Data protection laws and international data transfers –

How can legal counsels deal with the complexities of a global digital world?

Nick Holland,
Partner, Shoosmiths

Nathalie Laneret,
Director of Privacy Policy,
Centre for Information Policy Leadership

Knut Mager,
Head Global Data Privacy,
Novartis International AG

Aoife Sexton,
Chief Privacy Officer and
Chief of Product Innovation, Trūata

25 May 2021

Overview of current privacy law around the world and how best to comply?

The GDPR in the news……

General Data Protection Regulation overview

- Creates uniform data protection laws across Europe.
- Came into force on 25 May 2018.
- Applies to all global businesses, offering goods and services to UK or European citizens or monitoring them.
- Introduces several new rights for individuals, with increased administrative obligations on organisations, with a risk of civil claims brought by individuals if such rights are infringed by those organisations.
- UK has implemented UK GDPR as a result of Brexit which is, for now, very similar to GDPR.
- Empowers Regulators to impose significant fines in the event of a breach; the greater of €20M or 4% of worldwide turnover.
- Used as a template by many countries in the creation and adoption of privacy laws coming into force in 2020/2021; Californian Consumer Privacy Act (CCPA), Brazilian General Data Protection Law (LGPD), Turkey's Privacy Act, Japanese Act on the Protection of Personal Information (APPI), new Indian Privacy Bill-many of which will apply to corporates even though they are not located in those countries

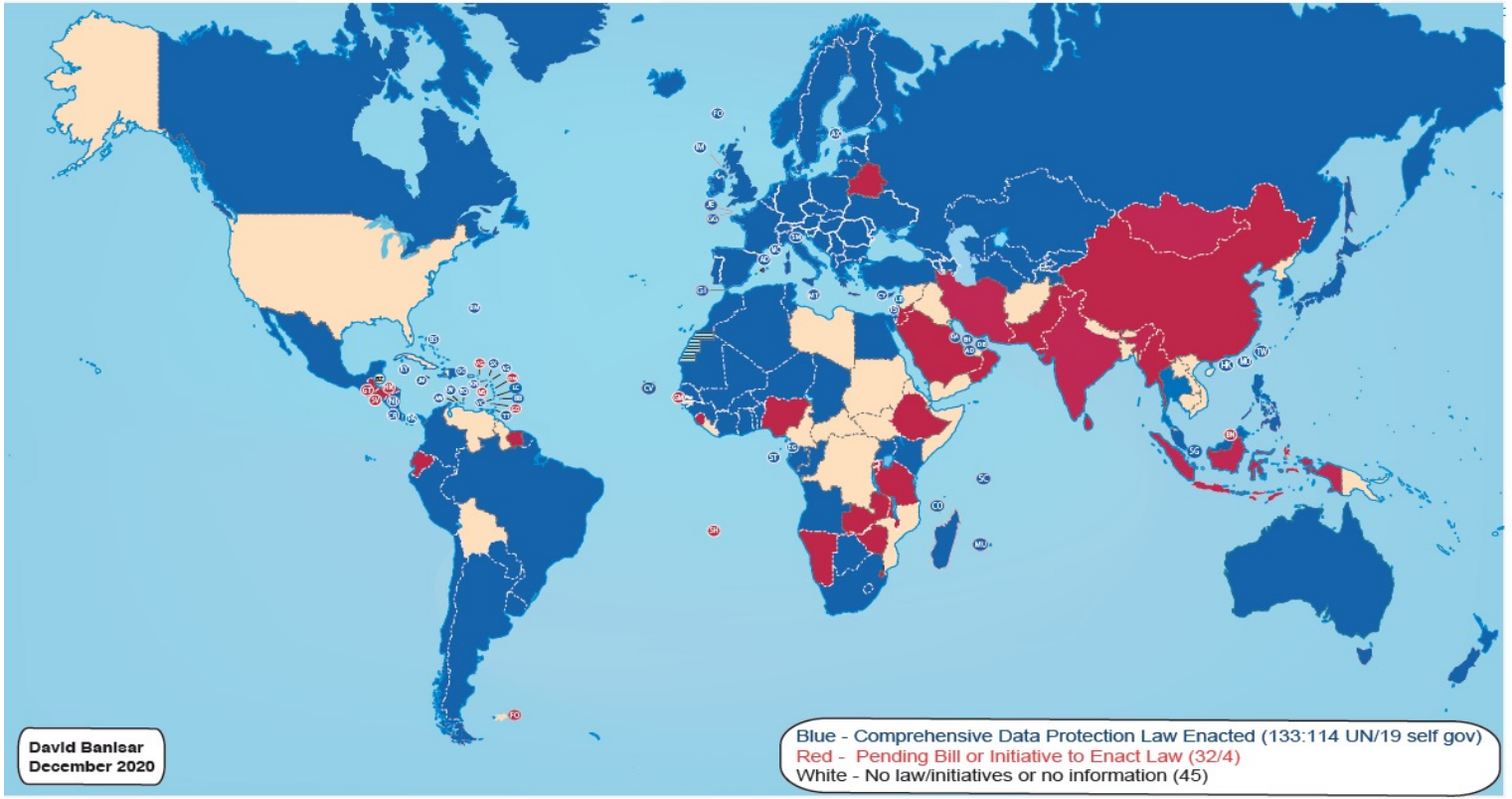
What does the GDPR require?

