apply, technology procurement contracts may fall under the definition of TTA which has corresponding prohibited and mandatory clauses.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Parties may agree to submit any controversy to arbitration or mediation under the Alternative Dispute Resolution Act, which may be the preferred mode due to the highly technical expertise required technology solution disputes. Disputes that are within the competence of the Construction Industry Arbitration Commission (CIAC) shall be referred to the CIAC (GPRA IRR, Sec. 59.2).

However, nothing prevents parties from directly resorting to courts.

For contracts involving TTAs, IPOPHL Rules require mandatory provisions on applicable law/procedure and venue in the event of litigation and/or arbitration.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

To protect their IP rights in a technology sourcing transaction, parties may enter into a TTA. While generally not required, parties may also have the TTA recorded before the IPOPHL.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes, recordal of agreements and transfer of ownership that involve the transmission of IP rights, through the submission of the notarised or certified assignment document and a signed power of attorney (if made through a representative) to the IPOPHIL, is necessary.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Yes, protection of trade secrets/undisclosed information is expressly recognised as an IP right (RA 8293 (1998); RA 10667

(2015); RA 7394 (1992); Act No. 3815 (1930); and the Agreement on Trade-Related Aspects of Intellectual Property Rights (1995)). Trade secret holders may also opt to: (a) pursue a patent application (if the subject is patentable); (b) enter into non-disclosure agreements or other similar contracts; and/or (c) seek protection in applicable criminal, commercial, and privacy laws.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes, the Data Privacy Act ("DPA") and its Implementing Rules and Regulations ("IRR") and the issuance of the National Privacy Commission of the Philippines ("NPC") regulate all forms of personal data processing, including those in the context of technology services contracts.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside the Philippine jurisdiction either through an outsourcing/subcontracting agreement (if the data controller-data processor relationship between the transferor and the recipient of the data will remain) or a data sharing agreement (in case no such data controller-data processor relationship will remain between the parties).

The DPA and its IRR require that these agreements be made with the consent of the data subject(s) and contain provisions on data privacy protection (DPA, Secs 43–45).

5.3 Are there any legal and/or regulatory requirements concerning information security?

Yes, the DPA and its IRR mandate that reasonable and appropriate security measures for the protection of personal information be enforced (e.g., organisational, technical, and physical measures) (DPA, Secs 25–29) be observed for the protection of personal information against any natural/human dangers, e.g., accidental loss or unlawful destruction or processing.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

In legitimate contracting/outsourcing arrangements, an employee of a service provider/contractor tasked to perform contracted services for a client/principal remains employed by the former. An employee cannot be transferred from one employer to another without the employee's consent. It is not unusual, however, for a service provider to physically deploy employees at the client's premises.

If the arrangement, however, involves labour-only contracting, which is prohibited under Article 106 of the Labor Code and the Department of Labor and Employment's Department Order ("DOLE DO") No. 174, Series of 2017, the law considers the service provider a mere agent of the client, with the client being considered the actual employer of the deployed employees.

6.2 What employee information should the parties provide to each other?

The contracting parties must provide employee information necessary to allow the proper discharge of their respective obligations under the law or their agreement. Any disclosure, however, should be with the consent of the data subject or, even without consent of the data subject, necessary for purposes of the legitimate interest pursued by the contracting parties with due notice to the data subject, in accordance with the DPA. *(Guidelines on Legitimate Interest, NPC Circular No. 2023-7 dated 13 December 2023 and Privacy Policy Office, Advisory Opinion No. 2024-003 dated 2 April 2024.)*

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Yes, provided the grounds for dismissal are among the just or authorised causes under Article 297, 298, and 299 of the Labor Code and upon compliance with procedural due process. Moreover, the client and service provider can only dismiss their respective employees.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, provided the harmonisation will not result in diminution of guaranteed/vested employee benefits.

6.5 Are there any pensions considerations?

In the absence of a more favourable retirement plan or agreement providing for retirement benefits, all employees (whether that of a client or service provider), upon reaching the age of 60 years or more, but not beyond 65 years, which is the compulsory retirement age, who have served at least five years of service may retire and shall be entitled to retirement pay equivalent to at least 22.5 days for every year of service. As a rule, the obligation to provide such retirement pay rests entirely with the actual employer of the retiring employee. In contracting arrangements involving security/protection services, however, the principal/client is required to contribute to the retirement pay of employees deployed by the service provider.

All employers are mandated to register with the Social Security System ("SSS") and remit employer and employee contributions to the SSS pursuant to the Social Security Act.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Yes, foreign employees deployed by the service provider to a client, pursuant to an offshore outsourcing arrangement, should obtain the necessary work permits and visas required by the host country. The parties should also consider the relevant employment laws and benefits of the host country with respect to the terms and conditions of employment of the foreign employee.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Yes, Article 106 to 109 of the Labor Code and DOLE DO No. 174 regulate legitimate contracting arrangements, in general, and prohibit labour-only contracting. The following, however, are not governed by the subject DO: (a) IT-enabled services involving an entire business process such as Business Process Outsourcing ("BPO"), Knowledge Process Outsourcing ("KPO"), IT Infrastructure Outsourcing, among others; (b) contracting or subcontracting arrangements in the construction industry under licensing coverage of the Philippine Contractors Accreditation Board (DOLE DO No. 13, Series of 1998); (c) private security agencies, except with respect to registration requirements (DOLE DO No. 150, Series of 2016 2016 and The Private Security Services Industry Act, R.A. No. 11917); (d) other contractual relationships such as contracts of sale, lease, carriage, management, and such other contracts governed by the Civil Code; and (e) contracting out a job to a professional or individual with unique skills and talent who himself performs the job for the principal.

Under the Special Economic Zone Act, organisations including BPO, KPO, and IT Infrastructure Processing businesses are given fiscal incentives when they operate in certain ecozones (RA 7916 (1995), Sec. 23–24).

Under the DPA, personal information controllers ("PICs") may subcontract the processing of personal information, provided that the PIC remains responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorised purposes, and generally comply with the requirements of the DPA and other laws for processing of personal information.

Some regulatory bodies have also released rules regarding outsourcing applicable entities under their jurisdiction, but these principally deal with accountability and liability concerns, e.g.: (a) *Bangko Sentral ng Pilipinas* ("BSP") Circular No. 1108-21, regulating Virtual Asset ("VA") Service Providers ("VASP"); (b) Insurance Commission Insurance Letter No. 072-18, providing guidelines on BPO activities of insurers/reinsurers; and (c) Securities and Exchange Commission ("SEC") Memorandum Circular No. 5-14, providing guidelines on the outsourcing functions by broker-dealers.

In relation to point (a), "VA" refers to any type of digital unit that can be digitally traded or transferred and can be used for payment or investment purposes. It can be defined as "property", "proceeds", "funds", "funds or other assets", or other "corresponding value". It is used as a medium of exchange or a form of digitally stored value created by agreement within the community of VA users. VAs shall be broadly construed to include digital units of exchange that: (i) have a centralised repository or administrator; (ii) are decentralised and have no centralised repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort. VAs are not issued or guaranteed by any jurisdiction and do not have legal tender status. For purposes of these guidelines, a digital unit of exchange that is used for the payment of: (i) goods and services solely provided by its issuer or a limited set of merchants specified by its issuer (e.g., gift checks); or (ii) virtual goods and services within an online game (e.g., gaming tokens), shall not be considered VAs. Also, virtual currencies as previously defined in BSP Circular No. 944 (Guidelines for Virtual Currency Exchanges) shall now be referred to as VAs. "VASP" refers to any entity that offers services or engages in activities that provide facility for the transfer or exchange of VAs, and which involve the conduct of one or more of the following activities: (1) exchange between VAs and fiat currencies; (2) exchange between one or more forms of VA; (3) transfer of VAs; and/or (4) safekeeping and/or administration of VAs or instruments enabling control over VAs.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Outsourcing transactions generally involve a service agreement between the customer/principal and the supplier/service provider, which contains the terms and conditions governing the performance or completion of a specific job or work being farmed out for a definite or predetermined period.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

The usual approaches are: (a) output-based, i.e., providing milestones upon which compliance and payment will be computed; or (b) performance standards, i.e., an outsourcing agreement is considered to have been performed when the criteria and conditions in the contract have been met.

Damages from substantially performed contracts (CC, Art. 1234), and reimbursements and/or price reduction, may be considered service credits, which may be applied to future contracts/services.

Service credits are not usually applied in the Philippines *vis-à-vis* technology outsourcing agreements.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods are: (a) milestone or progress-based, i.e., charging an amount for every milestone/progression point agreed upon; or (b) output-based, i.e., charging a final price, regardless of the manner in which the service is carried out, for the output intended.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Transferring contracts to service providers may constitute subjective novation, i.e., a change in parties, or assignment of rights. There are no formalities in novation or assignment of rights. Novation may be express or implied.

However, under the DPA, contracts which involve personal or sensitive personal information require that the data subjects give their free, specific, and informed consent in written, electronic or recorded means to the transfer and processing of their data by third parties.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Income tax is levied for income derived within the Philippines (National Internal Revenue Code, Sec. 28(A)). Revenues

related to the outsourced supply/service, such as the fees paid to the service provider, may be construed as taxable revenue of the outsourcing party, since foreign entities engaging in outsourcing transactions are considered to be doing business in the Philippines due to its profit-making nature (*Cargill Inc. v. Intra Strata Assurance Corporation*, G.R. No. 168266, 15 March 2010) and the continuity of its business (*Eriks Pte. Ltd. v. Delfin F. Enriquez Jr., et al.*, G.R. No. 118843, 6 February 1997).

Organisations operating in designated ecozones benefit from fiscal incentives under the Omnibus Investment Code and income tax holidays that have been standardised in the CREATE Law.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

These include data security, preservation and/or recovery, ownership of IP, third-party use, limitations on liability, maintenance and support, destruction of the data, and transfer of ownership upon termination.

These are usually resolved by stipulating guidelines in the software licensing agreement. For on–premise solutions that involve processing of personal information, compliance with the requirements of the DPA, its IRR, and NPC issuances, is required with respect to personal information.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

These include the hardware and software covered, response time for support and maintenance services, the level of "uptime"/"downtime", notification to avail of support and maintenance services, additional fees for out-of-coverage support and maintenance, designation and determination of authorised personnel, maintenance and support when the licensor/vendor "ceases to exist", and data privacy and security.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Escrow arrangements are uncommon due to added costs, a risk of the software in escrow becoming obsolete, and a lack of capacity to implement the software once it is availed.

Under the Financial Rehabilitation and Insolvency Act, escrow arrangements remain enforceable during rehabilitation but are subject to the control and administration of the rehabilitation receiver who may prohibit, or otherwise serve as the legal basis for rendering null and void, the results of any extrajudicial activity upon the escrow (RA 10142 (2010), Sec. 17).

During insolvency proceedings, the arrangement remains enforceable; however, legal title to and control of the assets of the licensor/vendor – including the escrow agreement – shall be vested in the liquidator. Any claim on the escrow arrangement must be coursed through the liquidation proceedings (RA 10142 (2010), Sec. 113).

Enforcement of the software escrow, i.e., relinquishing the developer's ownership over source codes to the beneficiary, is prohibited since this translates into a sale or disposition of assets without the consent of the rehabilitator or liquidator.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

Yes, specific services that comprise "cloud computing services", depending on the technical description of the service, may trigger the application of the Public Telecommunications Policy Act of the Philippines ("PTPA") and its implementing rules which may require a Certificate of Public Convenience ("CPC") or Certificate of Public Convenience and Necessity ("CPCN"), issued by the National Telecommunications Commission ("NTC"), for those engaged in telecommunications. However, the provider will not be considered a public telecommunications entity ("PTE") if it does not have its own network infrastructure and does not provide telecommunications services to the public through its own network, but only in conjunction with the existing network facilities of licensed PTEs and internet service providers. In this case, the relevant regulations of the Department of Information and Communications Technology ("DICT") and NTC on Value Added Services ("VAS") may apply, if these cloud computing services merely enhance telecommunications services.

If the providers are foreign entities with customers in the Philippines, they may be considered as doing business in the Philippines and must be licensed.

For banks and non-bank financial institutions, procurement of cloud computing services must comply with the Information Technology Risk Management Standards under BSP Circular No. 808-13, which requires an integrated approach to risk management, as well as the Enhanced Guidelines on Information Security Management under BSP Circular No. 982, which requires the establishment of a robust and effective technology risk management processes, governance, structures, and cybersecurity controls.

For the public sector, under DICT Department Circular No. 2017-002 entitled "Prescribing the Government's Cloud First Policy", as amended by DC No. 2020-10, Cloud Services may be subject to accreditation and the regulations of the DICT if offered to the Philippine government.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Its use is becoming more common due to efficiency, economic and security benefits highlighted by remote working conditions.

However, cloud computing is not yet widely used in the Philippines considering that effective internet connectivity and availability remain an issue.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Procurers must be cognizant of the applicable regulatory approvals as discussed in the answer to question 9.1 that the cloud service providers must have before being authorised to provide cloud computing services.

Additionally, providers must be compliant with the DPA in relation to processing of personal or sensitive personal information (RA 10173 (2012), Sec. 4), and the Cybercrime Prevention Act, which requires preservation of traffic data and subscriber information (RA 10175 (2012), Sec. 13). This includes

compliance with the DPA and its IRR should the cross-border transfer of personal data of Philippine-based data subjects be required in rendering cloud computing services. Compliance involves securing the consent of the data subjects and the execution of an agreement if there is a separate entity collecting the information from the Philippines ("PIC" or data controller"), and another foreign entity that will process the information in the course of rendering cloud computing services (the "PIP" or data processor). This agreement need not to be registered with the NPC but must contain the mandatory clauses prescribed by the DPA and its IRR.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

Yes: (a) the IP Code, which provides for certain mandatory provisions and specific grounds for cancellation, if the procurement or use of AI-based solutions or technologies is carried out through a licensing agreement; (b) the GPRA, if the procuring entity is the government; and (c) the DPA, if the AI-based solution or technology involves processing personal information.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Collected information alone, in its plain form, even if expressed, explained, illustrated or embodied in a work, is unprotected subject matter and cannot be the subject of ownership rights. However, a copyright over a derivative work can exist over a selection and arrangement of individual components of the compilation as long as they are original by reason of the selection or coordination, or arrangement of their contents. A certain database may be legally protected, if made in accordance with the aforementioned manner.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Algorithms may be considered mathematical methods that are non-patentable and cannot be the subject of patent ownership rights (RA 8293 (1998), Sec. 22.1).

Copyright over algorithms improved or developed by machine learning techniques shall be attributable to the natural person (RA 8293 (1998), Sec. 171.1) who owns the machine (RA 8293 (1998), Sec. 171.1), consistent with *jus fruendi*, i.e., the owner of the property has the right, by accession, to everything produced thereby (CC, Art. 440). If the work is commissioned, the person who commissioned the work shall have ownership rights; however, the copyright remains with the creator unless otherwise agreed upon (RA 8293 (1998) Sec. 178.4).

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

Blockchain-based solutions are covered by BSP Circular No. 1108-21, which requires providers to secure a Certificate of Authority application with the BSP and subjects them to capitalisation requirements, service fees, provisions on wallet security, technology outsourcing, internal controls, consumer protection, and customer due diligence.

In 2019, the SEC released a Notice that it intended to issue Rules on Digital Asset Exchange, proposing that the Rules would require registration, qualifications before the operation of a Digital Asset Exchange, and disallowed activities. Pending the issuance thereof, the SEC has issued advisories warning the public of organisations that purport to invest client funds in digital assets but are not registered with the BSP. However, the SEC decided to delay issuance of these rules until further notice.[1]

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Apart from the financial and banking sector, blockchain-based technology is not yet widely adopted in many other industry sectors in the Philippines.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

These issues involve confidentiality, data privacy and security, data management, data preservation, contract management security, performance monitoring and business continuity, among others.

The thresholds and reportorial requirements under the Anti-Money Laundering Act (RA 9160 (2001) Sec. 8(c)), and the Terrorism Financing Prevention and Suppression Act of 2012 (RA 10168 (2012) Sec. 17) on financing terrorism also apply.

Endnote

1 https://www.philstar.com/business/2023/06/05/2271456/sec-delays-issuance-framework-crypto-assets

Leland R. Villadolid, Jr. is the Co-Managing Partner of ACCRALAW. He specialises in litigation and arbitration principally in the areas of information, telecommunication and technology. He also handles cases in areas of cybercrime and cyber security, public utilities, antitrust and trade regulation, environment and natural resources, consumer protection and product liability. After obtaining his Master of Laws degree, he was awarded a fellowship grant by the United States – Asia Environmental Partnership Program (US-AEP) which enabled him to study at the Environmental Law Institute (ELI) in Washington D.C.

Angara Abello Concepcion Regala & Cruz (ACCRALAW)
22/F, ACCRALAW Tower, 2nd Avenue Corner
30th Street Bonifacio Global City, 1635 Taguig
Metro Manila
Philippines

Tel: +632 8 830 8130
Email: rvilladolidjr@accralaw.com
URL: www.accralaw.com/lawyers/leland-r-villadolid-jr

Chrysilla Carissa P. Bautista is a Partner at ACCRALAW. She leverages her extensive litigation experience. Her complex litigation work involves shareholder disputes, mass tort actions, telecommunications issues and environmental law matters. She has conducted internal investigations involving allegations of self-dealing, fraud, and corruption, and has represented clients before trial and appellate courts and other government or regulatory agencies.

Angara Abello Concepcion Regala & Cruz (ACCRALAW)
22/F, ACCRALAW Tower, 2nd Avenue Corner
30th Street Bonifacio Global City, 1635 Taguig
Metro Manila
Philippines

Tel: +632 8 830 8042
Email: cpbautista@accralaw.com
LinkedIn: www.linkedin.com/in/chrysilla-bautista

John Paul M. Gaba is a Partner of ACCRALAW. His primary practice areas are intellectual property law, e-commerce and cyberspace/IT law, and data protection/privacy and informational privacy.

Mr. Gaba completed his Bachelor of Arts degree in Public Administration (*cum laude*) and Bachelor of Laws degree at the University of the Philippines. He has published local and international articles, and regularly gives lectures on topics related to his practice areas.

Angara Abello Concepcion Regala & Cruz (ACCRALAW)
22/F, ACCRALAW Tower, 2nd Avenue Corner
30th Street Bonifacio Global City, 1635 Taguig
Metro Manila
Philippines

Tel: +632 8 830 8047
Email: jmgaba@accralaw.com
LinkedIn: www.linkedin.com/in/john-paul-gaba-02186a176

Erwin Jay V. Filio is a Partner of ACCRALAW. He has extensive experience handling employment termination disputes and money claims, labour inspections and audits, outsourcing concerns, the labour aspect of M&A, rightsizing and downsizing programmes, collective bargaining negotiations, union organisation issues, and strikes. Mr. Filio also handles labour-related criminal litigation work, which includes criminal prosecutions for unfair labour practice acts, violations of the Revised Penal Code and other special laws. He has also co-authored several articles on outsourcing and various topics on labour-related matters.

Angara Abello Concepcion Regala & Cruz (ACCRALAW)
22/F, ACCRALAW Tower, 2nd Avenue Corner
30th Street Bonifacio Global City, 1635 Taguig
Metro Manila
Philippines

Tel: +632 8 830 8000
Email: evfilio@accralaw.com
URL: www.accralaw.com/lawyers/erwin-jay-v-filio/

Founded in 1972, ACCRALAW is a cohesive multi-disciplinary team of legal professionals with in-depth knowledge of specialised legal fields. With 52 years of experience in Philippine law, the firm has grown to a prestigious service organisation of 170 lawyers and 178 non-legal personnel.

A top-tier institutional firm, ACCRALAW is based at ACCRALAW Tower in Bonifacio Global City, Metro Manila, and has full-service branches in Cebu City and Davao City – thriving commercial and business centres. The firm is linked to a global network of correspondent lawyers, law firms, and Bar Associations.

www.accralaw.com

Singapore


Jeremy Tan


Chester Lim

Bird & Bird ATMD LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

There is no legislation in Singapore that regulates the procurement of technology products and services in the private sector. However, sector-specific rules may apply to certain types of technology procurements, particularly in the financial services sector (see question 7.1).

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The public procurement of technology products and services is regulated by the Government Procurement Act 1997 ("**GPA**") and its subsidiary legislation, which include the:

- Government Procurement (Application) Order ("**GP Order**"), which sets out the relevant states, contracting authorities and procurements which are subject to the GPA and procurements which are excluded from the GPA;
- Government Procurement Regulations 2014 ("**GP Regulations**"), containing the procedure for procurements subjected to the GPA, including the principles for evaluating and awarding procurement contracts; and
- Government Procurement (Challenge Proceedings) Regulations, which establish the framework for challenges brought by a supplier before the Government Procurement Adjudication Tribunal on procurements governed by the GPA.

Additionally, there are non-binding guidelines published by the Ministry of Finance such as the procurement guidelines on the Government Electronic Business portal ("**GeBIZ**") and the Public Private Partnership Handbook ("**PPP Handbook**"), which set out the government procurement procedures for public-private partnership projects.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, it does not.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, it does not.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Singapore law does not have any legal requirements of fairness or good faith in relation to contracts generally or specifically for technology-related contracts.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The following remedies are available to the customer under general law:

- damages;
- specific performance/injunction (available at the discretion of the court); and
- termination.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In addition to the remedies available at law, the customer could seek the following protections:

- service credits;
- indemnities from the supplier for loss suffered by the customer in specified circumstances;
- other forms of financial consequences, such as loss of exclusivity, a reduction in the price payable to the supplier or the right to withhold payment;
- warranties;
- step-in rights allowing the customer to take over management of an under-performing service or to appoint a third party to manage the service on its behalf;
- specific provision for termination in defined circumstances (for example, material breach or insolvency);
- a requirement for the supplier to hold insurance and note the customer's interest on its insurance policy;
- a parent company guarantee; and
- an appropriate governance or escalation structure.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Any termination that occurs in accordance with the terms of the contract would be justified without giving rise to a claim for damages from the terminated party.

In addition, the following events are considered sufficiently serious to justify immediate termination, regardless of the terms of the contract:

- a repudiatory breach, i.e., a breach of a condition or a breach of a contractual term that would deprive the innocent party of "substantially the whole benefit of the contract";
- a breach that indicates that the counterparty no longer wishes to continue with the contract or honour their obligations under the contract; and
- if the contract is frustrated, i.e., through no fault of the parties, the performance of the contract becomes impossible or if external events conspire to make it radically different from what was originally envisaged by the parties.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties can exclude or agree to additional termination rights.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

In most business-to-business contracts, the parties are free to exclude liability altogether, put a financial cap on liability, restrict the types of losses recoverable or remedies available and/or impose a short time limit for claims which are always subject to the following:

- under the Unfair Contract Terms Act ("**UCTA**"), it is not possible to exclude or restrict liability for death or personal injury resulting from negligence. In the case of other loss or damage, the exclusion or restriction of liability for negligence must satisfy UCTA's reasonableness requirement;
- an exclusion or restriction of liability for fraud or fraudulent misrepresentation is unenforceable;
- exclusions or restrictions of liability for pre-contractual negligent or innocent misrepresentation must satisfy the requirement of reasonableness under UCTA; and
- liability for breach of the terms implied by section 12 of the Sale of Goods Act ("**SGA**") (i.e., the right to sell, freedom from encumbrance and quiet enjoyment) cannot be excluded or restricted, while liability for breach of the terms implied under sections 13, 14 and 15 of the SGA (i.e., satisfactory quality, fitness for purpose and certain other matters) can only be restricted in business-to-business contracts where this meets UCTA's reasonableness requirement.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, subject to the limitations set out in question 2.8 above and the reasonableness test under UCTA.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, they do not.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

The main methods of dispute resolution used for technology services contracts are court litigation and arbitration. Additionally, it is common for parties to a technology services contract to include certain levels of "alternative dispute resolution" as preliminary steps to be taken in order to try to resolve a dispute before the final stages of litigation or arbitration. Such steps often include mediation, commercial negotiation and escalation and having disputes of a technical nature resolved by expert determination.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In the technology services contract, the parties will define which intellectual property ("**IP**") rights belong to each party at the start of the technology transaction ("**Background IP**"). This Background IP will be ring-fenced such that only prescribed use by the other party will be permitted. This will typically be accomplished by way of an IP licence within the scope of the technology services contract. The intention is that any use outside of those parameters will be prohibited.

The parties will also have to consider what new IP rights may come into existence during the course of the technology transaction ("**Foreground IP**"). The technology services contract will need to make provisions for who will own the Foreground IP and what permission may have to be sought in order to make use of it.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes – different formalities apply depending on the IP right being assigned:

- for patents, trade marks and registered designs, the assignment must be in writing and signed by the assignor. The assignment must be recorded with the Intellectual Property Office of Singapore in order to be effective against a third party who acquires rights in the patent, trade mark or registered design without notice of the assignment; and
- for copyright, the assignment must be in writing and signed by the assignor. There are, however, no registration requirements.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Know-how, trade secrets and other business critical confidential information are protected by the law of confidence under common law. If confidential information is disclosed under circumstances that demonstrate that the information is confidential, the party receiving the information has a duty to keep the information confidential. Failure to do so constitutes the tort of breach of confidence.

However, parties will typically agree to confidentiality provisions in technology services contracts rather than relying on confidentiality protection at common law. Confidentiality provisions in a technology services contract are likely to:

- define the know-how, trade secrets and confidential information of each party;
- create a contractual duty to maintain this information in confidence (subject to some typically agreed carve-outs);
- specify its use within the scope of the IP licence (see question 4.1 above); and
- define the duration of the confidentiality undertakings (for a fixed period or potentially indefinitely depending on the perceived value of the confidential information).

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

The processing of personal data is regulated by the Personal Data Protection Act 2012 ("**PDPA**"). Sector-specific rules may also apply to certain types of technology services contracts, particularly in the financial and healthcare sectors.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Personal data can be transferred outside Singapore, but the organisation will need to ensure that the recipient of the data confers on the personal data a standard of protection that is comparable to that under the PDPA. This can be achieved through various mechanisms, including:

- entering into a data transfer agreement which requires the recipient of the data to provide the personal data with a level of protection that is comparable to the PDPA;
- obtaining the individual's consent to the transfer, subject to such consent satisfying certain prescribed conditions including giving the individual a summary in writing of how his or her personal data will be protected to a standard comparable to the PDPA; or
- confirming that the recipient is certified under the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System or Asia-Pacific Economic Cooperation Privacy Recognition for Processors System.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The PDPA sets out baseline standards that all organisations must meet in relation to the protection of personal data. An organisation is required under the PDPA to protect the personal data in its possession or control by making reasonable security arrangements to prevent:

- unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

Sector-specific information security requirements may apply to certain types of technology services contracts. For instance, the Monetary Authority of Singapore ("**MAS**") issues various notices and guidelines on cybersecurity applicable to financial institutions.

Certain organisations may have their computer system designated as critical information infrastructure ("**CII**") under the Cybersecurity Act 2018. A full discussion of this law is beyond the scope of this chapter but, in summary, owners of CII must comply with codes of practice and standards issued by the Cybersecurity Agency of Singapore. Accordingly, if the customer falls within such scope of the Cybersecurity Act, additional obligations may need to be added to the technology services contract to facilitate the customer's continued compliance with the Cybersecurity Act. It should be further noted that the Cybersecurity (Amendment) Act was passed on 7 May 2024, and once it enters in force, a greater number of entities will be regulated. The Cybersecurity (Amendment) Act expands the scope of the Cybersecurity Act to include owners of systems of temporary cybersecurity concern ("**STCC**"), entities of special cybersecurity interest ("**ESCI**") and major foundational digital infrastructure service providers ("**FDI**").

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

There is no legislation in Singapore that regulates the transfer of employees in connection with an outsourcing transaction or other contract for the provision of technology-related services.

Employees are only transferred by operation of law where a part of a company's business is transferred to another company, for instance in the context of the sale of a business. Otherwise, a transfer of employees is typically affected by terminating the employee's existing employment contract and then employing that same employee through the new employer.

6.2 What employee information should the parties provide to each other?

There is no legislation in Singapore that prescribes the types of employee information that parties should provide to each other. It should be noted that the PDPA restricts an employer's ability to disclose employee data to another party unless the employee's consent has been obtained, or if deemed consent or an exception to consent applies.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Yes, this is subject to the position under general employment law. An employee may, at any time, be dismissed in accordance with his or her employment contract or in the absence of an

employment contract, in accordance with the Employment Act. This dismissal may be for any reason including the outsourcing of that employee's role. Dismissals usually involve a notice period or payment *in lieu* of providing notice.