GDPR requirements	Impacts on the business
Expansion of scope	• New law applies to any business worldwide collecting or using EU data. • Applies to both data "controllers" and "processors" (i.e. service providers).
Enhanced rights for individuals	• Privacy policies need redrafting to include new mandatory transparency info. • New or enhanced rights for individuals to access, correct, delete and port data. • Consent needed for certain types of data profiling. • Greater protections against use of biometric data and genetic data.
Accountability requirements	• New policies, processes and training needed to "demonstrate" compliance. • Must be able prove valid consents given by individuals. • Detailed data record-keeping requirements. • Appointment of Data Protection Officer in some cases (plus registration in many countries). • Appointment of UK representative or EU representative • PIAs (and possible regulatory consultation) for "high risk" processing activities.

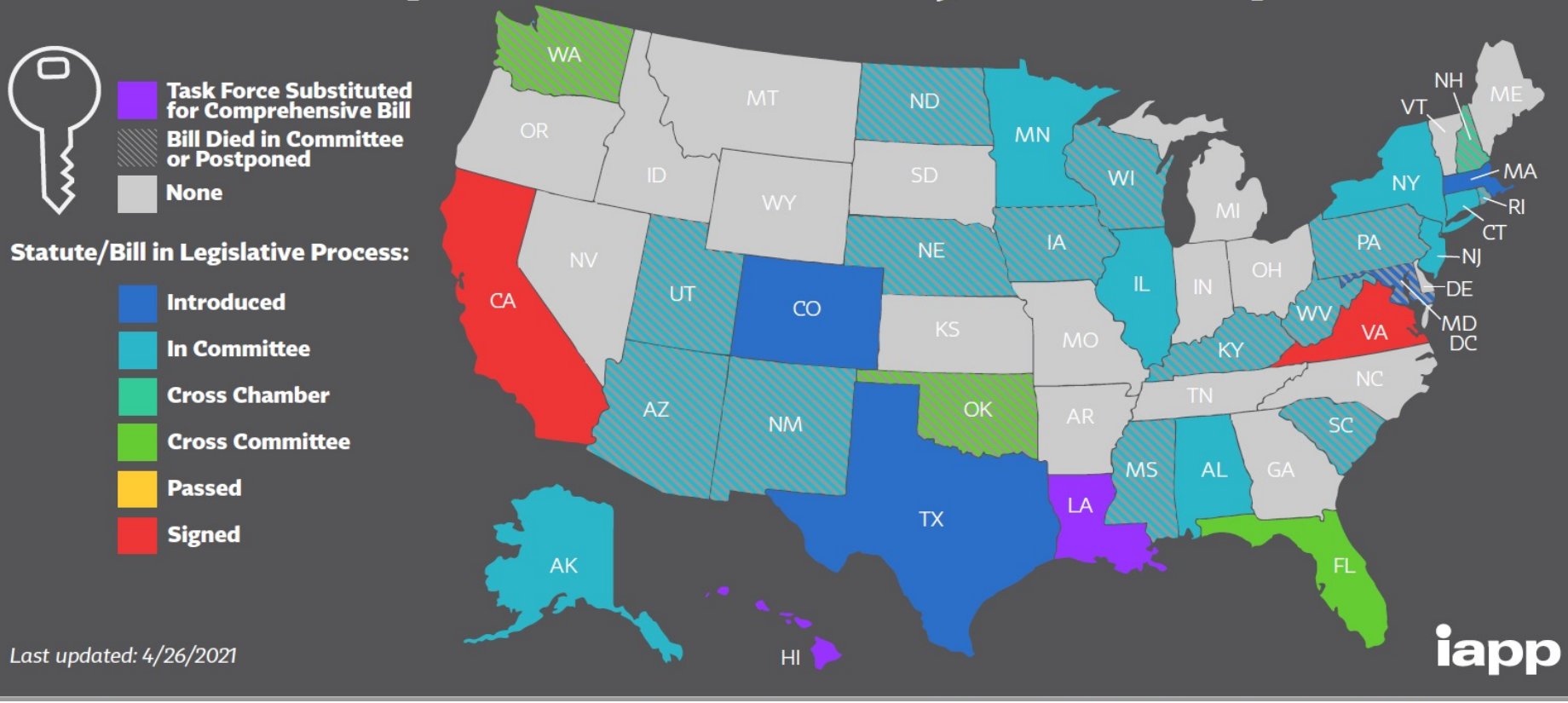
What does the GDPR require? (2)