If the customer or service provider is undergoing a retrenchment exercise, it must notify the Ministry of Manpower ("**MOM**") if certain thresholds are met. The employer is also encouraged to comply with the advisories and guidelines issued by the MOM in relation to responsible retrenchment.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes. As explained in question 6.1 above, a transfer of employees is typically affected by terminating the employee's existing employment contract and then employing that same employee through the new employer. The terms of the employment contract will depend on negotiations between the employee and the new employer.

6.5 Are there any pensions considerations?

No, as Singapore law does not have any legislation relating to pensions. However, it should be noted that a new employer has a legal obligation to contribute a portion of the transferred employee's salary to the Central Provident Fund ("**CPF**"), which is a mandatory savings account with contribution rates fixed by law.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

No, the legal position as set out above applies to offshore outsourcing.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

While there are no national laws or regulations that regulate outsourcing transactions generally, there are sector-specific rules that may need to be considered in relation to certain types of outsourcing transactions.

For instance, the following MAS notices and guidelines are relevant to technology outsourcing arrangements entered into by a financial institution:

- MAS Guidelines on Outsourcing – which set out the regulatory requirements on outsourcing for financial institutions. From 11 December 2024, the current MAS Guidelines on Outsourcing will be superseded by a new set of outsourcing notices and guidelines, namely MAS Notice 658 Management of Outsourced Relevant Services for Banks, MAS Notice 1121 Management of Outsourced Relevant Services for Merchant Banks, MAS Guidelines on Outsourcing (Banks) and MAS Guidelines on Outsourcing (Financial Institutions other than Banks);
- MAS Technology Risk Management Guidelines and the Notices on Technology Risk Management – which set out the risk management principles and best practice standards to guide financial institutions in establishing sound and robust technology risk governance and oversight, and maintaining cyber resilience; and
- section 47 of the Banking Act and the MAS Notice on Banking Secrecy – Conditions for Outsourcing (collectively, "**Banking Secrecy Rules**"). Please note that the Banking Secrecy Rules are relevant only to entities which are regulated under the Banking Act (e.g., banks, merchant banks) and not to other types of financial institutions regulated by the MAS.

While the Telecommunications Act does not prohibit a telecommunications operator from entering into outsourcing arrangements, the licences granted by the Infocomm Media Development Authority ("**IMDA**") may contain restrictions that will impact such outsourcing arrangements. For instance, a Service-Based Operator (Individual) Licence issued by the IMDA will typically hold the licensee liable for any act, omission, default, neglect or otherwise of the licensee's agents, independent contractors or sub-contractors when carrying out any work or providing any service.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The most common types of legal or contractual structure include:

- direct outsourcing – where the customer directly contracts with the technology provider;
- multi-sourcing – where the customer enters into contracts with different suppliers for separate elements of the outsourcing transaction;
- indirect sourcing – where the customer contracts with a technology provider, which then subcontracts the work to different suppliers; and
- joint venture – where the customer sets up a joint venture with the technology supplier. This may take the form of a corporate joint venture or a contractual joint venture.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Technology outsourcing agreements between the customer and technology supplier will typically set out pre-defined target service levels. If these service levels are not met, the supplier will provide a pre-defined quantity of service credits with which the customer can offset future payments for the services.

The supplier will typically want the service credits to be the sole remedy of the customer for the particular failure, but this should be without prejudice to the customer's wider rights in relation to more serious breaches of the contract or persistent service failures. Service credits are generally enforceable, provided they are not a contractual penalty.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The method of charging will depend on the type of services being outsourced, the nature of the supplier's appointment and the balance of risk between the parties.

The most common charging methods are as follows:

- fixed price – where the amount charged is a fixed amount regardless of the customer's consumption;

- consumption-based – where the customer is charged based on how much of the service is utilised;
- cost-plus – where the amount charged is the cost-price of the technology solution plus a mark-up; and
- gain-sharing – where the technology supplier has a share in the revenue generated by the customer's implementation of the technology solution.

Agreements typically include a mechanism for pricing to be adjusted. This could be with reference to a mutually agreed benchmark.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Third-party contracts can be transferred to a service provider by way of an assignment or novation.

An assignment is the transfer of the benefit of a contract from one party to another. However, the burden of the contract (e.g., the obligation to make payment) cannot be assigned to the other party. A legal assignment must be:

- in writing, clearly identifying the rights to be assigned;
- signed by the assignor;
- absolute; and
- notified in writing to the other party.

Novation is a transfer to a third party of both the benefit and burden of a contract, essentially by extinguishing the original contract and replacing it with a new contract. There are no formalities for a novation under Singapore law.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The transfer of certain assets to the supplier may produce taxable gains and be subject to corporate tax. Stamp duty is also payable on the transfer of shares and immovable property. If the transfer of assets involve a taxable supply of goods and services, Goods and Services Tax ("**GST**") will apply unless an exemption applies.

GST (currently at 9%) is levied on the supply of goods and services in Singapore. A supplier can zero-rate its supply of services (i.e., charge GST at 0%) to the extent that the service falls within the description of international services under section 21(3) of the Goods and Services Tax Act.

A GST-registered customer procuring technology services from an overseas supplier is subject to the reverse charge regime for business-to-business supplies of imported services and will be required to account for GST on the imported services (except for certain services which are specifically excluded from the scope of the reverse charge). The customer is also entitled to claim GST as input tax, subject to the normal input tax recovery rules.

Corporate income tax (currently at 17%) applies to the income derived by companies from corporate transactions. There is no capital gains tax in Singapore.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

The key issues a customer would typically consider include:

- licence grant and scope;
- timing of delivery and installation of the software;
- delivery of the source code, design documents and technical information for the software;
- acceptance testing;
- maintenance, patches and updates to the software;
- fees and timing of payment;
- confidentiality of customer data;
- IP rights, including ownership of IP in the software and protection of the customer's Background IP;
- warranty that the software has been screened for viruses and other unauthorised code;
- use of third-party or open source software and IP rights in relation to such third-party or open source software;
- warranties and indemnities, particularly in relation to the IP in the software;
- limitations of liability; and
- termination rights in the event of breach by the supplier, particularly non-delivery of the software and where the software does not conform to the customer's specifications.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

The key issues in relation to support and maintenance of software typically include:

- service levels and service credits;
- response and resolution times;
- frequency of scheduled maintenance and patches;
- payment schedule;
- confidentiality of customer data;
- IP rights and ownership;
- warranties and indemnities;
- limitations of liability; and
- termination rights in the event of breach by the supplier, particularly non-delivery of the support and maintenance services.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Software escrow arrangements are used in Singapore, but in practice most customers will not insist on an escrow arrangement (unless the software is truly bespoke to the vendor) as:

- a software escrow involves additional costs;
- the software in escrow may become obsolete if not maintained; and
- the customer calling on the escrowed software may ultimately lack the ability to implement the software.

Software escrow arrangements are enforceable in the case of the insolvency of the licensor/vendor of the software.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

There are no laws or regulations in Singapore that regulate the procurement of cloud computing services in general. However, sector-specific rules may apply to the procurement of cloud computing services in certain sectors such as in the financial services sector.

The Personal Data Protection Commission ("**PDPC**") has also issued non-binding policy papers and guidelines on matters relating to cloud computing services. These include:

- an infographic on Good Practices to Secure Personal Data in the Cloud Platform; and
- a dedicated chapter on cloud services in the PDPC's Advisory Guidelines on the PDPA for Selected Topics.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions are widely adopted in Singapore, including private, public and hybrid solutions.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Customers procuring cloud computing services should consider:

- service levels and service credits;
- IP rights, particularly ownership of the customer's IP;
- confidentiality of customer data;
- track record of cloud provider including in relation to cybersecurity and data policies and practices;
- location of where the data is stored;
- audit and record keeping requirements; and
- business continuity requirements.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

There are no laws or regulations in Singapore that specifically regulate the procurement or use of AI-based solutions or technologies. However, various governmental and regulatory agencies have issued non-binding policy papers and guidelines on matters relating to AI. Recent examples include:

- the PDPC's Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems, which among other things provide organisations with clarity on the use personal data to train or develop AI and set out best practices for how third-party developers of AI systems can support their customer organisations in implementing AI systems;
- the PDPC and IMDA's A.I. Verify, which is a governance testing framework and toolkit to verify the performance of an AI solution against internationally accepted AI ethics principles;
- the PDPC's Model AI Governance Framework ("**PDPC Model AI Governance Framework**"), which is a set of industry-agnostic guidelines developed by the Singapore data protection regulator;
- the AI Verify Foundation and IMDA's Model AI Governance Framework for Generative AI, which is a set of guidelines that expand on the PDPC Model AI Governance Framework to address generative AI concerns; and
- the MAS' Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector ("**MAS FEAT Principles**"), which are a set of principles and best practices for AI developed specifically for the financial services sector.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

In general, it is not possible to legally own and license data used to train machine learning-based systems, as data *per se* does not qualify for protection under Singapore's IP laws. Singapore does not recognise a *sui generis* database right, unlike the position in the European Union.

Having said that, a database owner would be able to claim legal ownership over the compilation of the data, and license it contractually, if it can demonstrate that the database qualifies for protection under Singapore's copyright law. A full discussion of this is beyond the scope of this chapter but, in broad terms, a database would qualify for copyright protection if the compilation of data constitutes an intellectual creation by reason of the selection or arrangement of its contents.

Alternatively, a database owner can rely on the law of confidence to protect the data from unauthorised disclosure allowing the owner of confidential information to bring an action against the recipient of the data if confidential information was disclosed by the recipient in breach of confidentiality obligations.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Generally, algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer are unlikely to qualify for IP protection.

Under the Patents Act, an algorithm *per* se will not qualify for patent protection. The Intellectual Property Office of Singapore ("**IPOS**") has stated in its IP and Artificial Intelligence Information Note that mathematical methods, i.e., algorithms *per se* are not considered to be inventions. In order to qualify for patent protection, there must be an application of the machine learning techniques to solve a specific problem in a manner that goes beyond the underlying mathematical method or algorithm, such as using the machine learning techniques to control the navigation of an autonomous vehicle. Apart from patent protection, algorithms could potentially be protected by copyright as original literary works. However, an AI or machine learning system cannot be considered the creator of such works under the Copyright Act. The current position adopted by the Singapore courts is that only natural persons may be considered authors of works, although ownership of the copyright in works may be assigned to legal persons such as companies. Accordingly, the creative elements of a work must be attributable to a natural person before copyright protection can arise. Under the present copyright regime, the courts have noted that "in cases involving a high degree of automation, there will be no original work produced for the simple reason that there are no identifiable authors" (*Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 at [81]). Therefore, unless there is a strong human influence on the AI process (such that the AI does not operate autonomously), there is no copyright protection for AI-generated work results.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There is no specific legislation in Singapore regulating the procurement of blockchain-based solutions.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

There is diverse adoption of blockchain in Singapore across various industry sectors including:

- healthcare data including certification for vaccination records;
- airline payments and loyalty programmes;
- education certificates; and
- real estate transactions.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

As blockchain-based technology is not specifically regulated under Singapore law, the key legal issues are the same as those applicable to technology procurement generally.

Jeremy Tan is an international technology, media and telecoms lawyer based in Singapore, advising a broad range of clients across the Asia-Pacific region. He is the managing partner of Bird & Bird's Singapore office and the co-head of Bird & Bird's International Privacy and Data Protection Group.

He advises an international clientele drawn from a broad range of sectors, including financial services, healthcare and telecommunications, on technology sourcing, outsourcing, fintech, communications and data protection matters. He also has extensive experience in large-scale multi-jurisdictional sourcing and outsourcing arrangements, services arrangements, commercial transactions and technology tenders.

He has particular expertise on the legal, regulatory and commercial issues arising in the digital space, as well as specific fields such as payments, the internet of things, artificial intelligence, distributed ledger technology, cybersecurity and cloud computing.

Bird & Bird ATMD LLP
2 Shenton Way
#18-01 SGX Centre 1
Singapore 068804

Tel: +65 6534 5266
Email: Jeremy.Tan@twobirds.com
LinkedIn: www.linkedin.com/in/jeremy-tan-twobirds

Chester Lim is a technology, media and communications lawyer advising clients across Asia-Pacific on commercial, regulatory and public policy matters.

He advises clients on the legal, regulatory and commercial issues that arise in the digital space. This includes technology sourcing, outsourcing, data protection, cybersecurity and licensing matters. His focus is on commercial and advisory work, with clients drawn from a number of industries including financial services, healthcare, retail and telecommunications.

He also has significant experience advising on public policy matters, including assistance provided to a Southeast Asian government as part of a World Bank-funded initiative to draft its data protection and cybersecurity laws.

Bird & Bird ATMD LLP
2 Shenton Way
#18-01 SGX Centre 1
Singapore 068804

Tel: +65 6534 5266
Email: Chester.Lim@twobirds.com
LinkedIn: www.linkedin.com/in/chester-lim-44b63726

Bird & Bird has more than 1,600 lawyers in 31 offices across Europe, the Middle East, Asia-Pacific and North America and clients based in 118 countries worldwide. We specialise in combining leading expertise across a full range of legal services and aim to deliver tailored local advice and seamless cross-border services.

Our technology sourcing practice is widely recognised as having a leading reputation in the field and enjoys top tier international rankings in the *Chambers* and *The Legal 500* Guides to legal profession. We advise on the full range of technology transactions, including complex outsourcings and managed services deals, system implementation projects, telecoms infrastructure and regulatory matters, strategic alliances and collaboration agreements, cloud computing deals and contracts for the deployment of AI and blockchain-based solutions.

www.twobirds.com

Bird & Bird

Sweden

Anna Fernqvist Svensson

Arvid Rosenlöf

Hellström Law

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

There are certain provisions to consider in the Swedish Electronic Communications Act (2022:482). The Act aims to ensure that individuals and public authorities have access to secure and efficient electronic communications and to maximise the benefits for all electronic communications services in terms of choice, price, quality and capacity. There is also sector-specific legislation, for example within the financial sector, see, e.g., question 7.1 below.

The EU Digital Services Act ("DSA") and the Digital Markets Act ("DMA") regulate online platforms (such as social media platforms and marketplaces) and since 17 February 2024, both Acts are applicable and need to be considered in Sweden.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

In Sweden, public procurement is regulated through several laws and regulations. It depends on the activities of the government or public sector body and what is to be procured as to which law is applicable. Most public contracts are regulated through the Swedish Public Procurement Act (2016:1145). The Swedish Act on System of Choice in the Public Sector (2008:962), the Swedish Act on Procurement in the Utilities Sector (2016:1146), the Swedish Act on Procurement of Concessions (2016:1147) and the Swedish Defence and Security Procurement Act (2011:1029) may instead be applicable in certain situations.

There are five principles which are applicable on public procurement stemming from EU law, which governs public procurement processes in Sweden. These are the principles of proportionality, transparency, mutual recognition, non-discrimination and equal treatment. Overall, the entire procurement process must thus be made in a manner which is proportionate and transparent and also objective and neutral.

Even though public procurement of technology products and services is not regulated through a specifical law, Chapter 6, Section 14 of the Swedish Public Procurement Act (2016:1145) should be noted. The provision states that a contracting authority may use a negotiated procedure without prior advertising if the goods to be procured can only be provided by a particular supplier because no other player on the market is capable of providing the product or the service in question. The rule corresponds to Article 32(2)(b)(ii) of Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

In Sweden there is a general freedom of contract. This also applies for technology-related solutions and services contracts. Specific rules apply for business-to-consumer relationships.

For public procurement, the maximum term allowed for a framework agreement in accordance with the Swedish Procurement Act (2016:1145) is four years, unless specific reasons for an extension applies. Under the Swedish Act on the Procurement in the Utilities Sector (2016:1146), there is a maximum term for a framework agreement of eight years.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

There is no maximum length of the notice period regulated in the Swedish Contracts Act (1915:218) as the parties are free to agree on a notice period of their choice. If there is no notice period stipulated in a contract, the applicable notice period should, according to case law, be determined in accordance with what is reasonable. The telecom industry is an exception, being distinctly regulated in the Swedish Electronic Communications Act (2022:482), in which the maximum length of the notice period is set to a month for consumers. Competition law rules may also have to be considered, especially if relationships are exclusive.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

The Swedish Contracts Act (1915:218) contains a general clause applicable to all contracts, stating that any provisions in a contract can be dismissed if found "unreasonable". The provision is seen as a test of fairness.

The terms of contracts that businesses use for consumers must be fair in accordance with the Swedish Act (1994:1512) on Contract Terms in Consumer Relationships. Fair implicates that the terms comply with applicable laws and regulations and that they do not favour the business at the expense of the consumer.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

There are a variety of remedies available under general law. Different types of claims depend on the current contract (e.g., purchase contract or service contract). If a supplier breaches the contract, a customer can demand rectification (e.g. repair), a replacement of a product, cancellation of the purchase or withhold the payment. If the breach is severe, damage claims can be filed against the supplier.

The National Board for Consumer Complaints ("ARN") is a Swedish authority that examines disputes between consumers and businesses. A decision from ARN is a recommendation on how the dispute should be resolved.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Such remedies can include liquidated damages in case of any delays from the service provider or step-in rights if the service provider needs to be replaced with a third party. If there is a major breach from the service provider, specific terms for termination usually apply.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Often the parties have agreed upon a specific notice period. If a party wants to terminate the contract without observing such a notice period, that party may be in breach of contract, unless there are clauses in the contract stipulating the right to terminate the contract due to specific mentioned circumstances such as, e.g., delays of supplies, etc., and such circumstances have occurred. Such clauses are often included in contracts. Provisions giving a right for a party to terminate the contract, to cease to be applicable immediately and paying a termination fee may also be included. As regards consumers, special rules may apply, such as e.g. the rules regarding telecommunications contracts and that it is only permitted to set a period of 24 months as the maximum contractual commitment. If the consumer would like to end the contract even though, e.g. five months remain on it, the provider of the services may require the consumer to pay an early termination fee which may amount to the remaining five months in one lump sum.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties may generally agree on additional termination rights since there is a general freedom of contract in Sweden.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

In the private sector, the parties may fully limit or exclude their liability in the agreement.

For public procurement, the terms stated in the contract must align with the principle of proportionality, meaning that the terms of the procurement must be proportionate in relation to the service performed. Some procurements procedures do not allow any negotiation of contract terms. Once the public procurement process is complete, the finalised contract must adhere to rules of the Swedish Contracts Act (1915:218) and general contract principles.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes; however, the financial cap can be found unreasonable under the previously mentioned Section 36 of the Swedish Contracts Act (1915:218) and be dismissed.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, the principles apply on all the above; however, there may be exceptions in the form of regulations concerning specific areas.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

The parties may agree on a specific dispute resolution method of their choice, as well as the governing law. In business-to-business relationships, arbitration is the most common method, and for the public sector, court litigation is often the preferred choice.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The intellectual property of each party is often protected in such transactions, with certain clauses pertaining to intellectual property rights. These often include clauses of specific ownership determination.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Assignment of intellectual property rights can be done through written or oral agreements or, in some cases, through implication. Some intellectual property rights must be registered with the Swedish Patent and Registration Office. For EU-trademarks, e.g., the assignment of Intellectual Property Rights must be done in writing, unless it is a result of a judgment in accordance with Article 20(3) of the European Union Trademarks Regulation (2017/1001).

The Swedish Patent Act (1967:837) should be considered when applying for patents. If an employee invents something that is patentable, there are certain rules that apply for such invention in the Swedish Act (1949:345) on the Right to Employee Inventions.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Trade secrets are protected in the Swedish Act on Trade Secrets (2018:558), which is applicable on information on business or operating conditions and know-how, as long as: (1) the information is not generally known or easily applicable; (2) the holder has taken reasonable steps to keep the information secret; and (3) the disclosure of the information is likely to cause damage in terms of competition for the holder.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes, processing of personal data is regulated by the General Data Protection Regulation (EU) 2016/679 (GDPR), supplemented by the Swedish Data Protection Act (2018:218) and the Swedish Ordinance (2018:219), with supplementary provisions to the EU General Data Protection Regulation. There is also sector-specific legislation impacting data protection, for example the Swedish Camera Surveillance Act (2018:1200), the Swedish Credit Information Act (1973:1173) and the Swedish Criminal Data Act (2018:1177) implementing directive (EU) 2016/680 on data protection for law enforcement authorities.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Within the EU/EEA, personal data can flow freely but personal data can only be transferred outside of the EU/EEA if certain criteria are met. Such transfer can be permitted if there is a so-called adequacy decision by the European Commission, ensuring that a non-EU/EEA country upholds an adequate level of protection. A transfer can also be permitted if appropriate safeguards are in place, such as Binding Corporate Rules ("BCRs") or Standard Contractual Clauses ("SCCs"). Specific situations and individual cases may also affect the possibility of a third country transfer. Overall, high standards are required to be fulfilled if private and public actors want to transfer personal data outside of the EU/EEA.

A data protection assessment can also be deemed necessary in accordance with Article 35 of the GDPR, depending on the personal data being transferred. It is worth noting that the European Commission adopted its adequacy decision for transfers from the EU/EEA to the United States on 10 July 2023.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The Swedish Protective Security Act (2018:535) and the Act on Information Security for Essential and Digital Services (2008:1174) contain important legal requirements concerning information security. The latter implements the NIS directive (EU) 2016/1148, which is an EU-directive aiming to ensure the overall cyber-security within the region. The Protective Security Act contains legal requirements for both private and public actors who conduct activities classified as security sensitive.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Yes, there is a right for employees to be transferred to the new entity in case of a transfer of either the whole or a part of the business where the employee is based. The right is stated in the Swedish Employment Protection Act (1982:80). The right is an implementation of Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses. To determine whether a transaction counts as a transfer of business, an overall assessment is required. The transferred business shall constitute an economic entity and the economic entity shall have retained its identity.

The employees concerned have the right to object to the transfer of their employment. In such case, the current employment shall stay with the current employer. It is then likely that the employment is terminated due to redundancy if that entity no longer conducts any business.

Certain rules and procedures apply if one of the parties is bound by a collective bargaining agreement. The transferring party is obliged to negotiate with the parties which the employer is bound by a collective agreement with, in accordance with the Swedish Employment (Co-Determination in the Workplace) Act (2021:1114). Prior to the transfer, the transferring party must ask the employees affected by the transfer if they are members of an employee organisation, and must then negotiate with any and all organisations concerned.

6.2 What employee information should the parties provide to each other?

The transferring party should inform the new employee regarding the applicable terms and conditions of the employment relationship. In some cases, the new employer is obliged to apply the transferring party's collective bargaining agreement in a transitional period of up to one year, making it a requirement to provide such information before the transaction takes place.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

No, neither party can dismiss an employee solely based on a transfer of business. However, an employer is not prevented from terminating employees based on economic, technical or organisational reasons that entail changes in the labour force.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

As a starting point, the employees being transferred keep the

current salary and terms of employment. The employment contract does not need to be rewritten to be valid with the new employer. There is nothing preventing the new employer from offering a transferring employee new terms, but the employee must agree to such offer.

The period of employment from the previous employer is added to the period with the new employer. It is important to consider when it comes to the priority rules of the new employer. In Sweden, businesses need to consider a principle of "first in last out" when it comes to redundancy, making it important to keep track of employees' total period of employment.

6.5 Are there any pensions considerations?

The Swedish Employment Protection Act stipulates an exception for the new employer regarding pensions considerations. This means that the employee cannot direct claims against the new employer when it comes to unpaid pension contributions prior to the transfer of activities.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Yes, employee transfer considerations are applicable when it comes to offshore outsourcing.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Yes, the Swedish Professional Secrecy Act (2020:914) is applicable when a public authority entrusts a company or a private service provider with the task of solely processing or storing technical data. According to the Act, any person that engages in a service provider's business with the task of processing or storing technical data has a secrecy obligation and must not disclose or use any information without authorisation. Entities falling under the scope of the Swedish Protective Security Act (2018:585) must enter into a so-called security protection agreement before a counterparty can gain access to any of the security sensitive information of the entity. Therefore, the act must be considered for security sensitive entities before an outsourcing transaction takes place.

Financial actors (e.g. banks, investment funds, security market companies) that wish to make an outsourcing transaction for a party to perform certain financial services, must notify the Swedish Financial Supervisory Authority and submit the outsourcing agreement, before making the transaction in order to obtain approval. The Authority's application for such transfers is considered equivalent to the European Banking Authority's ("EBA") guidelines on outsourcing.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Usually, the contractual structure of such a transaction consists of a master service agreement with several appendices covering, e.g. data processing agreement, pricing and the service levels. The structure and details of each transaction must of course be assessed on a case-by-case basis.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Service levels and service credits are often included in such an agreement. Such terms state the availability of the services and response times. A breach of the service level can have a bearing on the validity of the main service agreement.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Usually, the charging method consists of a basic fee and variable fees based on variables such as usage or other criteria.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

It depends on what is stated in the third-party contract. If it is not regulated or not accepted, the approval of the third-party is usually needed. Data protection requirements such as data processing agreements need to be completed if any contracts are to be transferred to a third party, as personal data often is handled regarding an outsourcing transaction. Usually, the main parties have already agreed the process of how the data controller should be notified if a third-party contract needs to be transferred.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

For tax advice and tax-related questions, we recommend seeking specific tax advice. From our experience, value-added tax ("VAT") may be applicable for an outsourcing transaction if it only involves transferring of specific assets. However, VAT is usually not applicable if the transaction is defined as a transfer of business.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

On-premise solutions can help reduce risks regarding handling of personal data and sensitive information relating to the customer's business. Key issues for a customer often relate to integration possibilities, maintenance, security solutions and costs.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Key issues to consider are the description of the services, service levels, processing of personal data and security, secrecy-regulations, penalties, right of termination, rights of use, remuneration and term of the contract. For public authorities there are public procurement regulations to consider before procuring such service. The key issues also depend on the customer's need and the industry in which the customer is active and therefore the need for updates, bug-fixes and continuous support may vary.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

It is difficult to estimate how common such arrangements are, but they can be used. The Stockholm Chamber of Commerce ("SCC") provides a model escrow agreement for such arrangement. However, the model does not consist of any clause relating to bankruptcy. The SCC also offers companies a service for secure storage. The offered depositing protects the party procuring the services if something unexpectedly happens to the licensor of the software.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No, in Sweden there are no such specific laws. However, in July 2023, legislative changes were introduced in the Public Access to Information and Secrecy Act (2009:400) to simplify the process for outsourcing, such as cloud computing services, for the public sector.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Such solutions are widely adopted, both for the private and public sector.

9.3 What are the key legal issues to consider when procuring cloud computing services?

In addition to what has been mentioned in the answer to question 8.2, the following shall be observed. As it is common that cloud computing services providers are based outside of the EU/EEA (i.e. the USA), the transfer of personal data to a third country has for a long time been an issue. On 10 July 2023, the adequacy decision EU-U.S. Data Privacy Framework was adopted by the EU Commission. However, all recipients in the USA do not adhere to that regime. Further transfer measures may need to be taken. Also, other measures may have to be taken to ensure a safe transfer of personal data to third countries. Furthermore, it is likely that the adequacy decision will be held invalid by the EU court. As regards the public sector, despite the legislative changes mentioned in question 9.1 above, the public sector must still consider issues relating to information subject to statutory obligations of secrecy.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No; however, it shall be noted that the AI-Act was finally approved on 21 May 2024. The next step is publication in the Official Journal of the EU. The Regulation will enter into force 20 days after its publication and will apply after a certain period thereafter, generally, after 24 months. The Act involves a definition of AI-systems which will likely have a big impact on the legislative landscape in the EU/EEA and Sweden. The Act classifies AI according to different risks, and it also includes definitions of AI systems that are prohibited (e.g. social scoring systems and manipulative AI). There are also certain obligations that fall on providers of high-risk AI systems, and such providers will be subject to additional requirements.

The AI Act will be complemented by provisions in Swedish law, including which authorities will be competent within the meaning of the Act.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

The legal implications of training such systems depend on the type of data being used. If the data involves trade secrets of businesses, personal data or other sensitive information, specific legislation must be taken into consideration. There is no Swedish legislation preventing contractual arrangements of the ownership and right to "training data". However, personal data can never be owned by anybody other than the data subject her/himself; agreements regarding other sensitive information will be limited by the applicable law or other agreements taking precedence.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

The Swedish legislation regarding intellectual property is written with the assumption that property is created by a physical person, meaning that what applies when it comes to development without human interaction is still unclear.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There are no specific Swedish laws or regulations that regulate procurement of such solutions. The EU Commission has launched a so-called regulatory sandbox for blockchain, offering businesses the chance to try their products and services in a safe and confidential environment.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain-based technologies are most common in financial services relating to cryptocurrencies.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

The lack of regulation makes it hard to regain potential losses if valuable data is stolen from a storage using a blockchain-based solution. There is also uncertainty of the security-aspects of blockchain-based technology, since the technology is based on transparency. Therefore, some businesses should be careful before opting for such technology, for example when it comes to operators handling record-keeping or personal data on a large scale.