GDPR requirements	Impacts on the business
Engineering requirements	• Requirement to implement Data Protection by Design. • Requirement to implement Data Protection by Default. • Emphasis on “data minimisation”.
Security requirements	• “Appropriate” measures needed to protect data security. • Strict time limits for reporting data breaches to regulators and individuals. • Mandatory contract terms with vendors = vendor re-procurement. • Do NIS Regulations apply
Data localisation requirements	• Prohibition against exporting personal data outside the EEA… • …unless one of a limited number of compliance solutions implemented… • …or transferring to a country designated “adequate” by the EU.
Enhanced powers for regulators	• Business primarily answered to a “lead authority” based on office establishment. • Mandatory audit rights over businesses. • Significant fining powers – **up to 4% annual worldwide turnover**.

National Comprehensive Data Protection/Privacy Laws and Bills 2020



State Comprehensive-Privacy Law Comparison



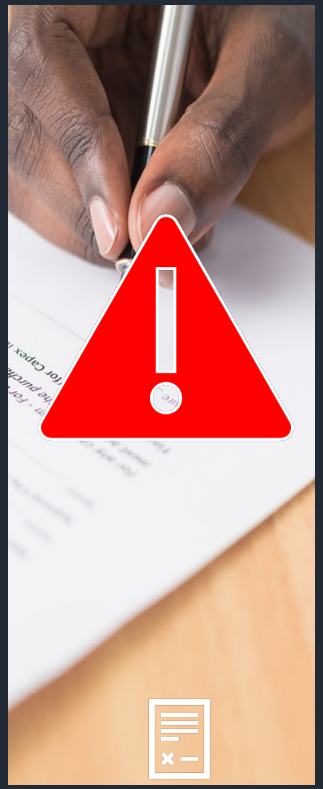
Handling international data transfers in a post Schrems 2.0 world

What was the Schrems 2.0 case about?

The case was principally about whether the Privacy Shield and existing SCCs offered enough protection:

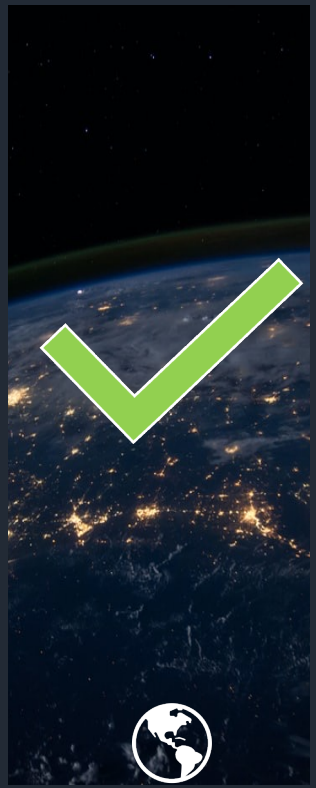
- *The Privacy Shield was invalidated with effect from 16th July 2020 because of U.S. surveillance activities and there being no actionable rights for EU/EEA citizens*
- *Current SCCs are seen to be technically valid, but they are not a paper or tick box exercise. Businesses on both sides must now do an assessment of whether there is equivalence with EU law and either not transfer or terminate the contract if necessary. We have called this exercise "SCC+" since the Schrems 2.0 decision. The new SCCs and guidance give clarity on these aspects*
- *BCRs remain a key safeguard*

"protection granted to personal data in the EEA must travel with the data wherever it goes"



Standard Contractual Clauses (SCCs)

Privacy Shield



Binding Corporate Rules (BCRs)

What next? Privacy Shield

Check

- Do you transfer personal data from the EU/EEA to the U.S. using the Privacy Shield? Check your records of processing activities/ data maps

Alternatives

- BCRs
- Hybrid DTA (not long-term solution for medium to large companies but an option for smaller companies) for internal matrix and SCC+
- SCC+ for external transfers
- Specific derogations (extremely restrictive)

Implement

- Do not wait for an alternative to the Privacy Shield
- Continue complying with your Privacy Shield obligations – for now
- Safest option is to use BCRs

BCRs

Check

- Are BCRs sensible for your business? For smaller businesses they are unlikely to be feasible (Hybrid DTAs are a good alternative). For multinationals they are by far the safest option