The relationship with personal data processing overall is also a big issue. It can be hard to determine the ownership of the data and subsequently the data controller, making it difficult to hold businesses accountable for any wrongdoing. The GDPR contains important principles such as the right for data subjects to have their personal data erased or to be forgotten once there is no legitimate purpose to process the data any longer. Data controllers should also ensure that personal data is up to date and accurate, as well as not processing more data than necessary for a specific purpose. The above-mentioned principles can be hard to combine with blockchain since such technology is considered eternal.

Anna Fernqvist Svensson is a member of the Swedish Bar Association. She specialises in IT/IP and data protection law. She is head of the Hellström Data Protection and Employment law practice group. She has more than 20 years of experience of national and international assignments. Anna Fernqvist Svensson has experience of dealing with complex legal matters within the current fields of law and has experience of working as an advisor to both larger and smaller companies and organisations. She represents clients within both the private and the public sector and both national and international clients. She is ranked in *The Legal 500* and is a *Recommended Lawyer* and *Leading Individual*.
Assignments include, *inter alia*, legal advice concerning IT contracts, procurement of IT services and systems, and legal investigations and negotiations.
Her related data protection assignments include acting as DPO and assisting DPOs in their daily work, assisting clients in performing data protection impact assessments and assessments on third country transfers, advice on personal data breaches, review and drafting of agreements and other documentation, assessments of whether companies/organisations fulfil the legal requirements of processing of personal data according to the EU and national data protection rules, drafting and reviewing policies regarding integrity and the protection of personal data, data processing agreements, transferring of personal data to third countries, i.e. countries outside of the EU/EEA, protection of personal data when marketing products and services and so-called whistleblowing schemes.

Hellström Law
Kungsgatan 33
Stockholm
Sweden

Tel: +46 709 55 09 15
Email: anna.fernqvist@hellstromlaw.com
LinkedIn: www.linkedin.com/in/anna-fernqvist-svensson-86ba3945

Arvid Rosenlöf is an associate at Hellström Law. He is a member of the Data Protection and Employment law practice group. He specialises in employment and data protection law.
Assignments include assisting clients with employment law matters such as drafting employment contracts, negotiating with trade unions, and terminations due to redundancy or other reasons. As regards data protection, Arvid Rosenlöf assists clients with the drafting of data protection impact assessments and assessments on third country transfers, reviewing and drafting agreements and other documentation within the data protection field. Arvid also has experience with assessments of whether companies/organisations fulfil the legal requirements of the processing of personal data according to the EU and national data protection rules, drafting and reviewing policies regarding integrity and the protection of personal data, data processing agreements, transferring of personal data to third countries, i.e. countries outside of the EU/EEA and so-called whistleblowing schemes.
Arvid Rosenlöf has also held seminars on subjects within his specialist areas of law.

Hellström Law
Kungsgatan 33
Stockholm
Sweden

Tel: +46 700 00 21 82
Email: arvid.rosenlof@hellstromlaw.com
LinkedIn: www.linkedin.com/in/arvid-rosenlöf-543a70147

Switzerland

Arioli Law

Martina Arioli

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, Swiss law does not specifically regulate the procurement of technology products and services in the private sector. Of course, mandatory statutory provisions must be adhered to that govern certain aspects of technology sourcing transactions, such as employment law, data protection law and merger law.

A number of industries are subject to strict secrecy obligations:

- Banking institutions are subject not only to Swiss banking secrecy (Article 47 of the Federal Banking Act) but also to multiple regulatory requirements, including circulars issued by the supervisory authority (the Swiss Financial Market Supervisory Authority (FINMA)) when procuring technology solutions. Similarly, insurance companies are subject to statutory regulations and, in particular for outsourcing of significant functions or partial outsourcing of control functions to third parties, to the FINMA Outsourcing Circular.
- In the telecoms sector, providers are subject to telecoms regulations (the Federal Telecommunications Act), which contain secrecy obligations.
- The healthcare sector is subject to extended secrecy obligations that render additional safeguards in technology sourcing contracts necessary. When deploying medical devices, healthcare institutions are obliged to implement stringent security measures.
- Article 321 of the Swiss Criminal Code obliges certain professionals such as medical staff, attorneys, notaries, auditors, members of the clergy, and their aides to professional secrecy. Any disclosure of confidential information that has been confided to them in their professional capacity or which has come to their knowledge in the practice of their profession is deemed a violation of the criminally sanctioned professional secrecy. IT providers are typically deemed aides (auxiliaries) to the aforementioned professions. Accordingly, they are subject to the same secrecy obligations. It is advisable to explicitly emphasise this in a technology sourcing contract.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes, the procurement of technology products and services by government or public sector bodies are indeed regulated. The processes set out in Federal and Cantonal public procurement laws need to be complied with. Depending on the value of the project (threshold), a competitive tender process is mandatory: open procedure; selective procedure; or invitation procedure. A direct award is only permitted in exceptional circumstances. Public procurement law applies not only to governmental bodies but also to private companies in the context of the provision of public services.

On a Federal level, the public procurement process is governed by the revised Federal Act on Public Procurement (PPA) of 21 June 2019. The Cantons unanimously adopted the revised Inter-Cantonal Agreement on Public Procurement (*Interkantonale Vereinbarung über das öffentliche Beschaffungswesen* – IVöB) on 15 November 2019 with the aim of harmonising the procurement principles at Federal and Cantonal level. The 2019 revisions implemented the paradigm shift from favouring the most economic tender to the best tender in terms of quality.

The basic features of the regulatory regime are transparency, objectivity and impartiality, and the prevention of conflicts of interest, corruption and negative impacts on competition. Further, all tenderers are to be treated equally at all stages of the procedure and safeguard the confidentiality of the process at all times. In addition, tenderers must comply with minimum requirements regarding the health and safety of their workforce, equal pay, compliance with employment laws and protection of the environment, and cybersecurity obligations based upon the Information Security Act of 1 January 2024.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, there are no mandatory minimum or maximum terms for a contract for the supply of technology-related solutions and services; the parties are free to determine the duration.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, there are no mandatory notice periods for technology sourcing contracts. However, when negotiating a notice period,

the customer should take into account the time it takes to move to an alternate provider in order to ensure a smooth transition and migration.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes, Article 2 of the Swiss Civil Code contains the general principle that all must act in good faith in the exercise of their rights and in the performance of their obligations. The manifest abuse of a right is not protected by law. This overarching principle of good faith is not only enshrined in law but is of utmost importance in Swiss daily business.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Technology-related solutions and services agreements may contain elements of the statutory provisions relating to contracts for work, services, sales, and to corporations. Consequently, the applicable statutory provisions and corresponding remedies are highly dependent on what contractual obligations of the sourcing agreement have been breached. Given that the statutory provisions are not mandatory, the parties are free to determine remedies in the sourcing agreement, such as:

- remediation of defects within determined time limits, including, e.g., the replacement of hardware;
- monetary compensation for damages, including liquidated damages/penalties;
- reduction of fees;
- step-in rights; and
- termination or rescission of the agreement.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Additional protection measures may include:

- specific warranties;
- regular charge or a service provision review mechanism;
- contract change management; and
- audit and benchmarking.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Given that Swiss law does not provide for specific termination provisions applicable to technology sourcing agreements, the parties typically agree on termination for cause and termination for convenience, including the respective notice periods. In particular, as regards termination for material breach, it is recommended that scenarios that constitute such material breach are specifically agreed on and respective contractual obligations are spelt out. If a party adheres to the contractually stipulated termination provisions, claims for damages from the terminated party should not arise. However, this does not necessarily preclude dire discussions on whether a breach may be deemed material or not.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties are free to exclude or agree upon additional termination rights such as insolvency events, change of control and multiple/persistent minor breaches.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Pursuant to Swiss law, the parties cannot exclude or limit liability for damages caused by intent or gross negligence. Further, it is not possible to exclude or limit liability for death or personal injury resulting from a negligent breach of contract.

Typically, the provider aims to extensively exclude liability for indirect and consequential loss or damages, for loss of business, profit or revenue. By contrast, the customer typically aims to have such damages contractually deemed as direct damages.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, the parties may agree on a financial limit on liability and indemnities, subject to the limitations set out in question 2.8. The cap can be a fixed amount or a percentage of the contract value.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, these principles apply to all of the aforementioned types of technology procurement contracts. Regarding (d) – the contracts for the procurement of AI-based or machine learning solutions – Switzerland to date does not have a specific Act regulating AI. Regarding (e), Switzerland takes a rather liberal approach to blockchain-based solutions.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

There are no main methods for dispute resolution used in Switzerland and there are no statutory rules on contract management, governance and escalation in Swiss contract law. Thus, it is recommended that detailed provisions are included in the agreement governing a dispute resolution process before a party can resort to a court or arbitration. Any dispute resolution process should ideally be limited to a resolution time-period to ensure expedited resolution. Typically, the parties agree upon an internal escalation procedure along the lines of the respective company's hierarchy and set timeframes at every level in order to reach a settlement in due time. If the parties fail to reach a settlement despite escalation or in the absence of such contractual escalation, the parties can agree to involve a mediator.

If a party initiates civil proceedings, the first hearing before the judge/court aims at reconciliation. Only in the event that such reconciliation fails does the court proceed to address the legal claim(s) put forward.

It is recommended to include provisions on arbitration and/or ADR.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

Typically, the parties agree on the rights to use pre-existing intellectual property and the allocation of rights in materials developed in the context of the technology sourcing agreement ("work products"). Further, depending on the transaction, the transfer of ownership in intellectual property rights or the assignment of licences may be agreed upon. It is advisable to specifically detail any and all intellectual property rights in the sourcing agreement in order to avoid risky terminations or difficult termination assistance negotiations.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

For the transfer, lease or license of intellectual property rights, the written form is recommended. Further, it is strongly recommended to register transfers of trademarks and patents in the respective registries administered by the Swiss Federal Institute of Intellectual Property as soon as possible.

Third-party intellectual property must be taken into account as the relevant licence agreements may require the consent of such third party.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

The Federal Act Against Unfair Competition and the Swiss Criminal Code provide for penalties for the breach of trade secrets and the exploitation of such secrets.

It is recommended to protect know-how, trade secrets and other business critical confidential information by including extensive confidentiality clauses in the sourcing agreement that provides for penalties to be paid in the event of breach. Note that EU Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure does not apply in Switzerland.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

The Swiss Federal Act on Data Protection Act (FADP) contains provisions pertaining to data processing as well as the transfer of data to countries without an adequate level of data protection similar to the GDPR.

In addition, industry sector-specific regulatory requirements governing data security and data protection matters may apply.

Under the FADP, the following requirements for sourcing transactions apply:

- the parties must conclude a written processing agreement if the provider is to be deemed a processor;
- personal data may only be processed by the supplier in accordance with the purpose defined and within the limits of the processing permitted to the customer itself and pursuant to the instructions of the customer;
- the processing of personal data must not be prohibited by a statutory or contractual duty of confidentiality; and
- the customer shall ensure that the supplier provides for data security in accordance with the requirements of the Ordinance to the FADP by implementing adequate technical and organisational measures, taking into account the purpose, as well as the nature and extent of the processing, an assessment of the possible risks to the data subjects and the current state of the art. The technical and organisational measures shall ensure confidentiality, availability and integrity of data by protecting data from unauthorised or accidental destruction, accidental loss, technical faults, forgery, theft or unlawful use, unauthorised alteration, copying, access or other unauthorised processing.

As the customer remains liable towards the data subject for the compliant handling of personal data by the supplier, there is a tendency not to apply a liability cap for breaches of data protection or other regulatory requirements in sourcing agreements.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside of Switzerland. However, the parties must either: obtain the consent of each data subject individually; or put measures in place to ensure that the data is adequately protected in the relevant jurisdiction, such as sufficient contractual guarantees, or binding corporate rules (BCR), provided the processing takes place within a legal entity or among legal entities under common control and all involved parties are subject to the BCR.

The *Schrems II* decision by the European Court of Justice of July 2020 does not apply in Switzerland; however, it of course has a great impact on the validity of cross-border transfers based upon standard contractual clauses (SCC), given that Switzerland follows the EU regime. For cases of cross-border outsourcing, the Federal Data Protection and Information Commissioner (FDPIC) adopted the SCC issued by the EU Commission in June 2021. In order to cover Swiss law, the FDPIC stipulates some changes to be made to the EU SCC.

Under the revised FADP, the parties no longer need to notify the FDPIC if the cross-border transfer is based upon the SCC or BCR.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Apart from the provisions in the FADP, sector-specific laws and regulations may apply which impose further obligations on higher risk areas, such as financial services, telecommunications, and healthcare. Further, the Swiss Criminal Code contains cybercrime-related provisions.

The Information Security Act (entered into force on 1 January 2024) applies primarily to Federal government. However, it is currently being revised to include obligations for private players that are deemed "critical infrastructure". Other than that, for the private sector, information security is left to the responsibility of self-regulatory regimes and certifications such as the International Organization for Standardization.

Data breaches must be reported to the Federal Data Protection and Information Commissioner (FDPIC) without undue delay. Further, financial institutions must notify FINMA within 24 hours of information security breaches. As of 2025, critical infrastructures will have to notify the Federal Office for Cyber Security (BACS) of information security breaches. For FINMA-supervised institutions, this means that – within a very short period of time – multiple notifications must be submitted to multiple authorities with different processes for the same data breach.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Article 333 of the Swiss Code of Obligations (CO) stipulates that if the employer assigns its business or a business unit to an acquirer in the sense of an outsourcing, the employment relationship of any employee affected automatically transfers to the acquirer, unless the affected employee objects to such transfer. This also applies to mergers, splits or asset transfers in accordance with Article 27 of the Swiss Merger Act.

The previous employer is obliged to inform or consult with the employees' representatives or, if there is no representation, with the employees themselves in good time before the transfer takes place (Article 333a CO).

The employment agreements are automatically transferred to the acquirer on essentially all existing terms and conditions, including benefits granted under the employment agreement or based on a collective bargaining agreement, as well as accrued holiday entitlements. After the transfer, the acquirer can modify the employment terms – see question 7.5.

The former employer and the acquirer are jointly and severally liable for an employee's claims that (i) are due prior to the transfer, or (ii) will become due up to the date the employment relationship can effectively be terminated or until its actual termination based on the employee's objection to the transfer.

6.2 What employee information should the parties provide to each other?

There are no statutory rules on what information must be exchanged by the parties to an outsourcing agreement. Prior to the transfer date, the data on employees disclosed to the acquirer must be limited to a "need-to-know" basis and should be anonymised to the extent possible. Information may include details on employment terms and conditions, function, seniority level, salary and notice period.

Upon transfer, the acquirer must be provided with all necessary information for the performance of the employment agreements in order for the acquirer to fulfil its obligations as the employer.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

As a rule, such termination would contravene Article 333 CO. However, if the respective notice period is observed, the employment agreement may be terminated after or even prior to the transfer.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, after the transfer, the new employer may modify the employment terms of the transferring employee subject to the employee's consent and provided that the modification pertains to non-material aspects only.

The acquirer may also terminate the employment agreements and offer new agreements on changed terms of employment (constructive dismissal). The new terms can enter into force only once the contractual notice periods have expired.

6.5 Are there any pensions considerations?

When employees are transferred under Article 333 CO, the employees' vested benefits under the former employer's pension scheme are transferred to the acquirer's pension scheme. After the transfer, the employees' pension benefits are calculated according to the new scheme's regulations.

If the workforce that forms part of the former employer's pension scheme reduces substantially, the respective pension scheme must be partially liquidated. The employees then have individual or collective claims to a portion of the non-committed funds (free reserves) in addition to their ordinary claims to the vested benefit.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

If the outsourcing agreement entails the transfer of business offshore, the parties need to assess whether the employment contracts of the affected employees actually transfer by operation of law given that Article 333 CO only applies if the business concerned preserves its identity post-transfer.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

The FINMA Outsourcing Circular 2018/03 contains regulatory requirements for outsourcing by banks, securities dealers as well as insurance companies organised under Swiss law, including Swiss branches of foreign banks, and securities dealers and insurers that are subject to FINMA supervision. It sets out provisions on the selection, instruction and control of suppliers, including a comprehensive audit right, as well as provisions to secure availability of data.

Article 47 of the Federal Banking Act protects customer-related data from disclosure to third parties and applies to all banking institutions in Switzerland (banking secrecy). An

outsourcing agreement with a customer subject to banking secrecy must therefore contain the supplier's obligation to comply with the banking secrecy rules. Further, any disclosure of non-encrypted data to a supplier is only permitted with the express consent of each banking customer; such consent may be obtained based upon the bank's general terms of business applicable to the individual customer contract.

Specific notification requirements must be considered in connection with outsourcings by other players in the Swiss financial market. In particular, insurance companies must notify FINMA of any outsourcing of essential functions deemed a change of business plan. The notification procedure can ultimately be deemed an approval process given that FINMA may open investigations within four weeks after notification has been submitted.

Financial market infrastructures such as stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories or payment systems are subject to the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading and must obtain prior approval from FINMA if it wishes to outsource essential services such as risk management.

Furthermore, asset managers, trustees, managers of collective assets, fund management companies and securities firms must comply with the Financial Institutions Act and, similarly, client advisers and providers of financial instruments must comply with the Financial Services Act when outsourcing tasks to third parties.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Generally, the outsourcing relationship is based on a master services agreement between two independent companies. For global outsourcing transactions involving multiple group entities, the contractual structure is more complex: in a centralised contractual set-up, the customer procures the provider's services on behalf of its group affiliates, whereas in a decentralised contractual set-up, the customer affiliates procure services from the provider directly as contractual parties.

Further, the customer and provider may choose to set up a joint venture or enter into a contractual joint venture or partnership agreement. The customer may also establish an (offshore) captive entity.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

The definition of service levels and service credits depends entirely on the technology outsourcing transaction.

In the Statement of Work, the parties define the services to be provided and the service levels, as well as the service criteria by which performance can be measured (key performance indicators). This entails detailed reporting and monitoring. In the event that the provider does not achieve the agreed-upon service levels, a (typically relatively small) amount is deducted from the service fees payable to the provider as a service credit. Service credits for a specific time period are usually capped at an at-risk amount in the range of 5% and 15% of the fees due in that particular time period.

The service credits shall incentivise the provider to consistently achieve the agreed service levels and to facilitate a partial compensation of the customer for poor service without the need to pursue a claim for damages or terminate the agreement.

Service credits are typically the sole remedy of the customer for the particular failure concerned, however, without prejudice to the customer's more extensive rights in relation to more serious contract breaches or persistent performance failures; *cf.* questions 2.4 and 2.7.

Of course, there are alternatives such as bonus/malus schemes or crediting an amount to a certain account dedicated to implementing, e.g., continuous improvements or innovations; this serves to further incentivise suppliers given that the service credit may be perceived as a penalty rather than an incentivisation.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods include cost plus (actual costs incurred by the provider plus a pre-agreed profit margin), fixed pricing for regular and predictable volume and scope of services, or consumption/transaction-based charging.

The outsourcing agreement should provide for a mechanism for cost control and adequate adjustment of charges, including:

- charge variation mechanisms;
- change management procedures;
- service level credits or bonus/malus;
- measures to share cost savings between the parties and provide an incentive to the provider to achieve these;
- auditing;
- benchmarking;
- disputed charges; and
- a pre-agreed inflation adjuster.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

For the transfer of third-party contracts, the customer shall first assess whether such transfer is permitted under the third-party contract. If the transfer is contractually excluded, the parties shall assess whether the contract can be at least managed by the provider on behalf of the customer or whether the contract should be terminated. If the transfer requires the consent of the third party, such consent shall be obtained in writing. If the transfer is not excluded or not made subject to consent, it suffices to inform such third parties of the transfer to the provider in writing to effect the transfer.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The transfer of assets within an outsourcing agreement may trigger corporate income taxes, real estate transfer tax, Federal securities transfer tax, and value-added tax (VAT). Pursuant to Swiss law, every transfer of assets to the provider constitutes a supply of goods or services and is, in principle, subject to VAT. If transferred assets are part of a transferred business entity, VAT must be notified. Intragroup outsourcing may result in a VAT leakage, which can be neutralised by group taxation.

Intragroup outsourcing must be at arm's length and in line with general transfer pricing principles.

For multijurisdictional outsourcings, it is recommended to consider holistic tax planning in order to avoid double taxation, reduce source income taxes and, for intragroup outsourcings, identify tax-optimising measures.

The termination of contracts without adequate compensation and/or a notice period may give rise to taxation of a constructive dividend/profit shift. According to prevailing doctrine, the mere shift of functions should not be taxed.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

For licensing on-premise, the customer requires a sophisticated IT department and/or secures the support from the licensor or its agents for the purposes of smooth roll-out of software updates. Otherwise, the same principles apply as to cloud computing.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

The customer should ensure the implementation of stringent security measures for the provider's access to its infrastructure, limit the access granted to the provider's personnel, conclude a confidentiality agreement and, if applicable, the requisite data protection agreements (e.g., DPA/SCC) with the provider and, potentially, the individual support staff members, and limit the access to personal data as far as possible.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Escrow agreements are used in Switzerland and they are enforceable; however, it would be an exaggeration to call this common practice. Many customers choose not to conclude an escrow agreement despite the risks of a lock-in to their provider as they deem it unfeasible to make use of the source code themselves or by third parties once released from escrow.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No. Governmental bodies on Federal and Cantonal level have moved to the cloud, including to services of hyper scalers abroad. This has sparked controversy and raised criticism that secrecy and data protection matters are not fully considered.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

In spite of the heated debate around issues such as data protection, secrecy, trade secrets, in reality, cloud computing solutions are widely used in Switzerland, not only by private citizens, private companies and government on all levels. The majority of outsourcing and resourcing projects entail at least a partial "move to the cloud".

9.3 What are the key legal issues to consider when procuring cloud computing services?

The key issues are, in particular:

- assurances of the provider as regards business continuity and disaster recovery;
- information security and data security;
- data portability/contractual migration obligations in order to avoid lock-in in the event of termination/expiry of the contract, also including the support of the cloud provider and its assurance to work with a new supplier, if necessary; and
- guarantees by the cloud provider regarding professional secrecy.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No. Irrespective of the fact that Switzerland considers itself to be a hub in the development of AI solutions by research institutions and private companies and private/public partnerships, Switzerland has not adopted any specific laws and regulations on AI to date. Interestingly, FINMA noted already in its Circular 2013/8 that "supervised institutions must document the key features of their algorithmic trading strategies in a way that third parties can understand". Furthermore, there are guidelines on the responsible use of AI within the public sector.

Given that Switzerland is not a member of the EU/EEA, the EU Artificial Intelligence Act will not take effect in Switzerland. Nevertheless, this EU Act will, once enacted, have an impact on Swiss businesses active in the field, similarly to the GDPR or the EU Medical Device Regulation (MDR). Potentially, Switzerland will adopt its own legal framework on the procurement and use of AI at some point in time. However, the recent rapid developments in AI have prompted prominent voices in Switzerland to call for regulation efforts and not to wait, in particular in view of the fact that Switzerland has the worldwide highest number of AI-related patents in relation to its population and big tech companies have relocated their research labs to Switzerland.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

There are no statutes or regulations that govern the training data of AI in Switzerland. Ownership of data has occasionally been the topic of academic debate in recent years; however, neither scholars nor the legislator have embraced the notion of data ownership. For the lack of a better term, however, technology sourcing contracts often deploy the term "data ownership" in order to allocate responsibility and a so-called "economic power of disposal" ("*wirtschaftliche Verfügungsmacht*"). In order to address access and use of data beyond data protection compliance, technology sourcing contracts contain provisions that can be deemed license-like granting of rights and obligations. The terms of use of today widely used AI applications can potentially not be upheld in this regard.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Pursuant to Swiss law, software is typically protected by copyright law; in very exceptional cases, patent protection can be obtained. However, under the Swiss Copyright Act, as well as under the Swiss Patent Act, only a human creation/invention can obtain legal protection. Accordingly, there must be a "human in the loop", be it the owner, the original developer or the user of the AI.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there are no Swiss laws or regulations that specifically regulate the procurement of blockchain-based solutions.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain has been adopted particularly in the context of disruptive fintech solutions, and for some time, Switzerland has become a hub for blockchain start-ups. This has led Switzerland to enact the new Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act), which entered into force on 1 August 2021. The DLT Act contains various improvements to the Swiss legal framework in connection with the use of decentralised technologies and blockchain, including, in particular the introduction of ledger-based securities that enable the digitisation of shares and other rights.

One of the key changes is a licence for DLT trading facilities, i.e., financial market infrastructures for DLT securities that can admit other companies and persons to trading in addition to financial intermediaries. Legal certainty will be increased in insolvency law by explicitly regulating the segregation of crypto-based assets in the event of bankruptcy.

The legislation improves the conditions for blockchain and DLT companies in Switzerland, thereby making the country an international pioneer in modern regulation of innovative financial market technologies.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Blockchain technology is decentralised, immutable, and transparent. Consequently, blockchain applications may pose a challenge as regards compliance with data protection law. The decentralisation means that there is no one responsible for compliance, i.e., there is no controller in the sense of data protection laws. This applies, in particular to public (permissionless) blockchain. Further, the immutability of data on the blockchain may be in conflict with the data protection principle of data accuracy.

In order to ensure compliance, companies tend to deploy private (permission-only) blockchains for internal applications only in order to be able to select the participants, manage the transaction content, and delete data in the event that it is rendered inaccurate. Alternatively, applications are deployed with which transaction-related personal data is stored outside the blockchain application itself (off-chain). Only the cryptographic hash values, including the timestamp, remain on the blockchain itself. Further, the transaction-related personal data can be encrypted on the blockchain itself and the private key is only available to a limited group of authorised individuals.

Martina Arioli has been listed by *Chambers Europe* for TMT since 2019 and recognised as one of Switzerland's leading business lawyers since 2016 by Who's Who Legal. She has been selected as Thought Leader Data in Switzerland since 2019 and won the Client Choice Award Data Switzerland 2020.

Martina Arioli is an experienced legal counsel, with more than 20 years of international practice, specialised in IT law and outsourcing. She has supported outsourcing engagements in all stages, from contract drafting, negotiating global and local agreements to implementation and transition, conflict mediation, termination and resourcing to new suppliers. Martina combines in-depth knowledge on complex contractual matters in outsourcing and information technology projects with the experience of implementing such global projects as in-house lawyer.

Arioli Law
Hornbachstrasse 22
8008 Zurich
Switzerland

Tel: +41 44 201 66 11
Email: martina.arioli@arioli-law.ch
LinkedIn: www.linkedin.com/in/martina-arioli-ab809b1

Arioli Law is a leading boutique law firm established in 2013 in the heart of Zurich. It was one of the first one-woman, pure technology law firms in Switzerland. Our attorneys are committed to providing excellent services to our clients in a wide range of industries and the public sector. We believe that hands-on work by highly specialised and experienced partners leads to better and faster results at lower costs to our clients. The renowned Swiss business magazine BILANZ has ranked Arioli Law amongst the Switzerland's top law firms in TMT and IP law since the first ranking issued in 2017. Our attorneys have garnered rankings and awards including *Chambers*, *The Legal 500*, *Leaders League* and *Who's Who Legal*.

www.arioli-law.ch

MARTINA ARIOLI
LAW FIRM

Taiwan


Tsung-Yuan Shen


Rachel Chen


Josh Tsai

Lee and Li, Attorneys-at-Law

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, the private sector procurement of technology products and services in Taiwan is not regulated, allowing for freedom of contract.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes, procurement of technology products and services by government or public sector bodies is governed by the Government Procurement Act. This act establishes a system that ensures fair and open procurement procedures, promotes efficiency and effectiveness in government procurement operations, and guarantees the quality of procurement. In principle, government procurement is conducted through tendering procedures, which include the publication of tender notices and/or qualification review notices.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

The parties involved can generally freely determine the terms of their transactions when no government or public sector entity is involved. However, if it involves government agencies in our country commissioning companies to undertake information services and adopting comprehensive outsourcing services, there is a maximum limit of ten years for the duration and contract period of the comprehensive outsourcing adopted by the agencies.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, the Taiwan laws do not regulate such notice period. If there is no contractual agreement regarding termination, in principle, any party can terminate the contract at any time according to the Taiwan Civil Code. However, if one party terminates the contract in a way that harms the other party, the terminating party will be liable for damages.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

The Taiwan Civil Code mandates that rights granted by contract or law must be exercised with honesty and good faith, and intentional or gross negligence cannot be waived in advance. These requirements are particularly stringent in the case of a standardised contracts. Any clause that seeks to release or diminish the liability of one party, increase the liability of the other party, or restrict the other party's rights would be considered invalid (please refer to question 2.9 for more information).

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

In Taiwan, the primary recourse for a customer in the event of a breach of contract by the supplier under general law is to seek damages, usually in the form of monetary compensation to cover the customer's losses and lost profits, as provided under the Taiwan Civil Code. Additionally, the Taiwan Civil Code allows the parties to agree on punitive damages.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In a contract for the provision of technology-related solutions or services, additional remedies or protections for a customer may

include provisions for price reduction or liquidated damages in the event of non-conformance during acceptance testing. The contract may also include provisions allowing the customer to request correction of non-conformities within a specified period. If the provider fails to correct them, the customer may be entitled to claim damages and even terminate the contract and request a refund of payments made. Additionally, the contract may specify that the provider must offer free maintenance, training, or technical support for a certain period after the completion of the technology project. Furthermore, the contract may include provisions holding the provider liable for any infringement of third-party intellectual property rights or other rights related to the technology.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Typically, a party can terminate a contract without facing a claim for damages from the other party if the termination is a result of the terminated party failing to fulfil its contractual obligations. The parties can also agree that either party can end the contract without giving a reason and without being held liable. If there is no such agreement, and one party ends the contract in a way that causes harm to the other party, the party ending the contract will be responsible for damages (please see question 2.2 for more information).

2.7 Can the parties exclude or agree additional termination rights?

Yes, parties are generally free to exclude or agree additional termination rights.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

According to the Taiwan Civil Code, except for liability arising from intentional or gross negligence, parties to a contract may limit or exclude their liability through the contract. Additionally, if circumstances change in a way that was not foreseeable at the time of contracting and enforcing the contract would be unfair, the parties may apply to the court to increase or decrease their obligations or change the original effects of the contract. Therefore, in practice, it is common to include "*force majeure* clauses" in contracts, which relieve either party from liability in the event of unforeseeable circumstances beyond their control.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

In principle, the parties are free to agree on a financial cap on their respective liabilities under the contract. However, in the case of standardised contracts, according to the Taiwan Civil Code, the following provisions are considered unfair and therefore invalid: (1) exemption or reduction of the liability of one party under the predetermined contract terms; (2) increase in the liability of the other party; (3) abandonment of rights or restriction of the exercise of rights by the other party; and (4) other provisions that significantly disadvantage the other party. The Consumer Protection Act shares similar regulations. Therefore, in the case of a standardised contract unilaterally drafted by the provider of technical services in a technical service contract, if the liability limitation clause significantly reduces the provider's liability and essentially prevents the customer from exercising their contractual rights, it may be deemed unfair and therefore invalid.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No. There are no specific regulations for different types of technology procurement contracts, so they are all governed by the Taiwan Civil Codes and other general regulations.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Litigation and arbitration are the primary methods of dispute resolution. In Taiwan, an arbitration award holds the same weight as a final court judgment. However, for a foreign arbitration award to be enforced in Taiwan, it must first be applied to the court for recognition. Generally, Taiwan courts are inclined to grant recognition, unless there is "no reciprocity", "violation of Taiwan's public order and good morals", "disputes that cannot be resolved by arbitration under Taiwanese law", or "serious defects in the arbitration agreement or arbitration procedure", in which case recognition will be denied.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The intellectual property rights involved in a technology sourcing transaction mainly include patents, copyrights and trade secrets. The laws governing the protection of these intellectual property rights are outlined as follows:

(1) **Protection of patents**: When a customer appoints a supplier to carry out research and development ("**R&D**") projects, the ownership of the right to apply for a patent and the resulting patent rights are determined by mutual agreement in the contract between the parties. In the absence of such agreement, the rights to apply for patents and the patent rights are vested in the supplier, while the customer is entitled to use and exploit such R&D outcomes.

(2) **Protection of copyrights**: If a supplier is appointed by a customer to complete a copyrightable work, then such supplier will be considered the author and copyright holder unless the customer is specified as the author and/or copyright holder under the underlying agreement between the parties. However, even if the supplier is considered the copyright holder, the customer is still entitled to use the appointed work.

(3) **Protection of trade secrets**: When a customer funds and contracts a supplier for R&D projects and the outcomes thereof contain trade secrets, the ownership of such trade secrets will be determined by the underlying contract

between the parties. If the contract does not specify the ownership, then the trade secrets belong to the supplier, while the customer is entitled to use the trade secrets for its business operations.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

The Taiwan laws do not stipulate the formalities required for the transfer of ownership of intellectual property rights. This means that the transfer of intellectual property rights can be simply made through an oral agreement between the parties involved. However, to avoid potential disputes and misunderstandings, it is advisable to specify the procedures and other terms and conditions of the transfer in a written contract.

Notwithstanding the foregoing, according to the Taiwan Patent Act, while the transfer of right to apply for a patent and the underlying patent rights will become effective between the parties upon mutual agreement, it will not be recognised as effective against third parties unless the transfer is recorded at the Taiwan Intellectual Property Office ("**TIPO**"), Ministry of Economic Affairs ("**MOEA**").

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Yes, trade secrets are primarily protected by the Taiwan Trade Secrets Act ("**TSA**"), which outlines the requirements for trade secrets and the civil and criminal liabilities for trade secret misappropriation. Other business-critical confidential information that does not qualify as trade secrets may still be protected under the Copyright Act and/or Criminal Code.

Under the TSA, trade secrets are defined as information such as methods, techniques, processes, formulas, programmes, designs, or other information used for production, sales, or operations that meets the following criteria:

(1) it is not known to persons generally involved in this type of information;
(2) it has economic value, actual or potential, due to its secretive nature; and
(3) the owner has taken reasonable measures to maintain its secrecy.

Furthermore, Article 3 of the Taiwan National Security Act ("**NSA**") specifically identifies trade secrets related to national core critical technologies. The definition of "trade secrets involving national core key technologies" is determined through consultation with the relevant authorities of the National Science and Technology Council. Misappropriation of trade secrets involving national core key technologies, particularly unauthorised use of such trade secrets in foreign countries, will result in more severe criminal liabilities.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes, the collection, processing and use of personal data are governed primarily by the Taiwan Personal Data Protection Act ("**PDPA**").

(1) **Collection, processing and use of non-sensitive personal data:** The PDPA defines "personal data" as any information or data that can be used to identify a natural person, either directly or indirectly. Under the PDPA, non-government agencies are required to inform individuals of the purpose, type, duration of use, geographical area, recipient, and method of data collection when collecting personal data. Furthermore, they must obtain the individuals' consent to use the data for the specified purpose.
(2) **Collection, processing and use of non-sensitive personal data:** In accordance with the PDPA, the collection, processing, or use of sensitive personal data is generally prohibited, unless specific conditions are met. These conditions include, but are not limited to, when it is required by law, necessary for a government or non-government agency to fulfil legal obligations or used for statistical or academic research with appropriate security measures. Sensitive personal data includes any information related to medical records, medical treatment, genetic information, sexual life, health examinations, criminal records, and similar categories.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Under the PDPA, cross-border data transfers are generally allowed unless restricted by the Taiwan central competent authorities. These restrictions may be imposed if (1) the transfer would harm material national interests, (2) the transfer would violate international agreements, (3) the country to which the personal data is to be transferred lacks adequate data protection law, or (4) such transfer aims to evade the restrictions imposed by PDPA.

For instance, the National Communications Commission ("**NCC**"), the Ministry of Health and Welfare ("**MOHW**"), and Ministry of Labor ("**MOL**") have issued rulings prohibiting the transfer of personal data to Mainland China due to inadequate personal data protection laws. The NCC's order applies to communications enterprises, while the MOHW and MOL rulings apply to social worker offices.

On 19 February 2024, the MOHW proposed a draft ruling to prohibit drug wholesalers and retailers from transferring personal data to Mainland China unless certain conditions are met. However, as of May 2024, this ruling has not yet taken effect.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The PDPA requires non-government agencies to have security measures in place to protect personal data from theft, alteration, damage, loss or leakage. The Enforcement Rules of the PDPA further provide specific technical and organisational measures that agencies may consider based on the principle of proportionality. These measures include allocating management resources, defining the scope of personal data, establishing risk assessment and breach response mechanisms, implementing internal control procedures, promoting awareness and training, managing facility security, keeping records, and continuously improving data security and maintenance.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

With the exception of cases involving mergers, acquisitions, or group reorganisations, employees will not be transferred automatically by operation of law. As a general rule, employers may only transfer an employee based on the following principles, unless otherwise agreed by the employees:

(1) The transfer should be based on the needs of business operations and should not be motivated by improper purposes.
(2) Wages and other working conditions should not be changed to the detriment of the employee being transferred.
(3) The employee should still be able to satisfactorily perform the required duties in terms of physical ability and skills after the transfer.
(4) The employer should provide necessary assistance if the relocated workplace is too far away for the employee.
(5) The livelihood interests of the employee and their family should be considered.

Additionally, under the Taiwan Labor Standards Act ("**LSA**"), a female worker may apply to be transferred to less strenuous work during her pregnancy. In this case, the employer cannot reject her application or reduce her wage. "Less strenuous work" refers to work that is within the capacity of the person to perform and objectively does not affect the health of the mother and the foetus.

6.2 What employee information should the parties provide to each other?

During the selection of a service provider and commercial negotiation, it is common to provide employee information, such as the birth, educational background, work experience and so on. However, it is important to note that any information that can be used to identify a person is considered "personal data", and the restrictions under the PDPA will apply. Employers should obtain their employees' prior consent before using their personal data.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

The employment relationship exists solely between the employer and the work. In the context of a technology outsourcing transaction, the customer is not considered an employer, and therefore does not have the right to terminate the employment relationship as pursuant to the labour contract.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

If both the service provider and the transferring employee agree on the employment terms, such terms may be aligned with those of the service provider's current workforce.

6.5 Are there any pensions considerations?

In Taiwan, employers are required to enrol their employees in the applicable labour pension scheme. All employees hired after 1 July 1 2005 should be covered by the New Pension Scheme. According to the Taiwan Labor Pension Act, employers should contribute a minimum of 6% of their employees' monthly wages to individual labour pension accounts at the Bureau of Labor Insurance on a monthly basis. Additionally, employees have the option to make voluntary contributions to their own pensions.

Based on the above analysis, the technical service provider, not the customer, is therefore responsible for contributing to the statutory pension for its workers.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Currently, there are no specific regulations in place that govern the transfer of employees in the context of offshore outsourcing. However, it is important to adhere to the principles outlined in our response in question 6.1 when transferring employees.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Yes, there are national laws and regulations that specifically regulate outsourcing transactions, but only if the transactions involve a government or public-sector body. In these cases, the outsourcing transactions shall follow procurement procedures outlined in the Government Procurement Act, which include outsourcing certain tasks to civilian entities (please refer to question 1.2 for more information).

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The common types of legal or contractual structures used for an outsourcing transaction include:

(1) **Purchase Agreement**: This contract involves the customer purchasing specific goods from the supplier.
(2) **Service Agreement**: This is a contract where the customer appoints the supplier to handle certain tasks or provide specific services on their behalf.
(3) **Mixed Agreement**: If the supplier is providing both technical services and goods, the parties involved may enter into a mixed agreement that combines elements of a service agreement and a purchase agreement.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

A common practice for specifying service levels and service credits between a service provider and service receiving company is to include a statement of work as an attachment to the agreement.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

In outsourcing transactions where no government or public-sector body is involved, parties have the freedom to choose their charging methods. However, for government procurement, the charging methods for professional and/or technical services provided in outsourcing transactions shall adhere to the following options:

(1) Payment based on total price or unit price.
(2) Monthly, daily, or hourly payment.
(3) Cost-plus fee, with the administrative contract setting an upper limit on costs and defining procedures for handling costs that exceed the limit. Only direct fees, fees for work, and business taxes may be included in the cost.
(4) A percentage of the construction expenses, determined based on percentage figures prescribed and published by the government, taking into account the type of construction work, service items and degree of difficulty.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

The laws of Taiwan do not regulate the formalities required for transferring third-party contracts to a service provider in an outsourcing transaction. However, it is necessary to obtain the customer's consent for the transfer. Without such consent, the original service provider remains obligated to fulfil the terms of the contract with the customer.

To address the rights and obligations related to the outsourcing transaction, the involved parties may consider establishing a tripartite agreement. If the transfer has not been agreed upon by the customer, it is important to carefully consider the legal implications and potential consequences.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

In the context of outsourcing transactions, a key tax issue that can arise is the taxation of service fees. This is particularly relevant when the services are provided in whole or in part within the country, such as when foreign suppliers send personnel to provide services in Taiwan. Additionally, if the services are provided entirely outside the country but require the participation and assistance of individuals or businesses within Taiwan to complete, the related service fees may constitute income from sources within Taiwan for the foreign supplier, potentially making them subject to corporate income tax in Taiwan.

If the service fees are deemed to be income from sources within Taiwan for the foreign supplier, and the foreign supplier does not have a fixed place of business or a business agent in Taiwan, the withholding agent is required to withhold tax at a rate of 20% on the total amount paid by Taiwanese enterprises to the foreign supplier, unless tax treaty relief applies.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Key considerations for software licensing for on-premise solutions include:

(1) Scope of the licence, including any restrictions on customisation, integration, upgrades, and usage for affiliated entities.
(2) Post-sales support, technical assistance, and maintenance terms, such as service duration, methods, frequency, standards, pricing and updates/upgrades.
(3) Indemnity clauses to protect against third-party infringement claims related to the software.
(4) Warranty responsibilities, including free debugging and fault resolution during the warranty period for software design defects causing business interruptions.
(5) Audit clauses to ensure accurate payment of licence fees, with reasonable audit frequency and locations that do not disrupt the licensee's daily operations.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

In general, software users may consider entering into a separate "Service-Level Agreement" ("**SLA**") with the software provider. This agreement could address key issues such as the supplier's response time, resolution time, and 24-hour availability, as well as specific conditions for after-sales service, technical support, and maintenance services. The SLA may also outline the duration, method, frequency, standards, prices, and subsequent updates and upgrade services.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

In Taiwan, software escrow arrangements are not commonly used, and if they are used, they are likely to be rare. In the most basic definition, a software escrow arrangement is a contract between a software supplier and its customer. If the supplier is declared bankrupt or acquired, the customer can still obtain the original source code of the software from the third-party escrow platform specified in the agreement to maintain the normal operation of the software.

In the event of a software supplier declaring bankruptcy, the intellectual property rights of the software may belong to the bankruptcy estate under the Taiwan Bankruptcy Act, and may need to be distributed according to the corresponding bankruptcy liquidation procedures, which might potentially affect the enforceability of the software escrow agreement.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

With the exception of financial institutions (including domestic banks and their foreign branches, branches of foreign banks in Taiwan, credit unions, bills finance companies, and credit card companies) as well as insurance companies, there are no applicable Taiwan laws regulating the outsourcing or use of cloud services by other non-regulated industries. In other words, companies that do not fall under the classification of financial institutions and insurers mentioned above may procure cloud computing services without obtaining prior approvals from the relevant competent authorities and are not subject to any reporting obligations.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions are being widely adopted in Taiwan, with many businesses and organisations leveraging the benefits of cloud technology.

According to IDC's 2022 research, the public cloud market in Taiwan is projected to soar from US$883 million (approximately NT$26.3 billion) in 2020 to US$2,782 million (about NT$83 billion) in 2025. This growth is expected to be fuelled by a compound annual growth rate of 25.8 per cent over the forecast period, with the IaaS market experiencing the highest growth rate and the SaaS market holding the largest share. Enterprise investment is anticipated to focus on cloud consolidation and multi-cloud deployment in Taiwan to improve efficiency, scalability and cost-effectiveness.

9.3 What are the key legal issues to consider when procuring cloud computing services?

When procuring cloud computing services, key legal issues to consider include compliance with the PDPA, contractual relationships between the user and provider, cross-border data transfers, data security and auditing, and data ownership. Compliance with the PDPA is essential, as the cloud service provider must adhere to restrictions on collecting, processing and using personal data. The contractual agreement should encompass specific provisions outlined in the PDPA and its Enforcement Rules, covering data processing scope, purpose, and duration, as well as measures to prevent data theft or disclosure. Cross-border data transfers may be prohibited by Taiwan central competent authorities if they jeopardise national interests or violate international agreements. Data security and auditing measures, including encryption and independent third-party audits, are required for financial institutions and insurance companies. Additionally, data ownership must be retained by the institutions, and the cloud service provider is strictly prohibited from accessing customer data for any purposes outside the scope of the outsourced operations.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

At present, there are no specific laws or regulations in place governing the use of AI or the procurement of AI-based technologies. While Taiwan had initially planned to enact the Artificial Intelligence Fundamental Act by the end of 2023, the emergence of generative AI has led to a delay, with the earliest adoption now expected by the end of 2024.

Currently, there is no comprehensive legislation specifically regulating AI. However, the Taiwan regulatory authorities have been formulating administrative guidelines to recommend appropriate use of AI within certain industries.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

When training machine learning-based systems using data gathered from publicly available sources, the user does not acquire proprietary rights in the training data. The ownership of training data is subject to intellectual property laws such as the Copyright Act and Patent Act. In Taiwan, developers of generative AI models must obtain consent or a licence from copyright holders before reproducing original works, except for fair use as outlined in the Taiwan Copyright Act. If personal data is collected in relation to training data, the PDPA applies, requiring the data collector to obtain necessary "informed consent" unless an exemption applies. However, there have been no cases where the illegal use of AI has led to prosecution for violation of the Copyright Act.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

According to a 2023 Administrative Rule issued by TIPO, copyright protection for content generated by generative AI models depends on the presence of "human expression". If the AI-generated content is produced solely by an AI model without any human input, it will not be protected by copyright. The copyright still belongs to the holders of the original works used for training the AI models. Additionally, a 2022 judgment by the Supreme Administrative Court states that generative AI content does not qualify for patent protection, as the Patent Act requires the inventor to be a natural person. Since AI is not considered a "person" under Taiwan laws, it cannot be recognised as an inventor or creator and cannot apply for a patent for the content it generates. Commercial use of the generated content may also require consent or a licence from the copyright holders, except for fair use as outlined in the Taiwan Copyright Act.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

Currently, there are no specific national laws regulating the procurement of blockchain-based solutions. The Taiwan Financial Supervisory Commission considers the sale of cryptocurrencies as the sale of a digital "virtual commodity" rather than "currency", in compliance with Taiwan's regulatory principles. However, virtual currencies with investment and transferability characteristics will be classified as "securities" and subject to regulation under the Taiwan Securities and Exchange Act ("**SEA**"). The regulation of security token sales is differentiated based on a threshold of NT$30 million, with sales below this threshold potentially exempt from filing obligations under the SEA, while sales above this threshold must first be tested in the "financial regulatory sandbox" before being conducted under the SEA.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain technology, known for its decentralised, transparent and immutable features, has found applications in various industries including agriculture, digital creation, smart cities, Internet of Things, and evidence preservation. Its most common applications include cryptocurrencies, NFTs and related activities. Presently, blockchain technology is being extensively utilised in retail, insurance, medical, and music and creative industries in Taiwan.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Key legal issues to consider when procuring blockchain-based technology in Taiwan include compliance with anti-money laundering regulations and reporting obligations for virtual asset service providers ("**VASPs**"), operating guidelines for VASPs issued by the Financial Supervisory Commission ("**FSC**"), compliance with the PDPA regarding cross-border transmission of personal data and the right to be forgotten, and the validity of electronic signatures using blockchain-based technology under the Taiwan Electronic Signatures Act. VASPs must establish internal controls to prevent money laundering and comply with customer identification and reporting requirements. The FSC's guidelines cover various aspects of VASP operations, including issuance of virtual assets, custody and segregation of assets and information security. Compliance with the PDPA is crucial for the cross-border transmission of personal data and the right to be forgotten. Additionally, the validity of electronic signatures using blockchain-based technology must meet the requirements specified by the Taiwan Administration for Digital Industries.

Tsung-Yuan Shen specialises in the fields of intellectual property protection, unfair competition, and dispute resolution. His professional background spans biotechnology, law, and economics.
Mr. Shen has represented high-tech companies in the fields of electronics, optoelectronics, communications, precision industry, and multinational construction companies on matters of IPR, high-tech laws and public construction disputes.
Clients served by Mr. Shen include Pfizer, Merck Sharp & Dohme, DuPont, TSMC, AU Optronics, Qualcomm, Molex, Lockheed Martin, and other leading companies or organisations.
In addition, Mr. Shen has also utilised his background in economics in cases involving the management or licensing of IP portfolios.

Lee and Li, Attorneys-at-Law
8F, No.555, Sec. 4
Zhongxiao E. Rd.
Taipei 11072
Taiwan, R.O.C.

Tel: +886 2 2763 8000 ext. 2539
Email: tsungyuanshen@leeandli.com
LinkedIn: www.linkedin.com/in/tsung-yuan-shen-沈宗原-02401019

Rachel Chen is a senior attorney in Lee and Li's Hsinchu Office. With a background in both finance and law, her practice areas include corporate investment, corporate governance and compliance, securities law and labour law, with a special focus on M&A, as well as commercial contracts review and drafting.

Lee and Li, Attorneys-at-Law
5F, Science Park Life Hub
No.1, Industry E. 2nd Rd.
Hsinchu Science Park
Hsinchu 30075
Taiwan, R.O.C.

Tel: +886 3 579 9911 ext. 3206
Email: rachelchen@leeandli.com
LinkedIn: www.linkedin.com/in/rachel-chen-93018726a

Josh Tsai's main practice areas encompass corporate investment, mergers and acquisitions, labour dispute resolution, commercial contract drafting and review, and corporate governance. He has participated in several mergers and acquisitions, joint ventures, start-up fundraising, and technical cooperation, transfer, and licensing cases.
Before joining Lee and Li, Mr. Tsai served as legal counsel at listed financial institutions and high-tech companies. During such period, he was involved in capital market fundraising, cross-border mergers and acquisitions, joint ventures, and other related matters. He has a strong background in reviewing, modifying and negotiating contracts within the high-tech industry.

Lee and Li, Attorneys-at-Law
5F, Science Park Life Hub
No.1, Industry E. 2nd Rd.
Hsinchu Science Park
Hsinchu 30075
Taiwan, R.O.C.

Tel: +886 3 579 9911 ext. 3273
Email: joshtsai@leeandli.com
LinkedIn: www.linkedin.com/in/tsai-chen-chuan-a65435143

Lee and Li, founded more than 50 years ago, is the largest law firm in Taiwan, providing services in the Greater China area by collaborating with law firms and intellectual property agencies in mainland China. Besides its main office in Taipei and offices across Taiwan in Hsinchu, Taichung, and southern Taiwan, Lee and Li has formed strategic alliances in Shanghai and Beijing.
Our services are performed by around 870 legal and support staff, including more than 200 Taiwan-qualified lawyers, 50 foreign lawyers, 100-plus Taiwan patent agents or patent attorneys, more than 100 technology experts, and specialists in other fields such as certified public accountants, as well as the PRC lawyers and patent attorneys of our strategic alliances. The firm's 29 practice groups and special task forces are highly experienced in identifying potential and resolving existing legal issues that its clients may encounter in their business operations.

www.leeandli.com/en

理律法律事務所 LEE AND LI ATTORNEYS-AT-LAW SINCE 1965

Türkiye/Turkey


Bora Yazıcıoğlu


Kübra İslamoğlu Bayer


Simge Yüce


Barış Aslan

Yazıcıoğlu Legal

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No specific rules govern the procurement of technology products and services in the private sector. Thus, the general rules enshrined in the Turkish Code of Obligations (**TCO**) apply. Additionally, laws such as the Turkish Code of Commerce (**TCC**), the Law on Protection of Competition, and other relevant laws come into play when applicable. Furthermore, sector-specific regulations, including those in telecommunications, banking, electronic money and payment systems, e-commerce, and healthcare, must also be observed.

One of the key principles accepted by the TCO is freedom of contract. This empowers private sector parties to decide on nearly every provision that governs their relationship, as long as both parties are private, or the relationship is deemed private as per the TCO.

While the Law on Protection of Consumers could potentially apply to the procurement of technology-related products and services, we have excluded it from consideration, presuming that the context of this chapter primarily involves legal entities.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Procuring technology products and services by government or public sector bodies is regulated by a complex legal framework, primarily consisting of the Public Procurement Law (**PPL**) and the Public Procurement Contracts Law, among others. These laws establish the foundational principles and procedures for tender processes conducted by public institutions.

The Public Procurement Authority oversees compliance with these laws, issues guidance, and monitors transparency and fairness in procurement processes.

The basic features of the applicable regulatory regime are as follows:

- **Procurement Methods:** The PPL outlines procurement methods based on specific service requirements, technical needs, and fees. These methods include open tender, tender among specific bidders, negotiated tender, direct procurement, and design competitions.
- **Electronic Tendering:** Electronic bid submissions are facilitated through the Electronic Public Procurement Platform, which has expanded notably during the COVID-19 pandemic, reducing physical contact and streamlining the procurement process.
- **Performance of Contract:** Contracts for procuring goods and services are executed using standard contracts published in the Official Gazette. These contracts include standard provisions, including the scope of the procurement, nature and definition of the goods and services, pricing, taxes, delivery conditions, technical specifications, as well as penalty and termination clauses.
- **Objective Criteria:** The PPL sets objective criteria (e.g., technical specifications, quality standards, price competitiveness) for selecting suppliers to ensure that they are treated equally and without discrimination.
- **Transparency and Competition:** The regulatory framework promotes transparency, competition, reliability, confidentiality, and efficient use of resources to ensure fair and accountable procurement practices.
- **Ethical Standards:** The PPL prohibits corruption and favouritism in procurement activities, with penalties for ethical breaches.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, typically, national law does not specify a minimum or maximum contract term for supplying technology-related solutions and services. Contract terms are usually negotiated between parties, unless other laws apply.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No specific regulation mandates a notice period for terminating such contracts, but parties can determine a reasonable notice period with good faith principles. Specific regulations or industry practices may also influence the notice period. Similarly, certain regulations may impose requirements for specific contracts.

According to the TCO, the parties may also terminate the contract without a notice period if (i) granting time to the debtor would be ineffective, (ii) the obligation becomes useless due to the debtor's fault, or (iii) it is understood from the contract that the

performance of the obligation will no longer be accepted due to non-performance at a specified time or within a specified period.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes, the Turkish Civil Code (**TCiC**) explicitly states that everyone must act in good faith when exercising their rights and performing their obligations. However, there is no established test for fairness or reasonableness, as courts assess the good faith and honesty principle on a case-by-case basis.

This principle extends not only to the performance of contractual obligations but also to pre-contractual negotiations and the termination of contracts.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The customer has several remedies available under the general law, specifically per the TCO. The customer may demand one or more of the following:

- Compensation for damages.
- Performance of the contract.
- Compensation instead of performance.
- Rescission of the contract.
- Termination of the contract.

The nature of the contract should be considered, as the TCO outlines specific conditions for certain contract types.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Contracts typically include the following remedies and protections for customers:

- Service level agreements (**SLAs**).
- Warranty clauses.
- Indemnifications.
- Data protection and privacy clauses.
- Intellectual property (**IP**) rights protection clauses.
- Audit rights.
- Penalty clauses.
- Dispute resolution mechanisms.
- Termination clauses.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

A party can terminate the contract without raising damage claims under specific circumstances defined within the contract or governed by the TCO. Primary methods include:

- Mutual agreement.
- Fulfilment of contract terms.
- Termination clauses.
- *Force majeure*.
- Impossibility of performance.
- Special termination conditions are regulated under specific legislation.

2.7 Can the parties exclude or agree additional termination rights?

Yes, parties can agree to include or exclude specific termination rights, as long as these do not contravene mandatory legal provisions.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Under the TCO, parties can limit liabilities for slight negligence through a prior agreement but cannot limit or exclude liabilities for gross negligence or wilful misconduct. Liabilities for their assistants' actions can also be limited or excluded. However, if the service requires special knowledge, profession, or licence, the supplier cannot limit or exclude its liability, even for slight negligence or their assistants' actions.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, parties can set a financial cap on their liabilities, subject to limitations on liability (please see the answer to question 2.8).

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

The general principles apply to all technology procurement contracts, except where specific laws provide otherwise.

For instance, these contracts may be subject to specific regulations, particularly regarding IP rights (please see the answer to question 4.1).

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Several methods are commonly used for dispute resolution in these contracts, including:

- Negotiation.
- Mediation.
- Arbitration.
- Litigation.

Some of these methods may be mandatory as per the applicable legislation. For instance, in commercial cases involving monetary claims, it is a prerequisite to engage in mediation before initiating legal proceedings.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

From an IP perspective, two laws are relevant: the Law on Intellectual and Artistic Works (**LIAW**); and the Industrial

Property Law (**IPL**). Meeting their conditions enables protection through either copyrights or industrial property rights.

For the LIAW copyright protection, assets subject to technology sourcing transactions must be considered intellectual products reflecting author characteristics (e.g., computer programs).

These assets may also be protected by industrial rights related to patents, trademarks, designs, and utility models under the IPL, providing a comprehensive framework for their protection.