Review your privacy program

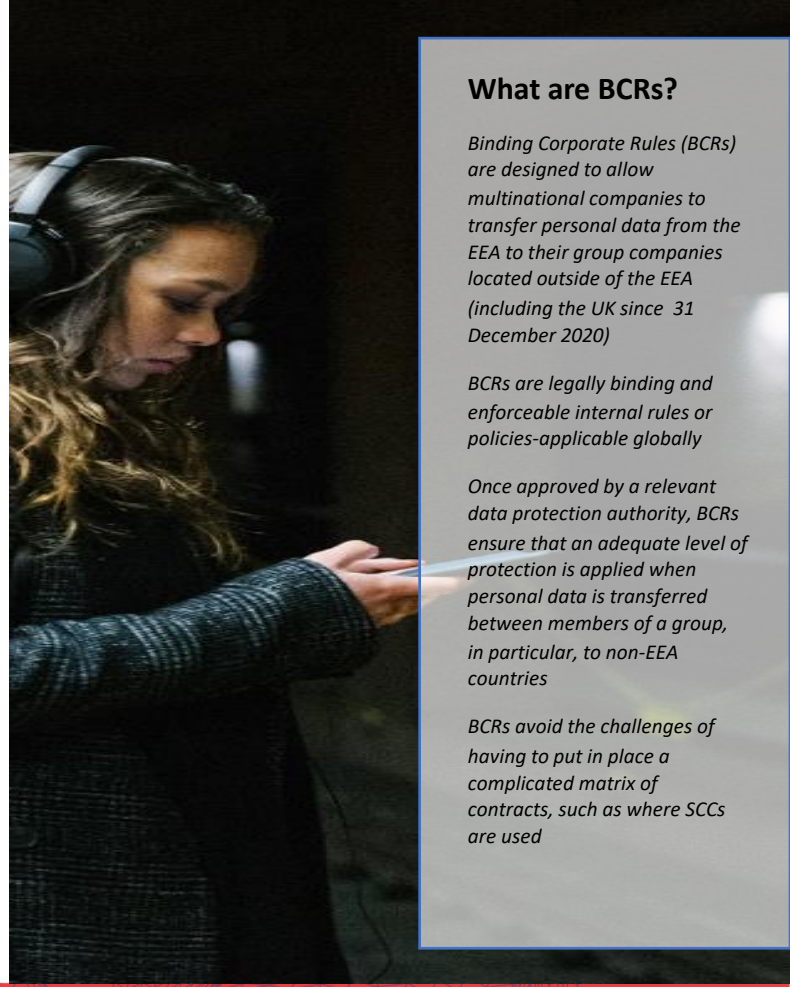
- Are you doing what you have committed to doing?
- How is your program doing generally?

Apply for BCRs

- Application offers regulatory protection (NB you are not irrevocably committed)

Existing BCRs

- A BCR holder with EU operations and the ICO as lead will need to have transferred to a new lead or otherwise the EU BCR will be invalid
- Changes will be needed as per EDPB checklist 22 July 2020
- ICO approved BCRs will need a UK BCR document suite
- EU BCRs will need to put a UK BCR in place (with or without formal approval)



What are BCRs?

Binding Corporate Rules (BCRs) are designed to allow multinational companies to transfer personal data from the EEA to their group companies located outside of the EEA (including the UK since 31 December 2020)

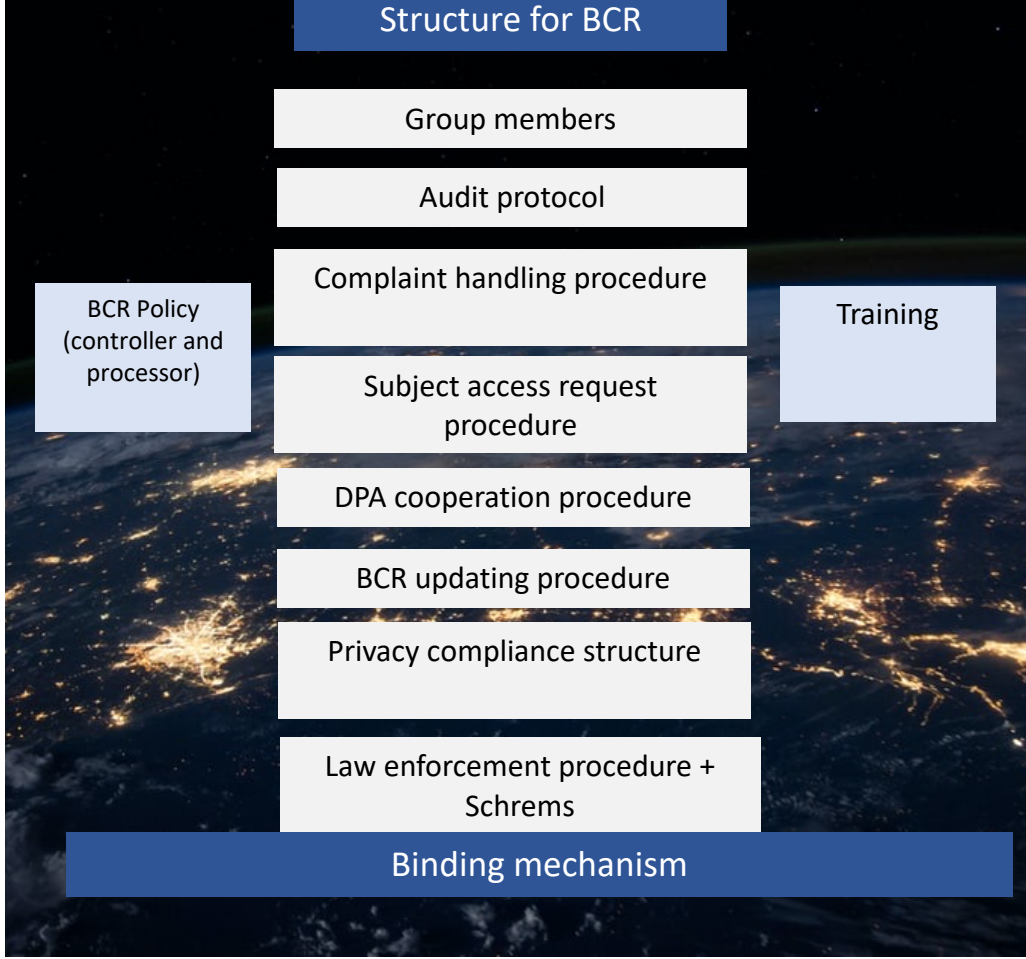
BCRs are legally binding and enforceable internal rules or policies-applicable globally

Once approved by a relevant data protection authority, BCRs ensure that an adequate level of protection is applied when personal data is transferred between members of a group, in particular, to non-EEA countries

BCRs avoid the challenges of having to put in place a complicated matrix of contracts, such as where SCCs are used

BCRs

- BCR means a collection of global policies and procedures that a multinational would sign up to apply globally-see the structure opposite for an overview of those policies and procedures
- Apply for a Controller and Processor BCR which therefore deals with both your employee and customer data processing globally
- **Customer Perception:** Your customers will perceive you as being "best in class" when it comes to having BCR status which in turn will significantly save time on negotiations and queries about your privacy compliance and assist in tender processes. You can also enter into a BCR processor agreement where you are processing their customer data
- **Relationships with DPAs:** By virtue of your negotiations with DPAs on the BCR you will have good relationships with them which will be beneficial for future compliance, particularly if you suffer a data breach (cf US attitude to engaging regulators)
- **Accountability under GDPR:** One of the key tenets of GDPR compliance is to show how you are accountable under GDPR and having a BCR, which you can show on your website, will prove your accountability to regulators, customers and employees. All your global privacy requirements and governance can flow under the BCR
- **Global applicability:** We have been working on producing BCR's that are GDPR compliant for the last 2 years (we achieved world's first controller/processor BCR post GDPR via the new BCR process in May 2020) and this will enable you to have the benefit of the BCR plus all of your GDPR requirements in one place as well as accommodating other privacy laws such as CCPA, Brazil, India, Turkey etc

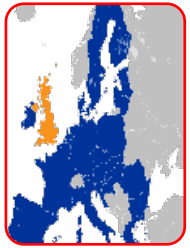


What does the new UK data protection regime look like?

- There are two regimes, and possibly temporarily three regimes depending on whether UK adequacy is achieved

The 'UK GDPR': the UK's new bespoke version + the DPA 2018
The 'UK GDPR' is the UK data protection regime based on the 'EU GDPR'
It entered into force at 11pm on 31 December 2020
After 31 December 2020, UK courts may interpret the UK GDPR differently from the EU GDPR and new CJEU judgments are no longer binding on the UK so the UK and EU regime could start to diverge. Previous CJEU decisions (including Schrems 2.0) will continue to be binding on UK courts (apart from the Supreme Court).
The Data Protection Act 2018 will continue in force and as amended will complement the 'UK GDPR'
The ICO will be the supervisory authority
Scope
UK controllers or processors wherever their processing takes place
Controllers and processors based outside the UK if their processing activities relate to offering goods or services to individuals in the UK, or monitoring the behaviour of individuals taking place in the UK

The 'EU GDPR': the original GDPR
The 'EU GDPR' is the existing EU data protection regime
After 31 December 2020 the EU may amend the 'EU GDPR' so that it starts to vary from the 'UK GDPR'
The ICO will not be the supervisory authority
Scope:
UK controllers who have an establishment in the EEA, or who have customers in the EEA, or monitor individuals in the EEA
As before, any controllers and processors who have an establishment in the EEA, or who have customers in the EEA, or monitor individuals in the EEA eg EEA controllers sending personal data to the UK