In practice, the most effective way to protect IP rights is to clearly define ownership and assignment terms within the contract and include provisions for confidentiality, non-disclosure, non-compete agreements, and indemnifications.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Yes. According to the LIAW, the assignment of material rights or their use must be formalised through a written agreement. The agreement must detail the rights transferred, their scope, limitations, and duration. Failure to meet these formalities could render the assignment invalid or unenforceable. While registration of copyright assignments is not mandatory, it is advisable to register them with the Ministry of Culture and Tourism for public notice and additional legal substantiation.

Under the IPL, industrial rights can be assigned through a written agreement to be notarised by a public notary. Although notary certification is sufficient for the agreement's establishment between the parties, registration with the Turkish Patent and Trademark Office (**TurkPatent**) is necessary for effectiveness against third parties.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Know-how and trade secrets are not explicitly defined by statutes but are recognised by their confidentiality, economic value, and protective measures. While sector-specific regulations exist to safeguard critical confidential information, there's no single law governing them. Protection relies on a combination of commercial, contractual, and criminal laws.

The Turkish Criminal Code (**TCrC**) imposes imprisonment and judicial fines for disclosing commercial secrets obtained through one's title, duty, occupation, or profession, though this provision is rarely applied.

Unauthorised use of know-how, trade secrets, or confidential information may also constitute unfair competition under the TCC, allowing the aggrieved party to seek compensation and prevent unfair actions. The TCC also penalises unfair competition with imprisonment or judicial fines; these penalties, however, are rarely applied.

Furthermore, the TCO mandates employee loyalty, prohibiting them from disclosing or using their employer's trade secrets during and after employment.

Typically, companies reinforce these protections with robust contractual agreements like non-disclosure agreements, non-compete agreements, and confidentiality clauses.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

The Turkish Data Protection Law (**DPL**) is the primary legal framework regulating the procedures and principles of processing personal data. While no specific law exclusively governs personal data processing within technology services contracts, the DPL's general principles and obligations, along with relevant sector-specific regulations, provide a robust framework for such activities.

Additionally, sector-specific regulations and guidelines issued by the Personal Data Protection Authority (**DPA**) may impact how personal data is handled in technology services. For instance, Guidelines on Cookie Practices, Guidelines on Personal Data Security, and Recommendations for Protecting Privacy in Mobile Applications would be relevant to technology services involving online activities.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes,[1] the provisions governing personal data transfer abroad were recently amended to align with the General Data Protection Regulation. The new system categorises transfers into three levels:

(i) adequacy decisions;
(ii) appropriate safeguards; and
(iii) occasional causes.

The DPA can now issue these decisions for international organisations, specific sectors, and countries. If no adequacy decision exists, appropriate safeguards must be implemented, ensuring data subjects can exercise their rights and access legal remedies. Appropriate safeguards include:

- agreements between public institutions, subject to DPA approval;
- binding corporate rules, subject to the DPA approval;
- standard contractual clauses, with notification to the DPA; and
- written undertakings providing adequate protection, subject to the DPA approval.

If there is no adequacy decision or appropriate safeguard, data transfers can only occur if the transfer is occasional and specific conditions are met. These include, for example, explicit consent from the data subject, the necessity for contract performance, or an overriding public interest.

These regulations also apply to onward transfers by controllers or processors.

5.3 Are there any legal and/or regulatory requirements concerning information security?

Yes, several legal and regulatory requirements under Turkish law address information security.

The primary regulation is the DPL, which focuses on safeguarding personal data and outlines principles and regulations governing its processing and protection, including provisions dedicated to information security.

Criminalisation of activities like unlawful recording, disclosure, or obtention of personal data, as well as failure to destroy data within specified deadlines set by the laws, falls under the TCrC, alongside cybercrimes like hacking, data theft, and cyber extortion.

Various additional regulations, directives, and industry-specific guidelines complement the DPL in addressing specific information security concerns. These legislative measures collectively aim to strengthen information security, protect privacy rights, and foster trust in data handling practices.

The Law on Electronic Communication emphasised information security, providing a framework for network security, communication confidentiality, and personal data protection. Secondary legislation further elaborates on these matters, such as the Decree on Information and Communication Security Measures No. 2019/12 (**Presidential Decree**), which mandates specific security measures for public institutions and operators providing critical infrastructure services.

Additionally, the Law on Regulation of Publications via the Internet and Combating Crimes Committed by Means of Such Publications outlines obligations and responsibilities for various entities, including content providers, hosting providers, and internet service providers, to combat internet-based crimes.

Banking and payment regulations outline specific requirements as well.

Türkiye's 12th Development Plan outlines the framework for enhancing cybersecurity across all sectors in Türkiye, aiming to protect critical infrastructure and national security interests from cyber threats.

Though not legally mandated, obtaining ISO/IEC 27001 certification is also widely recognised as a standard for information security management systems.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

The transfer of employees in outsourcing or technology service contracts is primarily governed by the Turkish Labor Law (**TLL**) and the TCO.

The TLL doesn't directly regulate the transfer of employment contracts, but rather the transfer of a workplace or part thereof (e.g., sale or rent of a workplace). In such cases, all rights and obligations from the employment contract are automatically transferred to the new owner. The transfer itself does not justify termination; valid reasons (e.g., economic, technological, or organisational changes) or justified causes are required per the TLL. The transferor and transferee are jointly liable for employee obligations for two years post-transfer.

The TCO contains a provision specific to employment contract transfers. Accordingly, employment contracts can be transferred with the employee's written consent, making the transferee the new employer with all associated rights and obligations.

Even without a transfer, outsourcing relationships where subcontractors employ workers for another employer's auxiliary tasks may result in joint responsibility for compliance with the TLL and employment contracts.

6.2 What employee information should the parties provide to each other?

Turkish law doesn't mandate specific information sharing during business transfers. In practice, the transferor provides the transferee with information kept in accordance with the TLL, which typically includes employees' personal files. This is crucial because the transaction involves transferring all associated rights and obligations of the employee.

Since main employers are also accountable in subcontracting relationships, they usually request guarantees and details regarding wages and social security contributions made by subcontractors for employees.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Neither the customer nor the supplier is entitled to terminate an employment contract solely on the grounds of the transfer of a contract. However, their right to terminate the contract based on valid or justified grounds as per the TLL (please see question 6.1) remains unaffected.

Furthermore, contractual clauses may allow the customer to request changes in the employee(s) assigned by the supplier. Such a request doesn't automatically lead to the termination of the employee's contract, provided that the supplier retains the right to termination on the grounds provided by the TLL.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

No specific regulations prohibit the new employer from proposing changes to employment terms. However, material changes that diminish the rights or benefits of transferred employees require their consent.

The TLL emphasises equal treatment, ensuring no discrimination or unfair treatment of transferred employees compared to the existing workforce. Therefore, it is possible to harmonise non-material general working conditions with the existing workforce.

If an employer, party to a collective bargaining agreement (**CBA**), acquires a workplace that does not have its own CBA, the rights and obligations under the CBA apply to the transferred workplace. This implies that the CBA of the acquiring employer extends to include the new employees.

6.5 Are there any pensions considerations?

The new employer is responsible for registering transferred employees on its payroll and paying social security premiums to the Turkish Social Security Institution. Additionally, if the former employer provides a pension scheme for transferred employees, the new employer is required to maintain this scheme.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

The TLL does not specifically regulate offshore outsourcing, but the Turkish International Private and Civil Procedure Law applies. Parties can choose the applicable law for cross-border employment contracts, but this choice must not deprive employees of the TLL protections.

Additionally, parties can agree on a forum selection clause, though Turkish courts may still assert jurisdiction if the employee habitually works in Türkiye or to protect the employee's rights.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

There is no specific law regulating outsourcing transactions, but general provisions from the TCO, TCC, and TCiC apply, depending on the transaction type (please see question 1.1 and Section 2). Sector-specific regulations also cover outsourcing transactions:

- **Banking:** Banks can outsource support services under certain conditions, such as risk management plans and specific contract provisions, as per the Regulation on the Procurement of Support Services by Banks. Services like catering, transportation, and consulting are exempt.
- **Insurance:** Insurance and pension companies can outsource support services under the Regulation on Insurance Support Services, provided they meet supplier qualifications and submit a risk report to the Insurance Information and Monitoring Center. Services like consulting and advertising are exempt.
- **Capital Markets:** Institutions and public companies under the Capital Market Law can outsource information systems services if they establish a monitoring structure, prepare a technical qualification report, and execute a written contract as per the Communiqué on Management of Information Systems.
- **Payment and Electronic Money Services:** Payment and electronic money institutions can outsource services as per the Regulation on Payment Services, Electronic Money Issuance and Payment Services Providers, provided they specify the service scope in a written contract and comply with regulatory obligations. Services like consulting and advertising are exempt.
- **Payment and Securities Settlement Systems:** System operators can outsource information system services after informing the Central Bank of the Republic of Türkiye and taking the necessary measures as per the Regulation on Activities of Payment and Securities Settlement Systems.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Although Turkish law does not prescribe specific structures, in practice, several common legal or contractual frameworks are utilised:

- **Direct Outsourcing:** The supplier works post-contract with the customer.
- **Indirect Outsourcing:** The supplier subcontracts post-customer contracts.
- **Multi Outsourcing:** The customer contracts several suppliers for different work parts.
- **Joint Venture:** The customer and supplier form a joint venture for outsourcing.

Additionally, technology services-related agreements often involve various arrangements such as IP licences, SLAs, master services agreements, software-as-a-service agreements, and outsourcing framework agreements.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Technology outsourcing agreements typically include detailed SLAs to ensure service quality. SLAs specify performance metrics like uptime, response times, resolution times, and targets or benchmarks. Penalty clauses and termination provisions are often incorporated to address SLA breaches.

While service credit mechanisms are less common, they can sometimes be found in agreements influenced by US contracts.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods are as follows:

- **Interim payment or per piece:** Payment upon completion of stages or delivery of goods and services.
- **Hourly/daily fee:** Payment based on man/hours or man/days.
- **Retainer fee:** Fixed periodic payments.
- **Lump-sum payment:** One-time fixed payment.

The choice of method depends on factors like the nature of services, complexity, and the parties' preferences.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

According to the TCO, transferring a contract requires the agreement of the transferor, transferee, and the remaining party, making the remaining party's approval essential. In practice, terms regarding contract transfers are often outlined in the main contract.

Additionally, specific registration and announcement requirements must be fulfilled for business transfers to limit the transferor's responsibility.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Several key tax issues may impact both the service provider and the customer. These include:

- **Stamp Duty:** Applies to written contracts, with certain exemptions. For a standard service contract, the rate is 0.948% of the contract amount levied for each counterpart. The maximum stamp duty for 2024 is TRY 17,006,516.30.
- **Value-Added Tax (VAT):** Applies to service fees paid by the customer to the supplier, unless exempted. VAT rates range between 1% and 20%, depending on the type of service provided.
- **Corporate Income Tax:** Companies headquartered in Türkiye (full liability taxpayers) pay tax on global income, while those headquartered outside Türkiye (limited liability taxpayers) pay tax only on Türkiye-sourced income. The general corporate tax rate was increased to 25% for 2024.
- **Withholding Tax:** Professional service and royalty payments to non-residents are subject to a 20% withholding tax, potentially reduced by double taxation treaties.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Key issues to be considered are as follows:

- **Licensing Model and Pricing:** Ensure the licensing model aligns with the customer's budget and usage requirements.
- **Licence Scope and Terms & Conditions:** Determine whether the licence covers the customer's needs without over or under licensing. Reviewing the licence to understand rights, obligations, usage restrictions, renewal terms, and termination clauses is crucial.
- **Data Security and Privacy:** Ensure the software meets the necessary administrative and technical measures as per the DPL and relevant legislation.
- **IP Rights:** Verify that the software adheres to IP rights and licensing agreements.
- **Maintenance and Support:** Assess the availability, cost, and quality of maintenance and support services, including response times and SLAs.
- **Training and Documentation:** Ensure adequate training and documentation are provided for users and administrators to use and manage the software effectively.
- **Backup and Disaster Recovery**: Verify that the service provider has robust backup and disaster recovery procedures in place to minimise downtime and data loss.
- **Migration of Data:** Develop a plan for data migration, software removal, and transitioning to alternative solutions.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Key issues to be considered are as follows:

- **Compatibility and Integration:** Ensure that the service provider's services align with the customer's existing systems, infrastructure, and software environment.
- **Service Agreement Scope and Terms & Conditions:** Ensure a clear description of the services, including software updates, bug fixes, troubleshooting, configuration assistance, and technical guidance. Ensuring that the agreement addresses the rights and obligations of both parties, including SLAs, uptime requirements, and mechanisms for enforcing obligations (e.g., penalties or termination rights in cases of breaches), is crucial.
- **Data Security and Privacy:** Implement measures to ensure compliance with the DPL and relevant legislation, including defining data access, handling, and confidentiality protocols.
- **IP Rights:** Clarify the ownership of data and IP rights.
- **Maintenance and Support:** Ensure that the support and maintenance services are provided for an adequate duration with reasonable renewal options.
- **Backup and Disaster Recovery:** Verify that the service provider has robust backup and disaster recovery procedures in place to minimise downtime and data loss.
- **Training and Documentation:** Ensure adequate training and documentation are provided for users and administrators to use and manage the software effectively and determine the extent of customer support to be provided.
- **Migration of Data:** Develop a plan for data migration, software removal, and transitioning to alternative solutions.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

While software escrow arrangements are not yet widespread in Türkiye, they are gaining traction as a risk mitigation strategy for software licensees. These arrangements are generally enforceable, provided they are well-drafted and comply with the TCO.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

Türkiye lacks a single national law for cloud computing services, but various regulations apply, including those on banking, payment services, data protection, and cybersecurity, which may impose specific conditions or restrictions on cloud service procurement and use.

For instance, the Presidential Decree prohibits public institutions from using cloud services unless within their private systems or by local providers under their supervision.

Additionally, the DPA addresses cloud services in its guidelines (e.g., Guidelines on Personal Data Security), emphasising the measures to be taken when using cloud storage, such as the use of cryptographic methods for transfers.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing adoption is on the rise, driven by the need for digital transformation, cost efficiency, and scalability. Various sectors, including financial services, telecommunications, healthcare, retail, and the public sector, are leveraging cloud technologies to enhance their operations.

9.3 What are the key legal issues to consider when procuring cloud computing services?

When procuring cloud computing services, it's important to consider the general key issues outlined for procuring support and maintenance services and the data transfer abroad rules since most cloud computing services host their servers outside of Türkiye (please see questions 8.1, 8.2, and 5.2). Additionally, sector-specific regulations may impose specific restrictions and requirements.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

Türkiye lacks specific laws for the procurement or use of AI-based solutions. However, on 25 June 2024 a Draft Bill on Artificial Intelligence (**AI Draft Bill**) was submitted to the Turkish Grand National Assembly. This AI Draft Bill aims to ensure secure, ethical, and fair use of AI technologies.

Even though it is unlikely to be approved, the AI Draft Bill is significant as it represents the first effort to regulate this field. On the other hand, existing laws, including the LIAW, IPL, DPL and other sector-specific regulations may apply for the procurement or use of AI-based solutions or technologies. While not legally binding, ethical guidelines and standards for AI development and deployment also offer valuable guidance.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Given Türkiye's absence of specific AI regulations, various laws may be applied to address ownership and licensing issues related to training data for machine learning systems. The DPL, LIAW, IPL, and TCC are particularly relevant.

- **DPL:** The DPL governs the use of data in training machine learning-based systems, focusing on personal data protection. However, challenges arise regarding data subject rights, data minimisation, purpose limitation, and automated decision-making (**ADM**) processes.
  Under the DPL, data subjects have the right to object to decisions against them based solely on automated processing. However, the scope of this provision is unclear, and the lack of obligations to inform data subjects about ADM processes leads to transparency issues.
  Complying with principles like data minimisation and purpose limitation in AI usage is also complex due to the widespread use of personal data in training sets, often collected from sources like web scraping and data brokers. The methods used to collect data, especially in generative AI, make it difficult to trace data back to its subject, complicating compliance with data subject rights.
- **LIAW:** AI models based on computer programs are considered intellectual products under the LIAW and enjoy copyright protection. For training data to be protected by copyright, it must be deemed an intellectual product that bears the characteristics of the author.
- **IPL:** Inventions can be patented as per the IPL if they meet the criteria of (i) novelty in all fields of technology, (ii) reaching an inventive level, and (iii) industrial applicability. Alternatively, they can be protected as utility models if they meet these criteria but have not reached an inventive level. If a product enjoys patent or utility model protection (please see questions 4.1 and 4.2), in order to use such a product's technology and/or components as training data, proper licences should be obtained to avoid infringement as per the IPL.
  Furthermore, training data meeting criteria of novelty and distinctive characteristics may be protected as designs, while input or training data registered as trademarks may be protected as trademarks under the IPL. Trademarks and designs can be licensed as well.
- **TCC:** If components, including training data, do not meet the criteria for copyright or other IP protection, they may still enjoy protection against unfair competition under the TCC.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Since no specific legislation directly addresses AI-generated works, other applicable laws can be implemented.

Typically, algorithms are protected under the LIAW as "copyrighted material". However, like most jurisdictions, the LIAW traditionally requires human authorship for copyrightable works.

Algorithms can be patented as well if they meet the required criteria as per the IPL (please see question 10.2). However, the patent's owner must be a natural or legal person.

Hence, the ownership of algorithms developed by machine-learning techniques without human involvement is a complex issue.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

There are no specific national laws or regulations that exclusively govern the procurement or use of blockchain-based solutions. However, several existing laws and regulations indirectly affect blockchain technology and its applications by giving references to crypto assets, particularly in areas such as finance.

The Turkish Central Bank issued the Directive on Crypto-Assets Not to Be Used in Payments, which for the first time defined "crypto-assets" in Turkish law. The use of crypto-assets as an instrument of payment and the provision of services using crypto-assets in payments in a direct or indirect manner were prohibited by this directive.

The Law on Amendments to the Capital Markets Law (**CM Law Amendments**) was published in the official gazette on 2 July 2024 and entered into force immediately. The CM Law Amendments introduce new definitions and concepts including cryptocurrency, trading platforms, custody services, and service providers. They also establish certain obligations for supervising platforms and service providers, along with sanctions for non-compliance.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

In recent years, blockchain-based technologies have gained traction in various sectors, especially finance, banking, entertainment, and gaming. Despite regulatory restrictions on using cryptocurrencies for payments, blockchain technology is being used for financial applications such as trading platforms, digital asset management, and tokenization of assets.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Despite the developments regarding the introduction of regulations regarding crypto assets (e.g., CM Law Amendments), the procurement of blockchain-based technology remains unregulated under Turkish Law. Consequently, it is crucial to carefully observe existing laws and regulations that indirectly impact blockchain-based technology (please see question 11.1).

Endnote

1 Infographic on the Amendments to Turkish Data Protection Law, Yazıcıoğlu Legal, March 12, 2024, https://yazicioglulegal.com/publications/infographic-on-the-amendments-to-turkish-data-protection-law-updated-12-march-24/84

Bora Yazıcıoğlu is the managing partner at Yazıcıoğlu Legal. He has significant experience advising national and international clients on several aspects of data protection, cybersecurity, and e-commerce law. Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority. He is one of the founding members and the current president of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Reddit, Acer, Cerus, Ookla, and Avalyn Pharma in Türkiye.

Yazıcıoğlu Legal
NidaKule - Göztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy, İstanbul
Türkiye

Tel: +90 216 468 88 50
Email: bora@yazicioglulegal.com
LinkedIn: www.linkedin.com/in/bora-yazıcıoğlu-6a4bb315

Kübra İslamoğlu Bayer is the managing associate at Yazıcıoğlu Legal. She advises clients on data protection, e-commerce, information technology, consumer protection and IP laws, commercial contracts, and dispute resolution. She is an active member of the Istanbul Bar Association's IT Law Commission: the Artificial Intelligence Study Group, and the Istanbul Bar Association's Data Protection Commission.

Yazıcıoğlu Legal
NidaKule – Göztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy, İstanbul
Türkiye

Tel: +90 216 468 88 50
Email: kubra@yazicioglulegal.com
LinkedIn: www.linkedin.com/in/kubraislamoglu

Simge Yüce is a senior associate at Yazıcıoğlu Legal. She mainly focuses on data protection, intellectual property, e-commerce laws and commercial contracts. Simge is a member of the Istanbul Bar Association's Data Protection Commission.

Yazıcıoğlu Legal
NidaKule – Göztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy, İstanbul
Türkiye

Tel: +90 216 468 88 50
Email: simge@yazicioglulegal.com
LinkedIn: www.linkedin.com/in/simge-yüce-907988178

Barış Aslan is a legal intern at Yazıcıoğlu Legal. He focuses on various fields of law, including data protection, e-commerce, and contract law. Barış Aslan graduated from Bahcesehir University Faculty of Law with an honours degree. He took various courses on European Union and German law during his one-year course at Julius-Maximilians University of Würzburg with Erasmus Study Mobility.

Yazıcıoğlu Legal
NidaKule – Göztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy, İstanbul
Türkiye

Tel: +90 216 468 88 50
Email: baris@yazicioglulegal.com
LinkedIn: www.linkedin.com/in/barış-aslan-a1ab87258

Yazicioglu Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media and telecommunications, data protection, and cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection, and dispute resolution. Yazıcıoğlu Legal has a dedicated team of 12 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-related matters. In particular, the firm is known for successfully representing its clients in investigations and data breaches before the Turkish Data Protection Authority. The firm is ranked in several legal directories on TMT and is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

https://yazicioglulegal.com

YAZICIOGLU
LEGAL

United Kingdom


Mark Leach


Amelia Morris

Bird & Bird LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, procurement by private sector entities is not the subject of regulation in the UK.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Depending on its nature and value, a public sector technology sourcing contract may be subject to the UK public procurement regime. The UK public procurement regime currently includes, but is not limited to:

- The Public Contracts Regulations 2015 (as amended) (PCR 2015).
- The Utilities Contracts Regulations 2016 (as amended) (UCR 2016).
- The Concession Contracts Regulations 2016 (as amended) (CCR 2016).
- The Defence and Security Public Contracts Regulations 2011 (as amended) (DSPCR 2011).
- The Defence Reform Act 2014 (as amended) and Single Source Contract Regulations 2014 (as amended) (SSCR).

Public procurement is a devolved matter, and the above regulations apply to England, Wales, and Northern Ireland, except for the DSPCR 2011 which applies across the UK. Scotland has its own public procurement regime, which is currently substantively the same as the other UK nations' legislation due to deriving from the same EU Directives.

Procuring bodies caught by the UK public procurement regime:

- have a general overarching duty to treat all suppliers equally and without discrimination and to act in a transparent and proportionate manner; and
- owe a duty to suppliers, from the UK and specific countries which the UK has a relevant trade agreement with or are a signatory to the WTO GPA, to procure in accordance with their obligations under the UK public procurement regime (subject to the nature and value of the services/goods/works being procured). Where a procuring body breaches that duty, a supplier which in consequence suffers, or risks suffering, loss or damage may be able to bring a claim. Public authorities in the UK are also subject to judicial review.

Additionally, if procuring bodies are caught by the UK public procurement regime, they may be required to (amongst other things):

- follow certain guidance (for example, the procurement policy notes (i.e., PPNs));
- advertise the contract opportunity on the UK's e-notification service, Find a Tender Service, and/or Contracts Finder;
- follow procurement procedures which include certain minimum stages and timescales;
- design their selection and award criteria in accordance with the UK public procurement regime;
- exclude suppliers from procurement procedures where certain grounds apply (there are mandatory and discretionary grounds);
- publish certain information about the awarded contract; and/or
- only modify contracts in certain circumstances permitted by the UK public procurement regime.

Following Brexit, the UK government has sought to reform its public procurement regime. The Procurement Act 2023 (Act) received royal Assent on 26 October 2023. The Procurement Act 2023 will be supported by secondary legislation and guidance. The UK Government has stated that it intends for the Procurement Act 2023 to "go-live" on 28 October 2024. However, it is important to note that the current UK public procurement regime (discussed above) will remain relevant. The UK Government has communicated that the transitional and saving arrangements' fundamental principle is that "*procurements that commence after the entry into force of the Act must be conducted by reference to the Act only, whilst those that were commenced under the [current UK public procurement regime (e.g. the PCR 2015)] must continue to be procured and managed under that legislation*".[1] For example, a contract procured under the PCR 2015 and with a term that continues past 28 October 2024, which requires modification post 28 October 2024, must continue to be modified in accordance with regulation 72 of the PCR, not the Act.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

In general, no. However, in a public sector contract for technology-related solutions and services, the term of the

agreement and any extension may be subject to the Public Contracts Regulations.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, this is left to the parties to negotiate.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

There has been a great deal of activity in this area over the last few years, and English law continues to develop through successive decisions of the courts. At present, there is no general duty of good faith and fair dealings in English contract law. However, recent case law has suggested that a duty of good faith may be implied in two circumstances in particular:

(a) in what the English courts are increasingly labelling "relational contracts", an obligation of good faith may be implied. No one factor is determinative, but a contract is more likely to be considered "relational" if it involves (amongst other things):
- a mutual intention to establish a long-term relationship;
- a need for a high degree of communication between the parties;
- an intention for the parties' roles to be performed with integrity and fidelity to their bargain;
- a need for co-operation and predictable performance based on mutual trust and confidence and expectations of loyalty;
- an inability for the spirit and objectives of the venture to expressed exhaustively in a written contract;
- a commitment to collaboration between the parties (by contrast, the contract is less likely to be "relational" if the parties are in direct competition);
- significant investment by one or both parties; and
- exclusivity.

However, these factors have been viewed by the courts as a "sense check" rather than a series of statutory requirements and much depends on the facts of the particular case. Moreover, before an obligation of good faith will be implied, the court will also need to be satisfied that the particular contract will lack commercial or practical coherence without it (which is the normal test that must be met for any terms to be implied into a contract under English law). Although there is no direct authority on the point, it is possible that some kinds of long-term technology contracts (such as, for example, complex outsourcings) may be considered to be "relational" contracts if they meet the above criteria and in certain circumstances be subject to an implied duty of good faith in the manner described above. However, there remains a significant degree of uncertainty in this area and, as a result, if the parties wish a duty of good faith to be implied, they would be better advised to include an express term to this effect and be specific as to which obligations it should relate to. Alternatively, if they do not wish for such a term to be implied, they should include an express term to this effect (although it is recognised that it will often be difficult from a commercial and practical perspective to agree such a term at the outset of a contract).

(b) in commercial contracts requiring one party to make a decision at its discretion, the decision maker exercising such discretion must do so 'rationally', i.e. honestly, in good faith and in the absence of arbitrariness, capriciousness, perversity and irrationality. This duty is commonly referred to as the 'Braganza Duty' and will be presumed to apply in the absence of clear language to the contrary. In practice, however, analysis of when a 'Braganza duty' applies (as opposed, for example, to a situation where a party is simply exercising a contractual right) and, where it does, whether that duty has been breached, is often complex.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

The following remedies are available:
- Damages.
- Specific performance/injunction (available at the discretion of the court).
- Termination.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

In addition to the remedies available at law, the customer could seek the following protections:
- service credits;
- indemnities from the supplier for loss suffered by the customer in specified circumstances and appropriate liability caps taking into account the risk profile of the activities;
- other forms of financial consequences, such as liquidated damages, loss of exclusivity, a reduction in the minimum price payable to the supplier or the right to withhold payment;
- warranties;
- an obligation on the supplier to prepare and deliver remediation plans;
- rights to require enhanced reporting or additional monitoring rights if performance is poor;
- source code escrow;
- step-in rights allowing the customer to take over the management of an under-performing service or to appoint a third party to manage the service on its behalf;
- specific provision for termination in defined circumstances (for example, material breach or insolvency);
- a requirement for the supplier to hold insurance and note the customer's interest on its insurance policy;
- a parent company guarantee; and
- an appropriate governance or escalation structure under which each party appoints specified relationship managers to manage problem areas and to escalate them to higher levels if solutions cannot easily be found.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Any termination that occurs in accordance with the terms of the contract would be justified without giving rise to a claim for damages from the terminated party.

In addition, the following events are generally considered sufficiently serious to justify immediate termination, regardless of the terms of the contract:

- a repudiatory breach, i.e., a breach of a condition or a breach of a contractual term that would deprive the innocent party of "substantially the whole benefit of the contract";
- a breach that indicates that the counterparty no longer wishes to continue with the contract;
- if a party is unable to perform its duties under the contract, for example, through its insolvency; or
- if, through no fault of the parties, the performance of the contract becomes impossible or if external events conspire to make it radically different from what was originally envisaged by the parties. This is referred to as 'discharge by frustration'.