The 'adequacy gap' or 'legacy' regime: the specific regime for 'non-UK personal data'
This 'adequacy gap' data protection regime, set out in Article 71 of the
Withdrawal Agreement, is designed for the period after 31 December 2020 and before the date of a UK adequacy decision (if any)
It entered into force at 11pm on 31 December 2020 and remains until the date of a UK adequacy decision is made (if any).
Scope:
Personal data of data subjects outside the UK but processed in the UK subject to EU GDPR before the transition period and which must remain subject to EU GDPR post 31 December 2020There is some debate about whether this is a "frozen" GDPR or not

UK Representative
From 1 January 2021, those companies who do not have a physical footprint in the UK but who sell to or monitor people in the UK must appoint a UK representative-see Shoosmiths' fixed price, online service /dataprivacyrep which offers this service at our dedicated webpage at https://www.shoosmiths.co.uk

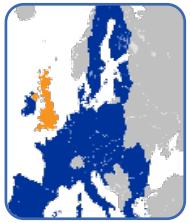
UK Adequacy

Process and deadlines

The EDPB must review and provide an opinion

The European Commission will request approval from member states

Data flows between the EEA and the UK are safeguarded under the EU-UK Trade and Cooperation Agreement temporary bridge until 30 June 2021



What does it mean?

That the UK is deemed to provide an essentially equivalent data protection regime to the EEA Data can flow freely between the EEA and UK without needing standard contract clauses added into contracts or other additional safeguards

The third countries deemed adequate by the EU which currently share data with the UK will have to decide about the UK status.

The UK government has said it intends for the EEA and EU-recognised adequate locations to be recognised by the UK and this is recognised on a transitional basis

What happens after 30 June 2021 when the temporary bridge ends?

If an adequacy agreement is approved

Data can flow freely between the EEA and UK

The decision will last for 4 years and will be reviewed

If an adequacy agreement is not approved

The UK will be deemed to be a "third country" and data flows will need assessment and additional safeguards (see later)

The ICO has said

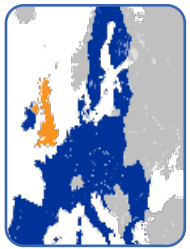
"The draft adequacy decisions are an important milestone in securing the continued frictionless data transfers from the EU to the UK. Today's announcement gets us a step closer to having a clear picture for organisations processing personal data from the EU and I welcome the progress that has been made."

Transfers	Free flow of personal data after end of temporary bridge?
Transfer of data UK → EEA	Y transitionally **Needs review** the UK could decide to impose restrictions in future particularly if the temporary bridge ends with no adequacy decision for the UK
Transfer of data EEA → UK	N Safeguards needed (see later) UK adequacy decision will mean free flow of transfers
Transfer of data UK → EU deemed adequate countries	Y transitionally **Needs review** as the UK could decide to impose restrictions in future particularly if the temporary bridge ends with no adequacy decision for the UK
Transfer of data EU deemed adequate countries → UK	Varied by location Each location can decide how they see the UK's data protection regime now post transition period and what impact that may have for data flows to the UK.Most (11 of the 12) have confirmed they intend business as usual although this needs implementing. **Needs review** UK adequacy decision may positively influence the free flow of transfers
Transfer of data UK → rest of the world outside of EEA	N Safeguards needed (see later) **Needs review** as it is possible that new cross border regimes are created by the UK
Transfer of data rest of the world outside of EEA → UK	Varied by location Each location can decide how they see the UK's data protection regime now post transition period and what impact that may have for data flows to the UK. **Needs review** UK adequacy decision may positively influence the free flow of transfers

International Transfers

- What can move freely?

Existing EU SCCs
EU SCCs entered into prior to 31 December 2020 remain valid for use where needed for transfers into and out of the UK
For new transfers the existing EU SCCs remain valid at present (see below for UK tweaks)
NEW UK SCCs
The ICO intends to publish new UK SCCs for consultation in summer 2021 and to conclude that by October. It has produced an amended version of the existing EU SCCs to make sense in a UK context
At some point EU SCCs may be invalid for transfers from the UK
NEW EU SCCs
The European Commission consulted on draft new SCCs in November 2020 which are radically different. They are expected to have a 1 year transition period for use
EDPB and EDPS issued a joint opinion on the draft clauses in January 2021 recommending some changes and clarifications
A final set of SCCs is expected sometime in May and June 2021. It is likely they will be valid where the EU GDPR applies. It remains to be seen whether the UK will approve them but they will be invalid for transfers out of the UK under UK GDPR otherwise



EDPB is consulting on recommendations on supplementary measures

These are in addition to the EU SCCs and involve complex assessments (see later)
EDPB guidance strictly will not apply directly to the UK GDPR transfer regime and the ICO will issue its own guidance subsequently. The guidance is very influential and the Schrems 2.0 decision is still binding so additional measures will be needed.