2.7 Can the parties exclude or agree additional termination rights?

The parties are free to agree specific termination rights, which can block or extend rights implied by general law.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

In general, in a business-to-business contract, the parties are free to exclude liability altogether, put a financial cap on liability, restrict the types of loss recoverable or remedies available and/or impose a short time limit for claims, subject to the following:

- under the Unfair Contracts Terms Act 1977 (UCTA), it is not possible to exclude or restrict liability for death or personal injury resulting from negligence. In the case of other loss or damage, the exclusion or restriction of liability for negligence must satisfy UCTA's reasonableness requirement;
- an exclusion or restriction of liability for fraud or fraudulent misrepresentation is unenforceable and should be carved out from any general exclusion of liability;
- exclusions or restrictions of liability for pre-contractual negligent or innocent misrepresentation must satisfy the requirement of reasonableness under UCTA;
- if the parties are dealing on written standard terms of business, any exclusion or restriction of liability for breach of contract must satisfy UCTA's reasonableness requirement. Where business parties have a negotiated agreement, UCTA does not apply to exclusion/restriction of liability for breach of contract; and
- implied terms as to title to, and quiet possession of, assets cannot be excluded or restricted, while those relating to satisfactory quality, fitness for purpose and certain other matters can only be restricted in business-to-business contracts where this meets UCTA's reasonableness requirement.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes; subject to the limitations set out in question 2.8.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, the same principles generally apply across all these types of technology procurement contract.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

The choice for the ultimate determination of a dispute that arises under a contract for the procurement of technology solutions and services is generally between court litigation and arbitration. Court litigation remains the most common mechanism, in part because, unless the parties agree to another approach, they will be obliged to litigate by default. However, arbitration is an increasingly popular method, particularly given that the process is confidential.

It is common for technology contracts to include certain levels of "alternative dispute resolution" as preliminary steps to be taken in order to try to resolve a dispute before the final stage of litigation or arbitration. Such steps – which can be agreed to be either mandatory or optional – often include:

- one party giving notice to the other of the nature of the dispute;
- levels of commercial negotiation between the parties about the dispute, first at an operational level with the issue being escalated up to project managers, any relevant steering/project committee and the parties' executives if it cannot be solved within specific periods of time; and
- mediation, being a confidential process under which a neutral third party (who has no binding decision-making power) is appointed to attempt to facilitate the parties in reaching a negotiated settlement.

It is also open for the parties to agree that disputes of a technical nature (or disputes that are particularly industry-specific) can be resolved by expert determination.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The parties will typically define which intellectual property (IP) rights belong to each party at the start of the relevant transaction (Background IP). This Background IP will be specifically ring-fenced to clarify that only prescribed use by the other party will be allowed. This will typically be accomplished by way of an IP licence within the scope of the agreement. The intention is that any use outside of those parameters will be prohibited.

The parties will also have to consider what new IP rights may come into existence during the course of the project (Foreground IP). The agreement will need to make provision for who will own the Foreground IP and what permission may have to be sought in order to make use of it (which may include a licence to the supplier in order for the supplier to provide the services).

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

A transfer of UK IP rights must generally be in writing and may require registration of the transfer at the UK Intellectual Property Office, depending on the IP rights involved.

The transfer of IP licences should be by written consent (where the licence is expressed to be personal or there is an express restriction on assignment).

Licences of registered trademarks must be in writing and signed by the licensor. It is also considered best practice to enter into a written agreement to license other types of IP rights. It is also usually advisable (but not a legal requirement) for an exclusive licensee of registered IP rights (such as patents or registered trademarks) to register the exclusive licence with the UK Intellectual Property Office.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

The Trade Secrets (Enforcement, etc.) Regulations 2018 came into force on 9 June 2018, implementing provisions of the Trade Secrets Directive in the UK.

Under English law, parties will typically agree contractual confidentiality provisions rather than relying on confidentiality protection at common law. Contractual confidentiality provisions are likely to include: defining the know-how, trade secrets and confidential information of each party; creating a contractual duty to maintain this information in confidence (subject to some typically agreed carve-outs); specifying its use within the scope of the IP licence (see question 4.2 above); and defining the duration of the confidentiality undertakings (for a fixed period or potentially indefinitely depending on the perceived value of the confidential information).

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Yes, the processing of personal data is regulated by national law. While detailed analysis of this area is beyond the scope of this chapter, some key issues to be aware of include the following:

a) Applicable laws: The UK's main pieces of data protection legislation are the UK GDPR and the Data Protection Act 2018.

b) Supplier's role: Are they a processor or a controller on the facts? Note that both controllers and processors have responsibility for compliance with the UK GDPR. A controller is a legal entity that alone or jointly with others determines the purposes and means (the 'why' and 'how') of the processing of personal data, whereas a processor is a legal entity that processes personal data on behalf of a data controller (i.e. it has no independent reason for processing the data for its own purposes and will only process data on the controller's instructions). It is possible for an organisation to be both a controller and a processor for different activities relating to the same data and contract – for example, a technology services provider may act as a processor for its primary SaaS services, but may act as a controller if permitted to reuse any of this data for service improvement. Parties may be joint controllers where they make joint decisions on the purposes and means of the processing. The accountability principle of the UK GDPR and the provisions of Article 28 (which governs the relationship between controllers and processors) require organisations to only select personal data processing parties which offer sufficient guarantees to maintain appropriate technical and organisational security measures. So procurement due diligence and ongoing audit measures will be required in relation to technology providers who will process data which is regulated by the UK GDPR.

c) Contractual provisions: Article 28 of the UK GDPR requires contracts with processors to set out certain information regarding the processing (including the subject matter, duration and nature of the processing). Compliance with this article is a mutual responsibility between the controller and processor – processors have been fined where their standard terms fall short of compliance. Contracts must impose all necessary contractual obligations set out in Article 28(3), which includes obligations on processors to act only on the instructions of the controller, to put in place appropriate technical and organisational measures to protect personal data and to notify the controller of a security breach amongst others. Processors must be placed under an obligation to flow down the same data protection provisions to any sub-processor appointed for processing activities on the controller's behalf. Article 28(3) also requires that the processor be obliged to assist the controller in fulfilling various of its obligations under the UK GDPR, including dealing with end user rights, such as access, data portability and the right to erasure, as well as the completion of data protection impact assessments and breach notification. The UK GDPR is silent on the question of costs so parties are free to negotiate who will bear the cost of such assistance. Under the GDPR, organisations are required to adopt significant new technical and organisational measures to demonstrate their compliance. Where a supplier is a joint controller, under Article 26 of the UK GDPR there is a need to set an allocation of responsibility in writing – this does not strictly need to be contractual, but it is usually in the parties' interests to ensure this is formally agreed. In all contracts where personal data is processed, liability provisions will need careful review, especially with maximum fines under the UK GDPR being the greater of 4% of worldwide turnover or £17.5 million.

d) Other legislation: Other legislation may be relevant depending on the nature of the parties and services. This includes (i) the Privacy and Electronic Communications Regulations 2003, best known for its cookie rules, (ii) the Investigatory Powers Act 2016 when processing communications content, and (ii) the Freedom of Information Act 2000 when dealing with public sector entities. Organisations should also be aware of the progress of reforms to the UK's data protection regime which has been proposed in various Parliamentary bills in recent years but none have passed through Parliament and been adopted. At the time of writing, it is unclear what reforms will be made following the 2024 General Election.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Like the data protection laws that preceded them, both the EU's and the UK's versions of the GDPR contain restrictions on transfers of personal data to locations that do not offer adequate protection for the rights of affected data subjects. Both legislative regimes provide for derogations from this restriction and for safeguards that can be used to facilitate the transfer of personal data to non-adequate destinations. In particular, in the UK, both an ICO produced International Data Transfer Agreement and a UK Addendum to EU produced Standard Contractual Clauses (SCCs) have been approved by Parliament. Other alternatives include the use of UK Binding Corporate

Rules, or reliance on approved certifications, codes of conduct or the exemptions available under the UK GDPR.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The UK GDPR requires controllers and processors to have technical and organisational measures to ensure appropriate levels of security when processing personal data under Article 32, including the security of processing systems and services. As covered above, this includes obligations that contracts contain obligations to apply these security measures in practice. The Network & Information Security Regulations 2018 (NISR) also apply to information security and may be relevant in the context of a technology sourcing contract. A full discussion of the NISR is beyond the scope of this chapter but, in broad terms, the provisions of the NISR apply to operators of essential services (OES) in the energy, water, health and transportation sectors, and digital service providers (DSPs), which include operators of online marketplaces, operators of online search engines and cloud computing service providers. OES and DSPs will continue to be accountable for the protection of the service they provide and must therefore: (i) demonstrate they have appropriate and proportionate security measures in place to manage the risks posed to their network and information systems; (ii) demonstrate they have appropriate measures in place to prevent or minimise the impact of incidents affecting the security of their systems; and (iii) be ready to report significant incidents to their relevant competent authority. Accordingly, in the context of a technology sourcing contract, if the customer falls within the scope of the NISR and the project involves the supplier having access to the customer's IT systems, additional obligations may need to be added to the contract in order to enable or facilitate the customer's continued compliance with the NISR. The UK government has published proposals to update the NISR to apply to a broader range of operators to include "managed services"; however, at the time of writing, there is no indication of when the UK would update the NISR. The UK has separately implemented sector specific information security requirements specifically for telecoms providers contained in the Telecoms Security Act 2021 (TSA) (amending the Communications Act 2003). A full discussion on the TSA is beyond the scope of this chapter, but, in general terms, it sets detailed requirements for providers to identify and mitigate against the effects of security compromises to their networks and services. Finally, the Product Security and Telecommunications Infrastructure Act and the associated PSTI (Security Requirements for Relevant Connectable Products) Regulations have implemented certain security measures for connected products made available on the UK market.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Unless there is a fundamental change in the nature of the work or how it will be undertaken, the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) are likely to apply to outsourcing transactions and certain other technology services-based agreements, but a careful factual and legal analysis is required to determine whether each element of the test for a 'relevant transfer' is met.

If TUPE does apply, the customer's employees who are, immediately prior to the transfer, wholly or mainly assigned (other than on a temporary basis) to an organised grouping of employees which has, as its principal purpose, the carrying out of the relevant service, will automatically transfer to the supplier. On a change of supplier, employees wholly or mainly assigned to such a grouping transfer automatically from the existing supplier to the new supplier. If the outsourcing or other technology services agreement comes to an end and the customer brings the relevant services back in-house, the employees of the supplier who are wholly or mainly assigned to the organised grouping transfer back to the customer. Employees of subcontractors of the supplier may also be covered.

Depending on the factual circumstances, where services are being split and transferred to multiple new suppliers, it may be possible for an employment contract of a transferring employee to be split between each of the transferees in proportion to the tasks being performed by the worker.

Under TUPE, all of the rights, liabilities, powers and duties of the outgoing employer under or in connection with the transferring employees' contracts of employment transfer, with limited exceptions. This includes any pre-existing liabilities (e.g. arrears of pay, discrimination claims) and accrued contractual benefits (e.g. holiday entitlement, car allowance). The transferee steps into the shoes of the transferor and legally it is as though the transferee has always been the employer.

6.2 What employee information should the parties provide to each other?

The transferor must identify those employees who are in scope to transfer and is required to provide the new supplier with "employee liability information" (prescribed by statute) at least 28 days before the date of the relevant transfer (normally, commencement of the contract term).

The transferor will therefore have to collate and disclose information to the transferee such as the number of employees involved in the outsourcing, their job descriptions and the key terms of their employment contracts. The parties will also have to consider the following (non-exhaustive) factors: (i) whether there are any unions involved; (ii) if so, whether there are any existing collective agreements; and (iii) whether consultations with unions/employee representatives have commenced.

The transferee must provide the transferor with details of any 'measures' it envisages taking in relation to the transferring employees. This must be done long enough before the expected transfer date to enable the transferor to inform and consult with appropriate representatives of its employees who are affected by the transfer. Currently, micro businesses (those with fewer than 10 employees) may consult directly with affected employees in certain circumstances. For transfers that take place on or after 1 July 2024, this exemption will also apply where either the employer employs fewer than 50 employees or fewer than 10 employees will transfer.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

A dismissal will be automatically unfair where the dismissed employee has two or more years' continuous service and where the sole or principal reason for the dismissal is the transfer itself, unless the dismissal is for an 'economic, technical or organisational reason entailing changes in the workforce' (ETO) and the dismissing employer acted reasonably in treating

the ETO reason as sufficient to justify dismissal. Dismissals effected before a transfer will usually not fall within the ETO defence and a transferor cannot rely on a transferee's ETO to justify pre-transfer dismissals.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Any change to terms of employment where the sole or principal reason for the change is the transfer is void save where there is an ETO reason or in certain other limited circumstances. Any change made purely to harmonise with those of the supplier's existing workforce is likely to be void. An employee who agrees to harmonised terms introduced in connection with a TUPE transfer may in some cases be able to rely on those new terms that are more beneficial than his or her old contract but will not be bound by any terms that are less favourable.

6.5 Are there any pensions considerations?

TUPE specifically exempts rights under occupational pension schemes that relate to old age, survivor or disability benefits from transfer. However, the European Court of Justice has established that occupational pension rights falling outside these categories (e.g. rights to benefits on redundancy or early retirement) may be transferred under TUPE in certain circumstances. Where stakeholder, personal or group personal pension arrangements are in place before the TUPE transfer, the transferor's contractual obligations to contribute to these schemes will transfer.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

TUPE applies to offshoring insofar as immediately before the transfer, there is an organised grouping of employees in the UK carrying out the relevant services. In theory, the employees should transfer to the supplier and it is then for the transferee supplier to effect redundancies as appropriate (assuming the employees cannot be relocated or do not wish to relocate). In practice, the transferor may decide to run a redundancy consultation alongside a TUPE consultation and, in some circumstances, there is a legal basis for the transferee to participate in a pre-transfer redundancy consultation, with employees being made redundant immediately upon transfer.

Parties involved in offshore outsourcing should pay attention to local laws when the customer re-tenders the outsourced services or brings them back in-house at the end of the outsourcing agreement. It is commonly thought that employment laws outside the EU are more relaxed than those within, but this is not always the case and it should not be assumed that the supplier's employees can simply be dismissed.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

a) Financial Services sector: the Financial Services and Markets Act 2000 (FSMA) is the main piece of legislation that regulates financial services in the UK. The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) are the regulators established with powers under FSMA, and each regulator consults and issues rules and guidance and supervises the conduct of firms in this area (as applicable). A firm that is regulated by the FCA or the PRA cannot delegate or contract out of its regulatory obligations when outsourcing and must give advance notice to the FCA or PRA (as applicable) of any proposal to enter into a material outsourcing arrangement and of any material changes to arrangements. Following the implementation of the MiFID II Directive and MiFID Organisational Regulation, MiFIR and the associated implementing legislation on 3 January 2018, outsourcing for banks, building societies and investment firms is now governed by Articles 30–32 of the MiFID Organisation Regulation, SYSC 8 and the Outsourcing Part of the PRA Rulebook. Firms falling within the scope of these regulations must enter into outsourcing arrangements in compliance with a number of conditions, and must also exercise due skill, care and diligence when entering into, managing and terminating outsourcing arrangements for critical or important functions. The European Banking Authority's (EBA) Guidelines on Outsourcing Arrangements (EBA Outsourcing Guidelines) came into force on 30 September 2019 – they apply not only to banks, building societies and investment firms but also to payment institutions and electronic money institutions. The EBA Outsourcing Guidelines set out requirements in relation to the assessment and monitoring of outsourcing arrangements, the contractual documentation of outsourcing arrangements and the necessary governance arrangements that should be in place when a firm outsources a function. With respect to reviewing existing outsourcing arrangements, these institutions had until their next contract renewal, or 31 December 2021 at the latest, to bring them into line with the EBA Outsourcing Guidelines.

In March 2021, the PRA published its own outsourcing guidance for UK banks, PRA authorised investment firms, building societies, insurers and UK branches of overseas banks or insurers, under the PRA Supervisory Statement on Outsourcing and Third-Party Risk Management SS2/21 (the SST). The aims of the SST are to facilitate greater resilience and adoption of the cloud and other new technologies by PRA authorised firms and implement the EBA Outsourcing Guidelines. The SST clarifies how the PRA expects banks to approach the EBA Outsourcing Guidelines in the context of its requirements and expectations. In addition, certain chapters in the SST expand on the expectations in the EBA Outsourcing Guidelines, for instance Chapters 7 (Data security) and 10 (Business continuity and exit plans).

For any outsourcing arrangements within scope of the SST entered into on or after 31 March 2021, firms were expected to have ensured such arrangements comply with the requirements of the SST by 31 March 2022. For any legacy outsourcing arrangements entered into before 31 March 2021, firms have had until the first appropriate contract renewal/revision point to meet the expectations of the SST as soon as possible on or after 31 March 2022.

The PRA has also developed operational continuity in resolution (OCIR) rules for certain banks and building societies that satisfy certain deposit thresholds (In-Scope Firms) which apply to critical services that are provided to these In-Scope Firms. The OCIR includes requiring these In-Scope Firms to have certain contractual rights to continuity of services when entering into resolution. These requirements are set out in further detail in the Operational Continuity Part of the PRA Rulebook.

Insurers are subject to certain outsourcing requirements under the Solvency II Directive (including Article 274 of the Delegated Regulation EU/2015/35) and SYSC 13 of the FCA Handbook, which require certain requirements to be included in their contractual framework with arrangements that involve a critical or important outsourcing. These include comprehensive audit and premises access rights and undertakings relating to the preservation of the integrity and security of customer data. The EIOPA Guidelines on outsourcing to cloud service providers (the EIOPA Outsourcing Guidelines) was published in January 2020 and since 1 January 2021 has applied to all cloud outsourcing arrangements entered into or amended on or after this date by insurers or reinsurers. The PRA has stated that it has considered and incorporated the EIOPA Cloud Outsourcing Guidelines in the SS.

The FCA and PRA have also published policy statements and final rules on operational resilience requirements. The regulators expect firms and the financial sector to prevent, adapt, respond to, recover and learn from operational disruptions, whether in relation to macro-economic events or specific third party arrangements. Firms are responsible for setting "impact tolerances" for each "important business service" which is the term used by the regulators to mean the maximum tolerable level of disruption to an important business service.

Dual-regulated firms must comply with both the FCA and PRA's rules, including the potential requirement to set different impact tolerances to comply with the different requirements. The FCA's Policy Statement PS 21/3 on building operational resilience set out expectations relating to outsourcing for FCA authorised firms: when a firm is using a third-party provider in the provision of important business services, it should work effectively with that provider to set and remain within impact tolerances. Ultimately, the requirements to set and remain within impact tolerances remain the responsibility of the firm, regardless of whether it uses external parties for the provision of important business services.

The FCA also expects firms in scope to be responsible for accurately mapping any relationship outsourced to an external third party. Ultimately, if a third-party provider supplying an important business service to a firm fails to remain within impact tolerances, that failure is the responsibility of the authorised firm. The authorised firm is expected to manage these impact tolerances through its risk management framework and oversight and supervision controls on the service provider including, but not limited to, agreed service levels, agreed downtime periods, business continuity plans and agreed penetration testing arrangements.

b) Other industry sectors: the following non-exhaustive list sets out the other main industry sectors (in addition to financial services) that are subject to sector-specific regulation and which may include requirements in relation to outsourcing. It is beyond the scope of this chapter to outline all of these sector-specific requirements. We therefore recommend checking with the relevant regulator as to whether any such regulations exist.

- Aviation (Civil Aviation Authority).
- Consumer credit (FCA).
- Education and childcare (Ofsted).
- Energy (Ofgem).
- Food (Food Standards Agency).
- Gambling (Gambling Commission).
- Health and social care (Care Quality Commission).
- Medicines and medical devices (Medicines and Healthcare Products Regulatory Agency).
- Pensions (Pensions Regulator).
- Rail (Office of Rail and Road).
- Road transport (Driver and Vehicle Standards Agency and Office of Rail and Road).
- Security services (Security Industry Authority).
- Telecommunications, broadcasting and postal services (Ofcom).
- Water and sewerage services (Ofwat).

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The simplest outsourcing structure is a direct outsourcing between the customer and the supplier.

In a multi-sourcing, the customer enters into contracts with different suppliers for separate elements of its requirements.

In an indirect outsourcing, the customer appoints a supplier (usually UK-based) that immediately subcontracts to a different supplier (usually non-UK-based).

An alternative option is for the customer and supplier to set up a joint venture company, partnership or contractual joint venture, perhaps operating in an offshore jurisdiction, which provides services back to the customer. This model is often used where there is an opportunity for the outsourced function to provide services to third parties (as well as the customer).

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

When negotiating the contract, the parties usually try together to identify and agree a set of objective, measurable criteria to measure the supplier's performance (key performance indicators (KPIs) or service levels). These service levels need to be combined with a:

- process for recording and reporting on success or failure in achieving the targets; and
- formula under which financial compensation is paid to the customer if targets are not met. These are referred to as service credits or liquidated damages.

The aim of service credits is to compensate the customer for poor service without the need to pursue a claim for damages or terminate the contract, and to motivate the supplier to meet the performance targets.

The supplier will want to ensure that the stated service credits are the sole remedy of the customer for the particular failure concerned, but this should be without prejudice to the customer's wider rights in relation to more serious breaches of the contract or persistent failures in performance. Service credits are generally enforceable, provided they are a genuine pre-estimate of the customer's loss or can be shown to protect a legitimate commercial interest of the customer and are not a contractual penalty.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The method of charging will depend on the type of services being outsourced, the nature of the supplier's appointment and the balance of risk between the parties.

The most common charging methods are as follows:

- Cost plus, where the customer pays the supplier both the actual cost of providing the services and an agreed profit margin.
- Where there will be a regular and predictable volume and scope of services and the customer wants to have greater certainty over its budget, a true fixed price will be a better option for a customer.
- Where the level and volume of service is less predictable, the parties may decide to opt for a pay-as-you-go charging model whereby the customer pays a pre-agreed unit price for specific items of service (such as volumes of calls taken), often based on a rate card.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

The assignment of key contracts must be in writing. The parties should check the terms of such contracts at an early stage to ensure that they are able to assign, without the counterparty's consent and attempt to obtain such consent if necessary. Alternatively, if the terms of the contract permit, the customer can retain ownership of the contract and allow the supplier to supply the services to the counterparty as agent of the customer on a 'back-to-back' basis.

It should also be considered whether the burden of the contract should also transfer to the supplier, either by:

- novation; or
- express indemnity (which leaves some residual risk with the transferor).

The concept of a contract being leased or licensed is not generally recognised under English law.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

On entering into an outsourcing arrangement, there may be a transfer of assets and/or part of a business to the supplier for tax purposes. The main UK tax issues that might arise are:

(a) **Direct tax on transfer of assets**

a) the disposal of certain assets may trigger corporation tax on any chargeable gains;

b) the disposal of any IP (including goodwill and certain other similar intangible assets) created or acquired on or after 1 April 2002 could be subject to corporation tax under a separate regime for intangible fixed assets. The supplier (as purchaser) should be able to obtain a corporation tax deduction for amortisation of the cost of such IP (including goodwill if acquired as part of the acquisition of a business and with other IP assets, from 1 April 2019);

c) the transfer of any interests in land may be subject to stamp duty land tax (if located in England or Northern Ireland), land transaction tax (if located in Wales) or land and buildings tax (if located in Scotland); and

d) the transfer of plant and machinery is unlikely to give rise to a taxable gain. However, the disposal proceeds in respect of those assets are likely to be credited to the company's capital allowance pool. This may give rise to a balancing charge or allowance.

In most circumstances, however, the only assets being transferred will be plant and machinery, along with the employees.

(b) **VAT**

a) An asset transfer taking place in the UK will generally give rise to VAT on the consideration provided or deemed to be provided in return for the asset. VAT may also be due on the service fees charged by the supplier for the provision of the outsourced services.

b) Where a part of a business is being transferred, this could amount to a 'transfer of a going concern' (TOGC) for VAT purposes. The effect of this would be that the transfer is not treated as a supply for VAT purposes so no VAT would be chargeable on the transfer. However, such treatment may be open to challenge in the outsourcing context as, for TOGC treatment to apply, the assets transferred must be part of a business 'capable of separate operation'. This generally requires the assets of the part of the business being transferred to have been used to make supplies (and not merely used for the overheads of the business) and, as such, may not apply to, for example, the transfer of back-office functions. HMRC's stated view is that an 'in-house' function is not a business for TOGC purposes when it only operates internally.

c) In outsourcing arrangements that are not entered into between two independent parties (e.g. a joint venture arrangement), the parties may be eligible to form a VAT group enabling intra-group supplies made between the group entities to be disregarded for VAT purposes. In the past, this arrangement was often used by financial services businesses using VAT grouping in the context of overseas outsourcing, although such arrangements have increasingly been challenged by HM Revenue & Customs (HMRC), including as to whether the overseas service provider has a UK establishment of sufficient substance to avoid being de-grouped.

d) VAT exemptions are being construed increasingly narrowly, in particular for finance-related outsourced services concerning payments or transfers. This has most recently been indicated in the 2023 Supreme Court's decision of *Target Group Ltd v HMRC* which considered whether outsourced loan administration services to a bank constituted VAT exempt financial services. The appellant was unsuccessful, based on a narrow and strict interpretation of the exemption being held by the Supreme Court as the correct test, overruling an earlier wider interpretation applied in case law. The decision clarified that these types of services must in themselves have the effect of transferring funds and changing the legal and financial situation, requiring functional participation in the execution of an order for payment or transfer. It is not enough to give instructions to other financial institutions to effect such transfers. Businesses involved in fintech payment services, where the functions performed within the payment chain are increasingly split between legal entities, may find it will become more difficult to argue that their services as a distinct whole fulfils the essential functions of a financial transaction qualifying for VAT exemption.

e) The termination of any outsourcing arrangements could involve a re-transfer of assets (or business) back to the customer. The tax issues set out above will therefore also be relevant on termination.

f) When a business outsources, e.g., an in-house function which, before the outsourcing, was not subject to VAT, the additional VAT costs at stake as a consequence of entering into an outsourcing transaction could become significant, depending on both the nature of the services to be supplied and the parties involved. In particular, VAT leakage in outsourcing arrangements,

in the form of increased irrecoverable VAT, can be a key concern for a customer if their main business involves making all or partly VAT exempt supplies (e.g. health, education, finance, insurance) where it is unable to recover any VAT incurred on the supplier's service fees or only some of this VAT in accordance with its partial exemption recovery method.

How to address any VAT leakage will usually involve commercial negotiation and may require looking at price adjustment mechanics if, for example, the parties are to share in or compensate a party for any increased irrecoverable VAT burden including on a change of VAT law or treatment by HMRC. Alternatively, the parties could work together and seek HMRC clearance and/or look to change or restructure the nature and delivery of the supplies to improve VAT efficiency, such as VAT grouping via a joint venture/LLP structure with the customer, unbundling supplies to genuinely make separate exempt supplies rather than single composite/packaged supplies subject to a single VAT rate treatment, extending the scope of services outsourced to meet the requirements of an applicable VAT exemption, or using joint employment contracts where there is no separate taxable supply of staff for UK VAT purposes (so no VAT cost) between each joint employer. However, although there may be a number of mitigation possibilities, it should be borne in mind that HMRC has been successful in challenging a number of outsourcing arrangements entered into with a view to mitigating VAT costs and has wide powers to counter artificial arrangements under VAT anti-avoidance legislation (e.g. supply splitting anti-avoidance) and/or the "Halifax" VAT abuse case law doctrine. For example, the effectiveness of joint employment contracts has been called into question by case law holding that fees payable for outsourced IT services were subject to VAT despite a joint employment arrangement, based on the substance and economic reality of how the services were provided. More recently, in *JPMorgan Chase Bank, NA v HMRC*, the First-tier Tax Tribunal (2023) has held that certain outsourced general support and business delivery services supplied in the UK within the banking group constituted a single composite supply of services for which, on the facts, a predominant or principal element could not be identified, and as such, as a whole this complex supply could not qualify for VAT exemption. It is understood that this decision is being appealed but it highlights the difficulties of identifying specific, individual exempt outsourced supplies within a global group context where there may also be a lack of a detailed descriptions of and separate group invoicing for the outsourced services. In contrast, HMRC has also recently lost in a case involving an NHS trust that had outsourced certain healthcare facilities and challenged HMRC's decision that consumable goods supplied to the trust were a separate supply, outside the scope of a special regime that provides refunds of VAT incurred in the supply of contracted-out services to NHS trusts and certain other public bodies. The Upper Tribunal agreed with the trust that objectively considered, from the point of view of the trust, the outsourced services and consumables formed, for VAT purposes, a single, indivisible and composite supply of services that it would be artificial to split, so the NHS trust was entitled to a VAT refund in respect of the VAT incurred on the consumables *(The King (on the application of Gloucestershire Hospital NHS Foundation Trust) v HMRC (2023))*.