Derogations

If the recipient is not located in a country that benefits from an adequacy decision and there are no adequate safeguards for the transfer, the final option is for the transfer to fall within one of the narrowly construed derogations set out in Article 49 of the EU GDPR for specific situations

Transfers needing safeguards

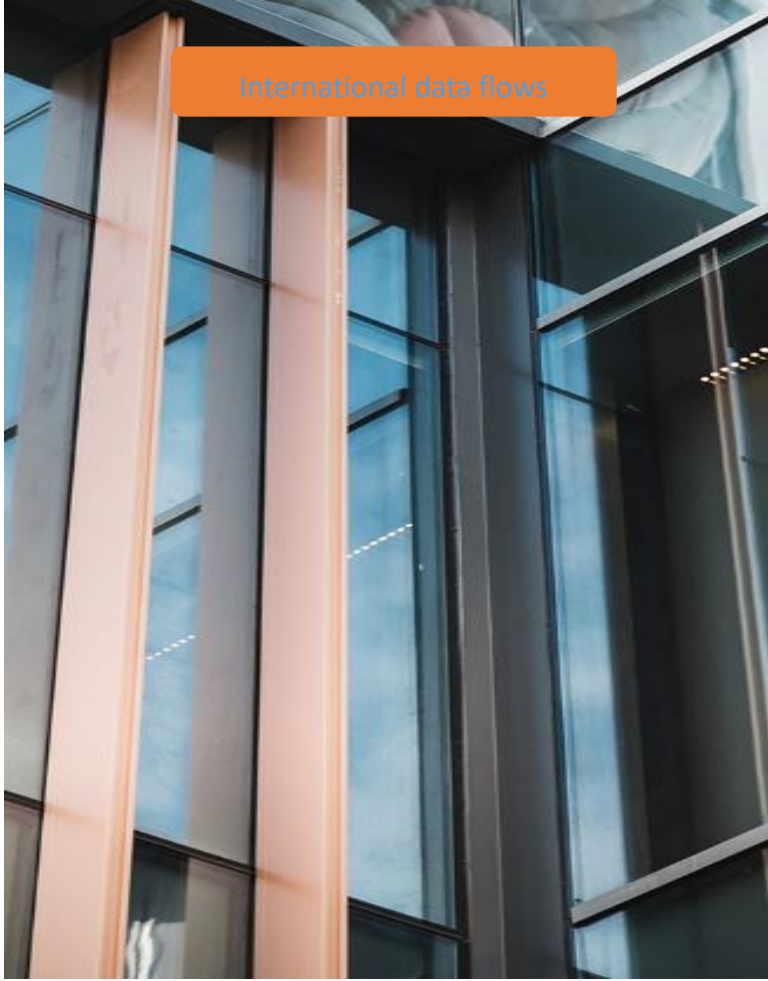
See later especially SCC+

What do you do now (and *assuming there will be a final UK adequacy decision)?*

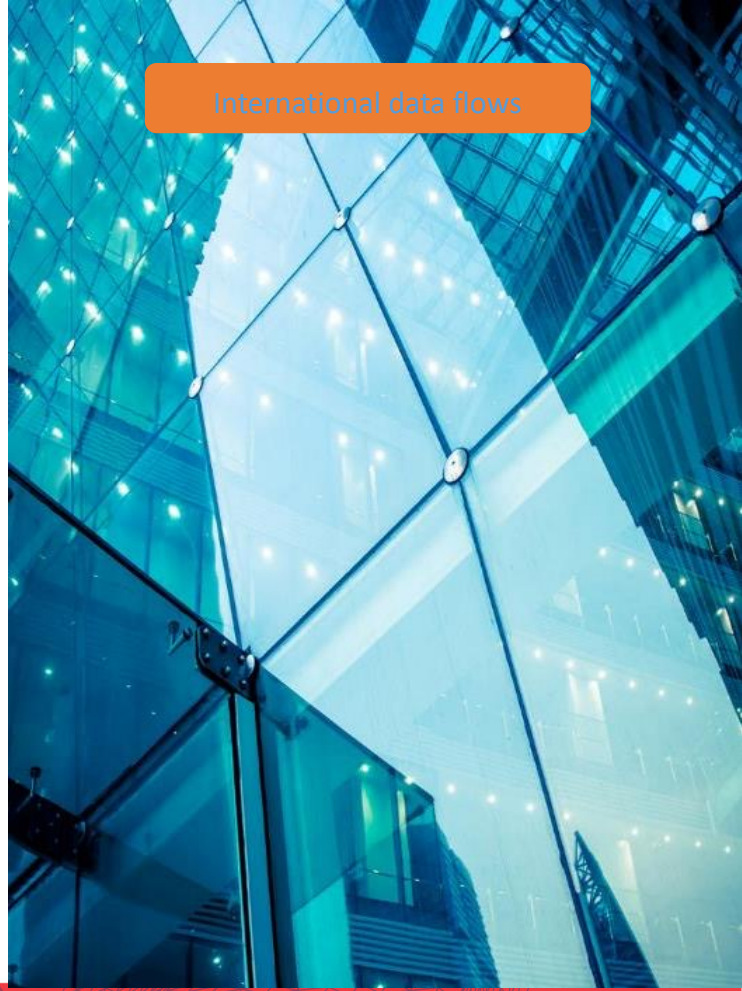
- Comply with the GDPR
- Understand what GDPR regime applies to your business either UK GDPR or EU GDPR.
- Understand your data flows (RoPA) and locations involved. You will need to distinguish UK processing from EU processing. Prioritise flows containing large volumes, special category data or criminal convictions and offences data, business-critical transfers, and those involving key higher risk areas such as the US.
- Appoint EU and UK and NIS representatives if necessary
- Assess your appropriate lead supervisory authority
- Update your BCRs and apply for UK BCRs as needed
- Keep track of privacy law changes
- Review your privacy notices, DPIAs, SCCs and other documentation to update references to EU law, UK-EU transfers and your UK and/or EU representative
- Ensure your DPO will be easily accessible from any UK and EEA establishments and has expertise in all regimes

What do you do now (and *assuming there will be a final UK adequacy decision)?*

- Between the EEA and the UK and all other “adequate” locations:
- Data likely to flow freely (see transfer table earlier, some review is needed)
- Between the rest of the world and the EEA and UK **where safeguards are needed: (see transfer table earlier)**
- Likely options medium to large companies:
    - BCRs controller and processor which address processing internally and with customers
    - Hybrid DTA, and
    - SCC+ (see later)
- Likely options smaller companies:
    - Hybrid DTA, and
    - SCC+ (see later)



What do you do now (and assuming there will be a final UK adequacy decision)?



- What is SCC+?:

- No contract will achieve compliance on its own. SCC+ involves supplementary measures as well as adding SCCs into a contract to justify transfers
- Understand your data flows!
- Understand the existing SCC obligations. They require significant vigilance, legal advice, ongoing monitoring and action
- Bear in mind the industry involved, categories and volume of personal data transferred, purposes of the processing by the importer, and duration of data retention in the third country