Any VAT mitigation approach would therefore require careful attention to ensure the structuring and documenting of the outsourcing transaction supports the intended VAT treatment and is properly implemented (with procedures in place to ensure such proper implementation is maintained over time) and reflects the substance and economic reality of the supplies in question.

Although tax on transferring assets and VAT are the main tax issues that arise in an outsourcing context, there are other tax issues that may arise. These include:

a) **Permanent establishment** – on a cross-border contract, the supplier may form a permanent establishment (taxable presence) of the customer in the jurisdiction in which the supplier is based.

b) **Withholding taxes** – payments to the supplier could be subject to withholding taxes, if the customer is not in the UK. This will depend on the nature of such payments and any double tax treaty protection. The UK currently imposes withholding tax (at the rate of 20%) on payments of royalties and interest. Therefore, if there are any payments for the use of IP, care should be taken to ensure that the contract is clear as to which party will bear that tax, otherwise the recipient will bear the whole tax burden. Further consideration in the contract should be given to allocating change of law risk between the parties. Although the UK currently only imposes withholding taxes in limited situations, if that scope were to be expanded, it would be sensible for the contract to allocate that tax risk.

c) **Employees** – where employees are transferred to the supplier under the outsourcing contract, the obligation to account for PAYE, National Insurance Contributions and any Apprenticeship Levy will also pass. The contract should deal with any specific payments that may be made.

d) **Changes to the arrangements** – where the services supplied under an outsourcing contract change, this could change the tax treatment of the services. The persons who bear any risk in this respect will need to be set out in the contract.

e) **Changes in law or HMRC practice** – complex drafting considerations may arise around how to respond to and address material changes in law or in HMRC practice, or an adverse HMRC challenge, which results in an unexpected outcome or material impact to the outsourcing arrangements (e.g. a new VAT charge, or reversal to VAT exempt treatment). Issues can include control and cooperation over handling HMRC disputes, future appeals, litigation and costs, pricing adjustments or other contractual changes to mitigate the tax impact for a party (for example, to take into account reduced VAT recovery on costs), whether to restructure the arrangements to help restore the previous tax treatment (if possible), and/or termination event rights).

f) **Contractors** – consideration should also be given to the off payroll working rules (also known as "IR35") under which UK businesses engaging workers via intermediaries are obliged to assess those workers' deemed employment status for tax purposes. These rules do not apply when a service is "contracted out" but as this is the only exemption, customers should expect increased scrutiny from HMRC for outsourced services. In a genuinely outsourced arrangement, a UK supplier (assuming it is not small) will be responsible for making these assessments if any workers are supplying their labour through intermediaries to the supplier.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Where software applications are installed on a customer's own systems (as opposed to being accessed remotely on a software-as-a-service model), some of the key issues to consider from a contractual perspective include the following:

- **Permitted users**: users will need to be expressly licensed to use the software so a customer should consider whether, for example, other group companies will need to be licensed in addition to the main customer entity. Restrictions will often be placed on the number of individual users who may access or use the software. Care should be taken if software may be accessed directly or indirectly by third parties, such as an outsourcing service provider or by the customer's own customers, and an analysis undertaken as to whether these entities need to be expressly licensed to use the software.
- **Other restrictions**: a software vendor will often seek to impose restrictions around the geographic locations in or from which the software can be used or accessed, the number of machines on which it can be loaded, the number of copies that may be taken, the processing volumes that may be handled and/or the nature of the operating environment on which the software is loaded. These should all be checked to ensure they are consistent with a customer's business requirements and intended use of the software.
- **Open source software (OSS)**: a customer should check whether the software includes any OSS code. A detailed analysis of OSS issues is beyond the scope of this chapter, but in general terms where OSS is present, it will be licensed under its own terms which, while free of many of the use restrictions that apply to proprietary software, will generally contain fewer protections for a customer and be licensed on an 'as is' basis. Particular issues can also arise where a customer wishes to modify and adapt and possibly distribute the software and one of the more restrictive OSS licences is used.
- **Warranties**: appropriate warranty protection should be sought in relation to the performance of the software and its conformance to specification; for package software this is often limited by vendors to an undertaking to rectify faulty software free of charge for a defined period after delivery/installation.
- **IP Infringement protection**: indemnities should be sought against the risk of a customer's use of the software infringing a third party's IP rights.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Key issues include:

- ensuring a clear description of the support and maintenance service is set out in the contract, including a clear definition of what constitutes a "fault" or "defect";
- ensuring appropriate service levels (and where applicable an associated service credit regime) are included; particular care should be taken around the categorisation of the severity of faults and the service levels that apply to each category;
- understanding whether the provision of upgrades and new versions of the software are included within the service or not and, linked to this, whether the vendor requires the latest version of the software to be run as a condition of providing the support and maintenance service;
- if the services will be provided remotely or on site (or a mixture of both); and
- understanding whether, in providing the services, the vendor will have access to personal data being processed by the software – where it does, the customer will need to put in place arrangements (including appropriate contractual clauses) to ensure that the personal data is processed in accordance with the Data Protection Act 2018 (DPA) and the GDPR.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Yes, although software vendors are often reluctant to agree to them.

In broad terms, escrow agreements are generally enforceable from an English law point of view, as long as they are not entered into when the insolvency of the vendor is actually in contemplation. From a practical point of view, the utility of an escrow arrangement for a customer will depend on the source code deposits being kept up to date and appropriate documentation being included in the escrow deposit that is sufficient to enable a competent programmer to understand the source code.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

There are no national laws or regulations that apply specifically to cloud computing arrangements *per se*, but the operation of cloud computing solutions in the UK will need to comply with UK data protection and, in certain industry sectors, cyber security requirements. There are also certain industry-specific regulations that affect the way in which cloud computing arrangements are undertaken and operated – for example, in the financial services sector.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Cloud computing solutions are being adopted widely in the UK, across a wide range of industry sectors.

9.3 What are the key legal issues to consider when procuring cloud computing services?

Many cloud vendors, particularly those offering multi-tenanted public cloud services, will insist on contracting on their standard terms and little if any negotiation is possible. For bigger deals or more bespoke arrangements based on private cloud delivery models, more negotiation tends to be possible but, generally speaking, a customer will still need to accept a different balance of risk than it would be used to in more traditional IT contracts.

Other key issues that a customer will need to consider include:

- appropriate licence and usage rights for applications made available via the cloud service;
- appropriate service levels, particularly around service availability, and appropriate remedies for a service level failure;
- ensuring that customer data that will be stored in the cloud is accessible and required to be returned (in a useable format) on termination/expiry;
- as the cloud vendor will normally be a data processor for data protection purposes, ensuring that GDPR-compliant processing provisions are included in the contract;
- understanding in which territories any personal data will be stored and ensuring that any data export arrangements comply with applicable Data Protection legislation;
- whether the level of protection afforded by the supplier's business continuity and disaster recovery arrangements is sufficient for the customer's purposes;
- the extent to which the supplier is entitled to use data stored on its systems for data analytics or other purposes; and
- the extent of the indemnity protection offered by the cloud vendor for third-party IP right infringement.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

There is currently no single overarching national law or regulation in the UK that specifically regulates the use of Artificial Intelligence-based solutions. However, in March 2023, the UK government published a White Paper outlining a framework for the UK's approach to regulating AI and sought responses from stakeholders over a consultation period. In February 2024, the government published its response to the consultation.

The government has decided to support existing regulators (e.g. ICO, the CMA, the FCA, Ofcom, the Health and Safety Executive, the MHRA and the Human Rights Commission) by developing a sector-focused, principles-based approach rather than legislate to create a single function to govern the regulation of AI and have announced they will provide £10 million to jumpstart regulators' technical capabilities in relation to AI. An analysis of the White Paper and government response is beyond the scope of this chapter, but in brief the government has confirmed that the following five cross-sectoral principles will initially form a non-statutory framework which regulators should consider in developing an approach to the use of AI in their sector:

- safety, security and robustness;
- transparency and explainability;
- fairness;
- accountability and governance; and
- contestability and redress.

In February 2024, the government released a paper titled "Implementing the UK's AI Regulatory Principles: Initial Guidance for Regulators" which sets out the first phase of voluntary guidance for regulators. The second phase is expected in summer of 2024 and should build upon the first phase, which provides guidance for regulators when applying the framework principles in practice and developing tools and guidance for their regulatory remits.

The government has also established the AI Safety Institute. The AI Safety Institute is not an AI regulator, rather, its role is to develop the technical expertise to understand the capability and risks of AI-based solutions which will inform the government's broader actions in the future.

The government has also asked various regulators to publish an update outlining their strategic approach to AI. A summary of some, but not all, of these regulators' strategies are set out below:

- **CMA**: In the CMA's AI strategy, they have outlined various risks that AI-based solutions pose to both competition and consumers. They have outlined six principles which companies should take into account when dealing particularly with AI foundation models. These principles are: access; diversity; choice; fair-dealing; transparency; and accountability. The CMA has noted that under the Digital Markets, Competition and Consumers Act 2024, the CMA has more powers to enforce consumer law protection against companies, which include those using AI.
- **FCA**: The FCA have highlighted that its regulations do not mandate or prohibit certain technologies, but objectively assess the risks and any adverse implications of the use of any new technologies (such as AI) by regulated firms. The FCA has highlighted that existing legislative and regulatory frameworks can be used in the regulation of AI, for example: the principle of proportionality under the Financial Services and Markets Act 2000, where any burden or restriction placed on a firm in relation to AI must be proportionate.
- **Ofcom**: Ofcom has an inspection framework which allows it to inspect the provisions and outcomes of AI affecting areas such as safeguarding, particularly regarding children and learners. Ofcom also highlighted the need for companies to comply with existing legislation such as the new Online Safety Act and the general conditions for telecom providers under the Communications Act 2003.
- **HSE**: The HSE has highlighted that the government principles (set out above) relevant to workplace health and safety are as follows: safety, security and robustness; appropriate transparency and explainability; and accountability and governance. The HSE also expects a risk assessment to be undertaken for uses of AI which impact on health and safety and appropriate controls to be put in place to reduce risk so far as is reasonably practicable, including how companies will address cyber security threats.
- **ICO**: The ICO has released guidance on AI and data protection. The ICO can enforce data protection rules by information notices, assessment notice, enforcement notices and monetary penalty notices, and have recently fined a facial recognition database company more than £7.5 million for breaches in relation to AI.

It should also be noted that:

- depending on the nature of the AI solution in question, existing laws in areas such as data protection and anti-discrimination may apply to the operation of particular AI-based solutions or software products;
- in the field of connected and autonomous vehicles, future development of AI-based systems is in part regulated by the Autonomous and Electric Vehicles Act 2018; and
- the Artificial Intelligence (Regulation) Bill is currently going through the House of Commons (having recently passed its third reading in the House of Lords), which aims to establish the "AI Authority", a body designed to address AI regulation in the UK. This may include ensuring regulators are taking account of AI and to ensure alignment in approach.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

Under English law, there is no single property right that applies to data *per se*. Depending on its nature and/or source, the use and/or disclosure of certain data may be regulated by the law of confidential information. In addition, certain data may qualify for copyright protection or, where the data has been aggregated with other data and compiled into a database, separate copyright or the EU database right may exist in the database.

Where these IP rights exist in the relevant training data, an appropriate IP or know-how licence can be granted. However, the English courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore be licensed on a purely contractual basis under English law.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Under English law, algorithms are potentially protectable by copyright as original literary works. Where an algorithm is written by a human, the author of that work is the person who creates it (Section 9(1) Copyright, Designs and Patents Act 1988 (CDPA)). This is taken to be the person responsible for the protectable elements of the work, being those elements that make the work "original" (i.e., those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using machine learning without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e., there is no human author such that the work qualifies as "computer generated" under Section 178 CDPA. In these circumstances, Section 9(3) CDPA deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under Section 12(7), the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created. While the test set out in Section 9(3) CDPA determines the identity of the author of a computer-generated work, it is not currently clear as a matter of English law whether such work will actually qualify as copyright work. Under Section 1(1) CDPA, copyright only subsists in original literary works, which requires an intellectual creation by the author that reflects an expression of their personality. It is questionable whether an algorithm developed by machine learning without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation. As a result, such an algorithm may not qualify for copyright protection under English law. An alternative view is that Section 9(3) CDPA in fact creates its own *sui generis* right for computer-generated works which is not subject to the usual requirement for originality. These issues have not thus far been addressed by the English courts and claims to copyright (or an absence of rights) in algorithms developed by machine learning without human intervention must therefore be treated with caution.

In light of this uncertainty and the growing use of AI solutions, the UK government has recognised that the current approach to computer-generated works is unclear and that there is a case for re-considering it. Accordingly, a consultation on whether to reform the UK's approach to computer generated works was issued in October 2021. The UKIPO sought views on whether to maintain the existing protection for such works under section 9(3) CDPA, abolish section 9(3) or to replace it with a more limited form of protection. The Government's response was published in July 2022. The UKIPO opted to keep the *status quo*, identifying that AI is still in its early stages and that changes could have unintended consequences. Instead, it committed to keeping the law under review and amending, replacing or removing protection in future if the evidence supports it.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there are not.

Financial regulation has developed around certain activities that relate to the issuance, exchange or custody of crypto-assets but this does not cover the specific use of blockchain-based solutions. The EU has introduced a Regulation on Markets in Crypto-assets (**MiCA**), aiming at creating an EU framework for crypto-assets falling outside the scope of existing EU financial regulation, as well as e-money tokens. MiCA considers within its scope:

a) e-Money tokens that are intended primarily as a means of payment aimed at stabilising their value by referring only to a single fiat currency:
b) Asset-Referenced tokens, intended to maintain by referencing several currencies that are legal tender, one or several commodities, one or several crypto-assets, or a basket of such assets. They could also be used as a means of payment;
c) Utility tokens, intended to provide digital access to a good or service available on DLT, are included in the scope of MiCA only if fungible and transferable.

Non-Fungible Tokens – whose value is attributable to each crypto-asset's unique characteristics – are excluded from the scope of MiCA.

The proposal for Regulation on Markets in Crypto-assets sets out: (1) rules for issuers and offerors of crypto-assets; and (2) rules for entities that provide services related to crypto-assets (exchanges, trading platforms, custodial wallet providers, etc.).

The UK is continuing to carry out a wider review on the approach to crypto-asset regulation and is currently focusing predominantly on establishing a UK regulatory environment for stable tokens (also known as "stablecoins"). The UK government has identified stable tokens as the area of the crypto-asset ecosystem which requires immediate regulatory attention due to their rapid adoption and use in retail and wholesale transactions. Currently, activities in the UK relating to the issuance, exchange and custody of crypto-assets requires registration under the UK money laundering regime.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

There are many blockchain-based technologies that are being adopted – in a live environment – in a variety of sectors, including the financial services, life sciences and media sectors.

Financial services

In the financial services sector, use cases are developing around tokenisation of financial assets using blockchain-based solutions. Tokenisation involves minting a crypto-asset to a blockchain ledger which represents a right or interest in an underlying physical or digital asset. For example, a token could represent rights in a financial instrument such as equity or debt securities. It could also include illiquid assets such as real estate. This could allow more people to access assets and to fractionalise more expensive assets that would otherwise be unaffordable. Real time settlement, access to illiquid assets and lower transaction costs could be drivers to adopting blockchain technology in financial markets.

Blockchain technology is also being utilised to help underpin settlement of payments in real-time. For example, payment scheme operators are considering how they can utilise distributed ledger technology to provide real time settlement of funds held in accounts with central banks.

Payment service providers are also considering ways they can offer crypto-conversion services to help fund remittances. Also, acquirers are considering ways they can offer additional payment methods for merchants in respect of crypto, such as in relation to bitcoin or other crypto-assets. There are a number of variations to the payments model which could include converting crypto-assets of payers or buyers into fiat on the issuer side, or alternatively, acquirers receiving crypto from buyers or their payment service providers and converting this into fiat for the merchant.

Life sciences

In the life sciences sector, electronic health records could be securely operated on a private blockchain network, protecting patient data and privacy while allowing doctors to access their patients' medical histories and empowering researchers to use shared data to further scientific research. Blockchain-based technologies enable permission layers to be built into the system. So, while patients are unable to change or delete medical information inputted by their doctors, they can control access to their profiles by granting full or partial visibility to different stakeholders.

Media

In the media sector, non-fungible tokens (NFTs) have been created or minted on blockchain networks and then bought and sold on NFT marketplaces that are integrated with the blockchain network: end users purchase an NFT on the marketplace and then the purchase history is tracked on the associated blockchain database providing an immutable proof of ownership. Its advocates claim that NFTs are the next-generation in digital collectibles (the electronic version of the Panini trading cards that have been widely traded in school playgrounds since the 1970s).

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Private blockchain contracting

Organisations looking to exploit blockchain-based technologies are often attracted to private blockchain networks (as opposed to public blockchain networks) because of the greater certainty as to the rules governing how the blockchain network operates and the opportunity to build in protection through contracting. Typically, an organisation will use proprietary software owned by a blockchain developer to set up a private blockchain network. In such circumstances, the organisation can engage the blockchain developer to run the blockchain network (including all the nodes) on its behalf as its subcontractor on the basis the blockchain network is made available by the organisation to its customers (let us call the organisation running the blockchain network the "**trusted intermediary**" and its customers the "**participants**"). In such circumstances, the key contracts governing the use of a private blockchain network would typically comprise:

- **a blockchain developer contract**, which is between the blockchain developer and the trusted intermediary operating the blockchain network. The trusted intermediary will license the right to use the blockchain developer's software and will engage the blockchain developer to provide it with ancillary services related to the launch, operation, support and development of the network, as the trusted intermediary's subcontractor;
- **a participation contract or charter**, which is the multi-lateral contract between the trusted intermediary and all the participants that want to gain access to the blockchain network. This contract governs the "rules" of the network. In this agreement, the trusted intermediary will include obligations on participants relating to acceptable use of the network (e.g. not uploading infringing material); and/or
- **a blockchain services contract**, which is a bi-lateral contract between the trusted intermediary and each participant governing the provision of access to any technology by the participant so it can access the blockchain network. In addition to IP licensing, this contract will deal with issues such as availability of the network and liability.

Key legal and practical issues that come up include liability (what happens if data is lost or corrupted), security (what security measures does the trusted intermediary have in place to ensure the integrity of the network), data protection (relevant if personal data is being processed on the blockchain), service levels (uptime of the network) and intellectual property (IP) (who owns the IP in any bespoke developments made by the blockchain developer). In addition, it is important that any commitments the trusted intermediary provides to a participant (for example, under the blockchain services contract) are, where applicable, flowed down to the blockchain developer under the blockchain developer contract.

IP in the blockchain – who owns it?

The blockchain network will comprise two key elements: the back-end blockchain software that determines how data is recorded on the blockchain database; and the user-facing app. The back-end blockchain software will often be pre-existing software that is utilised by the blockchain developer to service multiple clients. In contrast, the user-facing app may be bespoke software created by the blockchain developer for the trusted intermediary to solve its particular use case.

The user-facing app is what each participant accesses and will interoperate with the back-end blockchain software via an application programming interface (or API). One of the key IP battlegrounds between the blockchain developer and trusted intermediary is who owns the IP in the user-facing app; this is most likely to be decided by the needs and bargaining positions of the parties.

Irrespective of ownership, the user-facing app should, where possible, be developed in such a way that it is able to interoperate with other blockchain solutions. Otherwise, the trusted intermediary will be "locked-in" to the blockchain developer's solution.

Personal data on the blockchain?

The EU/UK GDPR defines 'personal data' as any information that relates to an identified or identifiable person. However, this

still includes "pseudonymous data" which is where individuals are not identifiable from the dataset itself but can be identified by referring to other information separately. On the other hand, truly anonymous data (i.e. where individuals are not identifiable and cannot be re-identified by any means reasonably likely to be used so the risk of reidentification is sufficiently remote) is not personal data and therefore not subject to data protection laws.

There is considerable debate as to whether data on the blockchain that has been encrypted or hashed still qualifies as personal data (e.g. the public key and the transaction data that i published). For example, see the European Parliament's study, '*Blockchain and the General Data Protection Regulation, Can distributed Ledgers be squared with European Data Protection Law*' which suggests a case-by-case analysis and there are certainly circumstances where the data will likely be considered as personal data even where it has been encrypted or hashed so this will need careful consideration.

The UK Information Commissioner's Office separately notes that "*the risk of re-identification* [of individuals] *grows with the volume of data stored on the blockchain. As points of data are progressively added through additional transactions, and as DeFi payments transition to paying for real-world goods and services, an increasingly detailed view of the wallet holder can be constructed, e.g. of their personal preferences, behaviours and attitudes.*"

Are there legal challenges with blockchain?

One of the key challenges is that regulation is playing catch up with the cutting-edge technical solutions already being used. For example, the EU/UK GDPR, which sets out the main EEA and UK legal framework for processing personal data, was not drafted with blockchain technologies in mind. As a result, there are a number of key principles of the EU/UK GDPR that can be hard to reconcile, in practice, with the fundamental features of any blockchain. For instance, it can be difficult to:

- identify the data controller(s) in a blockchain network and thereby allocate the appropriate responsibilities/liabilities under the EU/UK GDPR, particularly in public permissionless blockchains where there are many different parties involved;
- identify the relevant jurisdiction and address any data transfer restrictions as it is often uncertain where the personal data is processed at any time; and
- respect individuals' rights under the EU/UK GDPR – whilst some rights such as the right of access or right to data portability can be exercised easily, the rights of erasure and rectification can be particularly problematic on public permissionless blockchains given their immutable nature. One solution is not to store any personal data on the blockchain, with personal data being stored "off chain" instead where the data can be freely amended or deleted.

Another option, proposed by the French Data Protection Authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), is to use encryption technologies to make the underlying personal data practically inaccessible upon deletion of the encryption key. That deletion can then be done systematically (as part of a retention limitation policy), or in response to a "right to be forgotten" request; or to "delete" incorrect data and "replace" it with a corrected version, after a GDPR correction request. However, it likely requires a single entity to hold (and decide to delete) the keys – potentially undermining a key reason for using a distributed blockchain in the first place.

The practical implications of such solutions – and the reliance, often, on a distributed body of blockchain participants to ensure EU/UK GDPR compliance and accountability – make ensuring (and being able to demonstrate) EU/UK GDPR compliance a challenge, both on a day-to-day basis, and in drafting the multi-partite agreements and policy documents that the EU/UK GDPR requires.

Acknowledgments

The authors would like to thank the following colleagues in Bird & Bird's London office for their contributions to this chapter: Tom Ward, Zoe Feller, Tom Hepplewhite, Toby Bond, Caroline Brown, Alison Dixon, Olivia Baxendale, Rory Coutts, Matthew Buckwell, Gavin Punia, Neely Middleton and Jonathan Emmanuel.

Endnote

1 Cabinet Office, Guidance: transitional and saving arrangements < https://www.gov.uk/government/publications/procurement-act-2023-guidance-documents/guidance-transitional-and-saving-arrangements-html > accessed 21 May 2024.

Mark Leach is a partner in Bird & Bird's London office and co-head of the firm's International Outsourcing and Technology Transactions practice groups. He specialises in complex technology transactions, outsourcings and large-scale transformational projects. He also advises regularly on systems integration contracts, cloud computing arrangements and software licensing and development deals.
Mark's clients include financial institutions and major corporates (particularly in the aerospace, defence and technology sectors), as well as a number of technology vendors.
Mark speaks regularly at industry events on outsourcing and commercial technology issues and has been regularly named as a '*Leading Individual*' in outsourcing in the successive editions of the *Chambers Guide to the UK Legal Profession* and has been recognised in *The Legal 500's Hall Of Fame* for IT and Telecoms work.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: mark.leach@twobirds.com
LinkedIn: www.linkedin.com/in/mark-leach-bb83b94a

Amelia Morris is a senior associate in Bird & Bird's Tech Transactions practice group and advises clients on a range of complex and strategic technology contracts. Since joining Bird & Bird in 2016, Amelia has worked on a wide range of technology and commercial projects, acting for both suppliers and customers, with a particular focus on strategic and transformational projects for clients in the tech, defence & security, and retail sectors. Amelia regularly advises clients in relation to agreements for software licensing, development and support services, as well as SaaS and cloud-based technologies.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: amelia.morris@twobirds.com
LinkedIn: www.linkedin.com/in/amelia-morris-39770956

Bird & Bird has more than 1,600 lawyers in 31 offices across Europe, the Middle East, Asia-Pacific and North America and clients based in 118 countries worldwide. We specialise in combining leading expertise across a full range of legal services and aim to deliver tailored local advice and seamless cross-border services.
Our technology sourcing practice is widely recognised as having a leading reputation in the field and enjoys top tier rankings in the *Chambers* and *The Legal 500* Guides to the UK legal profession. We advise on the full range of technology transactions, including complex outsourcings and managed services deals, system implementation projects, telecoms infrastructure and regulatory matters, strategic alliances and collaboration agreements, cloud computing deals and contracts for the deployment of AI and blockchain-based solutions.

www.twobirds.com

Bird & Bird

USA


Sean Christy


Chuck Hollis


Derek Johnston

Norton Rose Fulbright US LLP

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No; however, there are federal and state laws and regulations that may apply to the subject matter or other aspects of the transaction (e.g., data privacy) or industry of the contracting party (e.g., financial services, healthcare).

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

The DoD, GSA, and NASA jointly issue the Federal Acquisition Regulation ("FAR") for use by executive agencies in acquiring goods and services, and part 39 of FAR describes the terms of acquisition of information technology. In addition, the head of an agency may issue or authorise acquisitions regulations that supplement or implement the FAR and incorporate additional policies, procedures, terms and provisions that govern the contracting process with that agency. The procurement of goods and services by state and local governmental bodies is governed by state procurement laws of the state in question, and for some municipalities, by the applicable municipal code.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, but parties to such a contract will generally agree to contract terms that range from one year to several years, depending on the nature, scope, and complexity of the arrangement.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, the length of any termination notice period and the termination provisions themselves are instead negotiated by the parties on a case-by-case basis in view of the nature, complexity and criticality of the technology-related services and the initial investments incurred by the parties. However, in the consumer context, there are various federal and state laws that may require the supplier to follow certain processes and provide the consumer certain notices before terminating, and the common law of some states may impose a presumptive reasonable renewal term on contracts that the parties continue performing beyond expiration.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

The common law of most states imposes an implied duty of good faith and fair dealing on the parties to a contract. It is not uncommon for a contract to include a more definitive, express covenant for the parties to cooperate and deal with each other reasonably and in good faith to effectuate the purposes of the contract.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Customers are entitled to recover proven, direct damages for breach of contract. The definition of direct damages varies from state to state, with some states having a more well-developed body of common law lending more predictability.

In addition, equitable remedies (e.g., injunctive relief) may be available where monetary damages are not sufficient to make the non-defaulting party whole and other conditions are satisfied, and additional common law remedies (e.g., restitution, rescission, specific performance) may be available.

Technology sourcing contracts frequently include:

- A definition of what constitutes recoverable "direct damages" to lend predictability to the types of damages

that are recoverable, including the cost of cover and other foreseeable damages that would result from a breach.*

- A negotiated monetary damages cap on amounts recoverable for breach of contract (typically ranging from 12 to 24 months' fees with outliers in exceptional circumstances).
- Disclaimers of indirect, special, consequential and punitive damages and often of lost profits, reputational harm, diminution in value and similar damages.
- Exclusions from both the monetary damages caps and the disclaimers of indirect damages, often with a separate, higher cap (typically ranging from 24 to 48 months' fees with outliers in exceptional circumstances) for certain types of damages and indemnities (e.g., for data breaches) and with other damages and indemnities not being subject to any limit (e.g., gross negligence and wilful misconduct).

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

These contracts often include a variety of additional remedies and protections depending on the scope and deployment model of the solutions and services, with more customer leverage mechanisms and remedies in outsourcing agreements and much fewer in cloud agreements. Remedies may include:

- The ability to withhold a portion of the fees in a scope dispute.*
- The right to step-in and correct performance failures and to recover the incremental costs of stepping in.*
- The right to set off amounts in dispute* and other amounts owed to a customer against the charges (sometimes subject to an escrow requirement above a certain threshold or, less commonly, an outright cap).
- Service levels and other performance metrics and remedies.
- A defined acceptance process, with no cost repair, cover, and termination remedies for non-conforming transition and other one-time deliverables.
- Milestone payments and sometimes credits to incentivise timely and proper completion of transition services/deliverables.
- A prohibition against intentional breach (abandonment) by the supplier and injunctive relief and enhanced recovery for same.*
- The termination rights described at question 2.7.
- An express obligation for the parties to continue performing during disputes.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

The contract typically provides when a party may terminate. These termination rights will, when properly invoked, enable a party to terminate the contract without giving rise to a claim for unspecified damages from the terminated party, but each party may have claims for damages independent of the termination.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties can, and typically do. Examples include: (1) a customer termination right for convenience (possibly subject to payment of an express termination charge);* (2) a right to terminate for the supplier's (and in rarer cases, the customer's) insolvency; (3) a customer termination right for repeated or significant service level failures; (4) a customer termination right for persistent, uncured breaches;* (5) a customer termination right for a supplier's breach of the agreement's confidentiality or data security requirements; (6) a customer termination right for other material breaches that remain uncured for more than a period of time (e.g., 30 days); (7) for certain customers in regulated industries, a customer termination right where required to comply with applicable law or where mandated by a regulator; and (8) limiting supplier termination rights to customer payment defaults.* A contract may also include certain rights, exercisable by the customer upon termination or expiration of the arrangement, which almost always include a post-expiration/termination wind down period during which the customer can continue to receive the services and request other cooperation to repatriate or transition services to a replacement provider.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

The interpretation and enforcement of clauses that seek to limit a party's liability are generally governed by state, not federal, law. As a general rule, if the parties to a contract are both sophisticated business entities dealing at arm's length, they are free under the laws of most states to negotiate both limits on liability and exclusions from those limitations in their contracts. However, some states view liability limitations in contracts less favourably than others, and the parties should take care in their choice of governing law.