- Undertake and record a transfer risk assessment both within the company group but also externally with existing third-party vendors and suppliers looking for anything in the law or practice of the locations involved that may affect the SCC safeguards. Specifically:
    - Prohibitions on transfers or guidance by location. We have tracked this globally;
    - law enforcement implications and processes and the rules for disclosure to and access by governmental agencies. Our location analysis questionnaire can be used;
    - conflicts with GDPR data protection standards;
    - an independent oversight mechanism and enforceability of rights and claims including in a court or tribunal.

What do you do now (and *assuming there will be a final UK adequacy decision)?*

- What is SCC+?:

- Consider technical measures such as:

    - Encryption (there is technical complexity to this)
    - Pseudonymisation
    - Split or multi-party processing

- Create additional clauses within your Hybrid DTA or GDPR-compliant contract to supplement the SCCs to address specific risks such as importer transparency, enhanced audits, challenging government access requests, notification requirements about being unable to comply with SCC clauses and enhanced data subject rights
- Update/review your due diligence processes for new vendors and suppliers especially in the US and risky locations. Our location questionnaire can be used
- Consider your data protection compliance assessment generally including internal policies for governance of transfers, and dealing with government access requests, staff training, data minimization processes, internationally recognized security standards, and commitments not to make onward transfers to countries that do not offer essentially equivalent protections

Top 10 Tips for Global Privacy Compliance

- Know your processing activities – it's not only a legal requirement, but a practical need (where would you start your assessments?)
- Partner with IT/ Information Security – technical safeguards are a must
- Partner with Compliance to implement strong processes and train associates
- Find a systematic approach to assess risk suitable for your context – there are many out there, find just one and stick to it
- Always Follow the Data…
- Educate your organisation as to what a risk based approach might look like in practice
- Explore how privacy tech might help your organisation continue to do transfers
- Create a practical governance structure to ensure maintenance
- Stay calm, Privacy is not a dark art – at its core it is about doing the right thing with data
- Doing nothing is NOT an option!