Certain liabilities may not be limited under the common law of many states, typically including the liability of a party arising from its fraud, wilful misconduct and gross negligence and, in some states, the wilful injury to person or property or violations of law (regardless of whether the violations are intentional or not).

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Generally, yes, if the proposed cap on liability: (i) is reasonable in relation to the fees for the services; (ii) generally relates to economic damages arising out of the negligent acts or default performance of either party; and (iii) would not otherwise violate public policy.

In the ordinary course, the amount of the liability cap, the inclusion of super caps or enhanced caps, the application of the liability cap, and any exclusions from the liability cap are among the most heavily negotiated matters in the contract. See also question 2.4 above.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

Not as a matter of state or federal law, but there are special considerations contextually. Cloud contracts and software license and support contracts are generally less customer-friendly inasmuch as they include fewer customer leverage points

(those marked with an "*" above being customarily excluded). By extension, the same limitations apply to the licence or cloud deployment of AI, machine learning and blockchain solutions. However, given the evolving regulatory landscape in the U.S. and public attention concerning some of the risks attendant to AI and machine learning (e.g., discrimination and bias), the procurement contract may include more detailed representations, warranties, termination rights, data use/limitations, audit/explainability requirements, indemnities and exclusions from the limitations of liability to afford the customer remedies and to allocate risk for issues that might cause compliance issues for, or give rise to claims against or by, either party.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

Most outsourcing contracts resort first to informal dispute resolution between the parties and sometimes with escalation to management before resorting to more formal dispute resolution – usually litigation or binding arbitration, although sometimes mediation is a precursor to litigation. Software licensing, cloud computing, and other technology contracts less often include informal dispute resolution, as those contracts are usually less robust as a general matter. In all cases, the contracts will often specify the federal and/or state courts for the resolution of litigated disputes, taking into account facts relevant to personal jurisdiction requirements under federal and state law. U.S. customers with foreign-domiciled suppliers often prefer arbitration, with the preferred arbitral rules and tribunal varying based upon where the parties are domiciled and other factors. If arbitration is chosen, the parties will usually reserve certain matters for litigation (e.g., equitable relief, confidentiality, intellectual property).

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

The intellectual property rights (IP) of each party are typically protected by the terms of the contract and statutory protections for certain IP (e.g., patents, copyrights, trademarks).

The licences and allocation of IP ownership under a contract vary based on the type and scope of services. Typically, the customer and supplier retain ownership of IP that they bring to the arrangement and any improvements or derivative works thereof. For new developments, the scope of the arrangement will dictate the allocation of ownership and any licences to such IP.

Each party will license to the other party its IP that is necessary to perform or receive the services. In certain instances, customers will receive perpetual licenses to the supplier's IP, which often relate to IP that is necessary for the customer to continue operations post-termination/expiration (less common in the cloud context) or to IP that is embedded within, or is otherwise necessary for the use and maintenance of, the customer's systems and other deliverables.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

Any assignment of IP rights should be in writing and executed by the assignor. The assignment may also require consents from third parties, may be governed by an agreement with such third parties, and may be subject to certain fees or other charges. Trademarks must be assigned with their goodwill in order to be valid. The transfer of patents and trademarks should be recorded in the U.S. Patent and Trademark Office, and copyrights should be recorded in the U.S. Copyright Office.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Generally, know-how, trade secrets and other business critical confidential information are protected by statute and by common law. In particular, 48 states have adopted some form of the Uniform Trade Secret Act protecting trade secrets at the state level. In the other two states, trade secrets are protected by common law. Trade secrets also may be protected under certain federal laws. In most instances, the contract includes language protecting know-how, trade secrets and other confidential information.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

There is no uniform federal law governing the processing of personal data in the U.S. The processing of personal data is instead governed by a patchwork of federal and state laws. At the federal level, the Gramm-Leach-Bliley Act and a patchwork of regulatory guidance by the federal financial institution regulators (applicable to financial services), HIPAA and the HITECH Act (applicable to protected health information), and the Family Educational Rights and Privacy Act (applicable to educational institutions and their vendors), along with their implementing regulations, are the most frequently implicated. Data security and protection requirements at the state level vary significantly, with breach notification laws in all 50 states and some of the more protective privacy regimes existing or coming online under the California Consumer Privacy Act/California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, Connecticut Data Privacy Act, Iowa Consumer Data Protection Act, the New York SHIELD Act, the NYDFS Cybersecurity Regulations and the Washington My Health MY Data Act. Finally, U.S. customers with international operations remain subject to international privacy laws like GDPR.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Generally, there are no geographic transfer restrictions applicable to personal data in the U.S. However, in February 2024, President Biden signed an Executive Order aimed at preventing access to America's bulk sensitive personal data

and United States Government-related data by countries of concern when such access would pose an unacceptable risk to the national security of the United States.

5.3 Are there any legal and/or regulatory requirements concerning information security?

In addition to the more generally applicable requirements referenced in question 5.1, there are industry-specific requirements related to information security. For example, federal guidelines apply to critical infrastructure operators and certain industries (e.g., financial institutions, telecommunications, electrical utilities, transportation, and the public sector) that are subject to federal and state regulations that include information security requirements.

In November 2023, the NYDFS finalised amendments to its Cybersecurity Regulations which enhance the information security requirements imposed on financial institutions operating in New York state. Even for those companies that are not regulated by the NYDFS, in the past, other state and federal regulators have adopted requirements similar to those of the NYDFS. Companies should follow the status of, and any revisions to, these proposed new Cybersecurity Regulations as a potential bellwether of requirements to come under other regulatory regimes.

In addition, the National Institute of Standards and Technology ("NIST") released a new 2.0 Cybersecurity Framework on February 26, 2024, which provides updated guidelines for assessing cybersecurity maturity and managing cybersecurity risks. This NIST Cybersecurity Framework is followed by many companies.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

No, in the absence of a collective bargaining agreement or other contractual arrangement, employees in the U.S. are never transferred to a supplier solely by operation of law pursuant to a commercial contract. Employees are generally considered "at will" employees and, therefore, these employees may be terminated at any time for any lawful reason.

6.2 What employee information should the parties provide to each other?

If the customer intends to transfer employees to the supplier, the supplier will need information relevant to making an offer of employment to those employees, including information relating to salary, benefits, years of service and skill sets.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

Generally, yes. Employees in the U.S. are considered "at will" employees and may be terminated by an employer for any lawful reason, in the absence of a collective bargaining agreement or other employment contract prohibiting such a termination. Further, the Worker Adjustment and Retraining Notification Act (the "WARN Act") and similar state laws may require certain employers to notify their employees of mass layoffs, widescale hour reductions or site closures. Employment contracts with certain employees, a prior course of conduct or other existing company policies might also obligate the employer to notify its employees or even to provide severance or other bonuses to employees whose employment is being terminated as a result of a new outsourcing or other services contract.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, as noted above, under the laws of the United States, the parties are generally free to negotiate and establish the new employment terms for transitioning employees, subject to any existing collective bargaining arrangements, employee contracts, company policies and/or prior course of conduct.

6.5 Are there any pensions considerations?

Yes, companies that maintain pension benefits for their employees cannot discharge or avoid these benefit liabilities by simply outsourcing the affected services and transferring the in-scope employees. Liability for any existing or future pension benefits is governed and determined by federal law.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

Current U.S. law generally accommodates the offshoring of work by U.S. corporations, subject to certain narrow exceptions (e.g., OFAC's Sanctions Programs and SDN List). The purchase of services by a federal or state entity is highly regulated and there may be restrictions on the offshoring of certain services. Multi-jurisdictional contracts may also trigger other laws that limit or apply conditions to transfers (e.g., ARD/TUPE). See also question 6.3 above.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Not generally, but certain federal and state laws and regulations may apply contextually. For example, (i) the regulations mentioned in section 5 above may apply where personal data is in scope, (ii) third-party risk guidance (from the FRB, OCC, FDIC, FINRA, and the NYDFS and other regulatory agencies) may apply in the financial services industry, and (iii) FERPA will govern the scope of permitted outsourcing in higher education. The type of services also may implicate additional laws. For example, the FDCPA, TCPA and other consumer protection laws (e.g., Do Not Call Registry and the CAN-SPAM Act) may apply to outbound contact centre services.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

While there are several common contract structures, the most widely utilised contract structure is a Master Services Agreement accompanied by one or more Statements of Work.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Service levels are commonly included in outsourcing contracts. Each service level is defined in terms of the process or service measured, a unit of quality, and a period of time for measurement. Service levels are typically measured on a monthly basis, but may be measured over longer periods of time (e.g., quarterly, annually), or as one-time events.

Service level metrics are set based on the customer's requirements, the customer's historical data or sometimes, via baselining. Measurement, monitoring and reporting tools should be specified for each service level. Service level accountability and/or credits may be delayed for a stabilisation period in certain instances.

There are often two or more classes of service levels, and each service level may have a single or multiple targets depending upon the complexity of the methodology. More critical service levels bear credits if the supplier fails to meet the applicable target. Other service levels may be tracked and measured, but not result in credits. Customers usually have the periodic right to reclassify service levels as credit-bearing or not and to reconfigure the allocation of credits across the service levels. In some arrangements, there are other general reporting metrics that are tracked, measured, and reported, but are not eligible to be credit-bearing.

Service level credits are reductions of the fees paid by the customer and are not characterised as penalties, which are generally unenforceable, or as liquidated or exclusive remedies. Rather, service level credits are most often treated as a credit against the customer's damages.

Service level credits are subject to a defined amount at risk (cap). Generally, that amount is defined as a percentage of monthly or annual fees, ranging from 10% to 15%, with outliers in exceptional circumstances. In more complicated transactions, the customer may have the right to over allocate the amount at risk, with the overallocation typically ranging from 150% to 275% of the amount at risk, but aggregate credits are always subject to the amount at risk. In some instances where overperformance has a direct benefit to the customer, the supplier may "earn-back" the service level credit for continued performance at or above the target.

Service levels in the cloud services context (including in the AI/ML context) are usually much more focused, and the methodology much more straightforward, with the most common framework being an availability service level with defined credits for certain levels of availability below the target availability level and incident response service levels, usually without credits. Customers sometimes have success in negotiating credits for incident response service levels and sometimes, for incident resolution service levels as well. Unlike the outsourced services context, service level credits in cloud services contracts are often exclusive financial remedies, but do not limit the customer's right to terminate the agreement for repeated service level failures, breach of warranty or otherwise.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Charging methodologies vary greatly. The following are a few examples:

- A methodology based on the volume of resources. This method may include a fixed charge with a variable fee or credit based on volume, or may be purely variable and is common in IT outsourcing transactions.
- A fee based on the number of FTE resources used to perform the services. These charges are often based on FTE hourly, daily or monthly rates. This approach is used in business process outsourcing ("BPO") and application development outsourcings where there are productivity commitments to help manage the resources. Whether or not fee increases are applied with the addition of FTEs varies, with some contracts limiting fee adjustments to adjustments in services volumes and precluding additional charges where more FTEs are required to achieve the originally anticipated baselines.
- A fee based on the supplier's costs, commonly referred to as a cost-plus model. This method requires the supplier to disclose its costs, which makes this method rare.
- A fee based on the number of users or transactions. As the number of users or transactions fluctuates, the fees fluctuate. This method is more common in BPO arrangements.

Certain distinct parts of outsourcing arrangements, such as the transition, may be priced on a fixed-fee or FTE basis, which may be tied to the completion of certain milestones.

Increasingly, in AI, automation and technology-driven arrangements, and in digital outsourcing, the technology components that drive AI, automation and the related systems integration, development and support may be priced separately. In addition, there are often measures in the contract that formalise the productivity commitments and resource reductions/savings so that the supplier bears some or all of the productivity risk.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

These transfers are much less common in today's market, with the prevailing trend being to extend usage of the subject of the third-party contracts without actually transferring the contract. However, if relevant, the transfer should be in writing, addressed in the contract, and noticed or documented as required under the applicable third-party contract. These transfers may require consents from third parties, may be governed by an agreement with such third parties, and may be subject to certain charges.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Services may be subject to state and local sales and use taxes, typically depending on the states from which the services are provided and received. If assets are transferred (e.g., software, equipment, facilities, real estate), the transfer may be subject to federal, state and/or local taxes. Outsourcing transactions that include a cloud- or other internet-based service delivery component may also trigger taxation of services provided over the internet, with taxation occurring at various points of receipt of the services and apportionment required based upon the extent of use from state to state. The contract typically allocates financial and remittance responsibility for taxes in connection with the arrangement. The customer is often responsible for applicable sales and use taxes, with remittance by the supplier, except in unusual circumstances. Each party retains responsibility for the taxes on their income and on their assets.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

Issues vary depending on the parties, available leverage and the operational purpose of the software. The following are a handful of key issues that a customer/licensee should consider:

- Authorised Users – Who are the appropriate users of, or are otherwise permitted to access, the software (e.g., affiliates of the licensee, end users, third-party hosting and/or service providers, customers, bots and automation tools, etc.)?
- Scope of Use – What are the permitted uses of the software by the licensee (e.g., are there business limitations, internal use limitation, quantity of transactions, revenue thresholds, etc.)?
- Implementation – Who is responsible for the implementation of the software? If the licensor will configure and implement the software, appropriate professional services need to be defined with additional relevant governing contract terms (e.g., acceptance and warranty provisions related to the professional services).
- Warranties/Warranty Remedies – What is the scope and duration of the software warranty, and what are the performance requirements measured against (e.g., documentation)? Also, what specific remedies are available to the licensee if the software fails to meet the warranty.
- Infringement – What is the licensor's responsibility, and what are the licensee's remedies if there is claim of infringement (e.g., indemnification, repair and replace, third-party licence, refund)?
- Limitation of Liability – What is the extent of the liability of the licensor if the licensor fails to implement the software, the software fails to perform, or there are infringement claims related to the software?

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

Issues vary depending on the parties, available leverage and the operational purpose of the software. The following are a handful of key issues that a customer/licensee should consider:

- Scope of Support – How will the licensor provide the support and what access do they need to the licensee's environment? Are there any service level commitments regarding response and resolution times?
- Data Access – Will the supplier need access to the licensee's data (e.g., personal/regulated data)? Are there ways to limit access or otherwise obfuscate or protect this data? If personal data access is anticipated, appropriate data processing terms must be applied to cover processing requirements under applicable laws and regulations.
- New Versions/Releases – What are the licensor's commitments regarding the provision of new versions and releases of the software? What obligation does the customer have to remain current and in what timeframe? Will the deployment of new versions or releases require additional implementation services, and if so, are those services in scope, separately priced or to be provided by the customer or a customer third party?
- Pricing – What are the licensor's commitments regarding future pricing? What is the maintenance and support term, including renewal options (consider the ROI period for the software licence)?
- Out of Support Options – What happens if the licensor no longer offers support? Is support available from a third-party supplier? Can the customer terminate support? If so, can the customer continue usage without support? Is there a right to reinstate support, and what is the cost to reinstate?

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Software escrow arrangements are more often used with niche providers and start-ups whose ongoing support capabilities or general viability are uncertain and for software that is particularly critical to operations. In today's market, escrow options exist for both premises-based licences and cloud subscriptions.

The enforceability of a software escrow agreement may be impacted by U.S. bankruptcy laws. However, there are provisions in the bankruptcy code that can be leveraged to greatly enhance the likelihood of enforcement and permit the licensee to continue using the software and access the escrowed code in the event of licensor bankruptcy. The provisions in the escrow arrangement should be specifically drafted to take advantage of the bankruptcy provisions (including a present grant of a licence to the escrow materials).

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No; however, as noted herein, there are federal and state laws and regulations that impact and relate to the specific uses of cloud computing services in certain industries or applications (e.g., financial services, healthcare, the public sector and higher education).

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

Adoption of cloud computing is nearly ubiquitous in the U.S., with all entities from small to large either directly deploying or indirectly utilising technology that is deployed on some form of cloud deployment model.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The cloud deployment model has created a fairly standardised (provider-friendly) contracting framework in the U.S. The issues that are most negotiated are outlined in question 8.1 above with the following nuances being more customary:

- Warranties/Warranty Remedies – A warranty that the service will perform materially or substantially in accordance with the specifications or documentation, a warranty that changes to the cloud services and governing policies and terms will not materially and adversely affect

the security, functionality or performance of the cloud services and a right for the customer to terminate the cloud services and receive a refund of prepaid fees in the event of a breach of the foregoing warranties that remains uncured (usually for 30 days or more).

- Data Privacy/Security – A commitment that the cloud provider will adhere to defined security standards and data processing terms and allocation of risk (exclusions from the limitations of liability and sometimes additional indemnities) for any breach of those standards or terms that causes or enables a compromise of personal data. Usually, liability in this context is limited to a separate, higher cap with types of damages being specified/limited to notification costs, fines, penalties and interest, and other remedial measures that companies customarily undertake to remediate the incident and restore their reputation in the event of a data breach.
- Disengagement/Data Migration – Whether, upon expiration or termination, the customer will simply have the right to download its data or, alternatively, to continue using the services for some period. The latter is the more common approach for operationally critical platforms. The format in which the customer data will be made available upon exit is often negotiated, with customers pushing for data to be made available in a format that is useable with commercially available software.
- Growth and Renewal Pricing – Whether the customer may extend the original unit pricing to additional quantities of cloud services, whether pricing for optional cloud services is specified and protected for the terms, and whether the pricing for any renewal term is subject to adjustment, and if so, any applicable cap on adjustments. With regard to the latter, inflationary adjustment caps have been increasing with inflation, with some customers still achieving renewal term caps as low as the lesser of CPI and 3%, but others seeing caps at 5% or higher given current inflationary conditions.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

While there are no comprehensive federal data privacy and AI laws or regulations, there are federal laws and regulations that specifically address the procurement and use of AI-based solutions and technologies. However, most are applicable to Federal agencies and, to a lesser extent, private companies. On 30 October 2023, the White House issued Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Many of the federal agencies are implementing oversight and publishing guidance which will affect those companies over which they have regulatory authority. The Executive Order establishes a government-wide effort to guide responsible AI development and deployment, and directs over 50 federal entities to engage in more than 100 specific acts to implement the guidance.

In March 2024, the Office of Management and Budget (OMB) also issued guidance to federal agencies on the use of AI products and services and established new agency requirements and guidance for AI governance, innovation and risk management, including implementing minimum risk management practices for the use of AI that impacts the rights and safety of the public.

In April 2024, the U.S. General Services Administration (GSA) released the Generative AI and Specialized Computing Infrastructure Acquisition Resource Guide to support the federal acquisition community as it purchases generative AI solutions and related specialised computing infrastructure. This guide is part of the implementation of Executive Order 14110.

In May 2024, the US Department of Health and Human Services (HHS) Office of Civil Rights (OCR) issued a final rule addressing discrimination in health care. These rules implement new AI requirements applicable to the use of AI in "patient care decision support tools".

Each of these federal agency regulations, and others that follow, will continue to have some impact on the private sector.

In addition to the Executive Order and the implementation of its directives, probably the most developed and well-known area of the law that touches on AI is in the privacy realm, where various U.S. federal and state privacy laws that govern the collection, usage and protection of personal data. See section 5 above. Several states, local governments and municipalities have implemented sectoral and other use case-specific laws that will impact the use and implementation of AI-based solutions and technologies (see, e.g., NYC Local Law 144, which requires pre-deployment and annual bias audits for HR screening and decisioning tools).

As companies look to use and implement AI use cases, companies will need to assess and determine the legal and regulatory landscape, on a federal, state and local level, which may impact the manner in which these use cases are deployed. In addition, given the evolving legal and regulatory landscape, companies will need to monitor and react to any changes.

Finally, while not a US-specific law or regulation, the EU Parliament voted on 13 March 2024 to adopt the EU's AI Act, which will have a significant impact on US companies operating in the EU. With the US not having comprehensive AI regulations, multinational companies will need to consider the impact of the EU AI Act on their operations – much like they did when the GDPR was implemented in the EU.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

The data used to train machine learning-based systems may be subject to certain data privacy laws and regulations (e.g., HIPAA, CCPA, State data privacy laws) and/or require consents from the data subject. In addition, the data that is used to train the machine learning-based systems may be protected by contract and/or copyright laws. Accordingly, the ability to use (copy) copyrighted data to train a machine learning-based system without infringing the copyright of the underlying data is a relevant, fact-based question that must be considered. The use of copyrighted data may be permissible under "fair use" standards and on a First Amendment basis, but these theories are being challenged on many fronts based on copyright, unfair practice, the Lanham Act, the CCPA, the Digital Millennium Copyright Act, publicity and unfair competition theories – to name a few. No AI developer is immune from these claims with numerous lawsuits filed across the country against the major developers. At this point, where these cases will end up is unknown. However, certain content owners are taking advantage of this unknown and licensing their content to AI and large language model developers, but the Federal Trade Commission ("FTC") is taking a closer look at these arrangements.

A user of a machine learning-based system needs to identify each source of training data and the data that is processed by the AI/ML model and ensure that it has the appropriate rights to use such data for the intended purpose. Such rights may be obtained by licence and/or consent.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

More recently in the U.S., there has been some clarification regarding the allocation of ownership of algorithms which are improved or developed by machine learning techniques without the involvement of a human programmer.

In March 2023, the U.S. Copyright Office issued a statement of policy to clarify its practices for examining and registering works that contain material generated by the use of machine learning-based systems. In general, there must be some creative contribution from a human for the work to be copyrightable. The Copyright Office did note that a work generated by a machine learning-based system may be copyrightable if the work contains enough human authorship. In such cases, the copyright will only protect the human-authored aspects of the work, but not the machine learning-generated portions. Whether there is enough human authorship to warrant copyright protection will have to be determined on a case-by-case basis. The Copyright Office has issued registration decisions on a number of requests.

Similar to the issue of copyright protection for materials improved or developed by machine learning techniques, in February 2024, the United States Patent & Trademark Office ("USPTO") issued inventorship guidance for inventions assisted by AI, which delivered on the USPTO's obligations under the Executive Order. The guidance is intended to strike: "[A] balance between awarding patent protection to promote human ingenuity and investment for AI-assisted inventions while not unnecessarily locking up innovation for future developments. The guidance does that by embracing the use of AI in innovation and focusing on the human contribution." This guidance is also consistent with the finding of the Federal Circuit (*Thaler v. Vidal,* 43 F.4th 1207 (Fed. Cir. 2022)), which held that an AI system may not be an inventor and is not an "individual" for purposes of patent protection.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, but several states have enacted laws that pertain specifically to the usage of blockchain, many of which enable the use of blockchain for corporate records (e.g., corporate ledgers), smart contracts, signatures and in legal proceedings and to permit the trade of corporate stocks on a blockchain, and several states have passed legislation to study or catalyse the usage of blockchain in public sector applications. Cryptocurrencies that leverage blockchain technology are subject to numerous federal and state laws and regulations, which are a function of the financial services nature of the currency and not the usage of blockchain technology itself.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain is most widely adopted in the financial services sector. However, cross-industry adoption for supply chain use cases is significant, and use cases in the healthcare sector and for supply chain management are prevalent. In addition, the use of non-fungible tokens ("NFTs") is becoming more mainstream with new and expanding use cases, including for automotive industry applications, electronic gaming, sports and entertainment, music albums, film, art, fashion and digital branding.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

In many respects, the issues are common to those outlined in section 8 for licensed solutions, those outlined in section 9 for cloud-based solutions, and those outlined in section 7 and this chapter generally for related development, systems integration and support services. However, there are some unique considerations for blockchain:

- Multi-Jurisdictional Issues – The distributed nature of many blockchain solutions require consideration of:
  - Jurisdiction-specific data privacy compliance obligations.
  - An effective means of dispute resolution where the participants may reside in different jurisdictions and an appropriate governing law that will yield a predictable outcome should disputes arise (see section 3).
- Exit and Data Return/Destruction – The distributed and immutable nature of blockchain technology itself requires careful consideration of a participant's ability to seek return or destruction of its data upon exiting the arrangement. If the user does not hold a copy of the ledger, then provisions must be negotiated for provision of data where required. If the blockchain is truly immutable, traditional return/destruction may have to be foregone in favour of encryption or other means of rendering the data inaccessible.
- Intellectual Property – Ownership of the blockchain technology itself and improvements to the technology, as well as allocation of ownership of the data on the blockchain should be dealt with contractually.
- Accountability/Liability – In a shared blockchain solution, the participants should contractually allocate responsibility for not only operation and support of the blockchain, but also for issues and liability that may arise in connection with usage of the blockchain (e.g., defects, data privacy/security, etc.).

Sean Christy is the Head of Technology Transactions, United States for Norton Rose Fulbright. He counsels public and privately-held companies around the world on technology, outsourcing and other strategic commercial transactions in the financial services, hospitality, healthcare, life sciences, consumer products, retail, energy and technology industries. His practice includes serving as both a business and legal adviser to his clients in the following areas: digital transformation (including as pertains to this Chapter, on the development, acquisition and deployment of AI); traditional and digital outsourcing; acquisition-driven technology and operations transactions and advice; technology and commercial disputes and workouts; and fully or portfolio outsourced commercial contract consulting and support. He provides guidance on strategic direction and negotiation strategy, analysing client operations, selecting suppliers, scope/pricing/quality, providing post-transaction support, counselling on post-transaction governance and disputes, audit defence and other key commercial issues his clients face throughout the lifecycle of their deals.

Norton Rose Fulbright US LLP

Tel: +1 404 443 2146
Email: sean.christy@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/sean-christy-8535564

Chuck Hollis is the Head of Artificial Intelligence, United States at Norton Rose Fulbright. He is a technology, outsourcing and strategic commercial transaction lawyer handling a range of technology and commercial arrangements both in the US and globally for a range of clients including those in the financial services, hospitality, energy, healthcare and consumer products/retail industries and sectors. Chuck provides not only transactional legal advice, but also negotiation business strategy, vendor selection and consultative advice. His technology, outsourcing and commercial transactions experience includes global support for cloud services, cloud operations, digital transformation initiatives, development and implementation of ERP, SaaS, XaaS, AI/ML and other technology and software platforms and solutions. Chuck's practice also includes support for the more traditional outsourcing arrangements (ITO, BPO, ADM), and provides post-transaction governance and dispute support, including realignments and workouts related to outsourcing and technology arrangements.

Norton Rose Fulbright US LLP

Tel: +1 404 443 2147
Email: chuck.hollis@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/chuck-hollis-855a5b9

Derek Johnston has over 25 years of experience representing public and privately-held companies in complex business process outsourcing (BPO) and information technology outsourcing (ITO) transactions, strategic IT products and service engagements, software licensing, maintenance and development agreements, including software as a service (SaaS) and cloud computing arrangements, internet-related and other technology-based service agreements, and other strategic procurements. His work in these areas has focused on Fortune 1000 clients in the financial services, hospitality, restaurant, franchise, consumer products, electronics, utility, energy and online data/analytics industries.

Norton Rose Fulbright US LLP

Tel: +1 314 505 8832
Email: derek.johnston@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/derek-johnston-1493879

We provide the world's preeminent corporations and financial institutions with a full-business law service. We have more than 3,500 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; consumer markets; transport; technology; and life sciences and healthcare. Through our global risk-advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Melbourne, Sydney and Johannesburg.

Norton Rose Fulbright US LLP, 7676 Forsyth Blvd, Suite 2230, St. Louis, Missouri 63105, USA.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Technology Sourcing 2024 contains two expert analysis chapters and 17 Q&A jurisdiction chapters covering key issues, including:

- Procurement Processes
- General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services
- Dispute Resolution Procedures
- Intellectual Property Rights
- Data Protection and Information Security
- Employment Law
- Outsourcing of Technology Services
- Software Licensing (On-Premise)
- Cloud Computing Services
- AI and Machine Learning
- Blockchain

The International Comparative Legal Guides are published by: glg Global Legal Group