BREXIT INSIGHT WEBINAR

Brexit and data protection

Will there be fireworks?

SHOOSMITHS

Today’s session

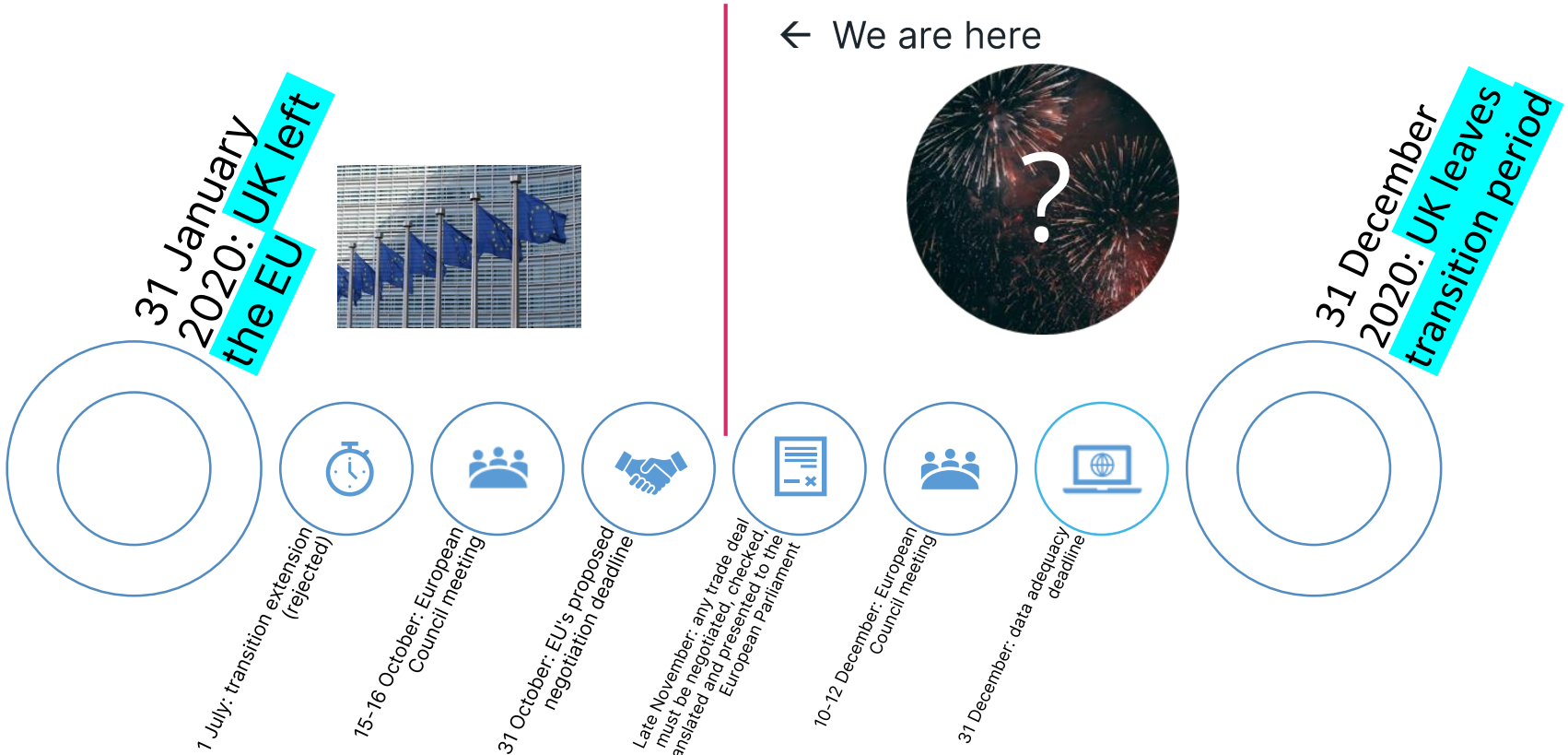
An update on Brexit and data protection

Presenters:

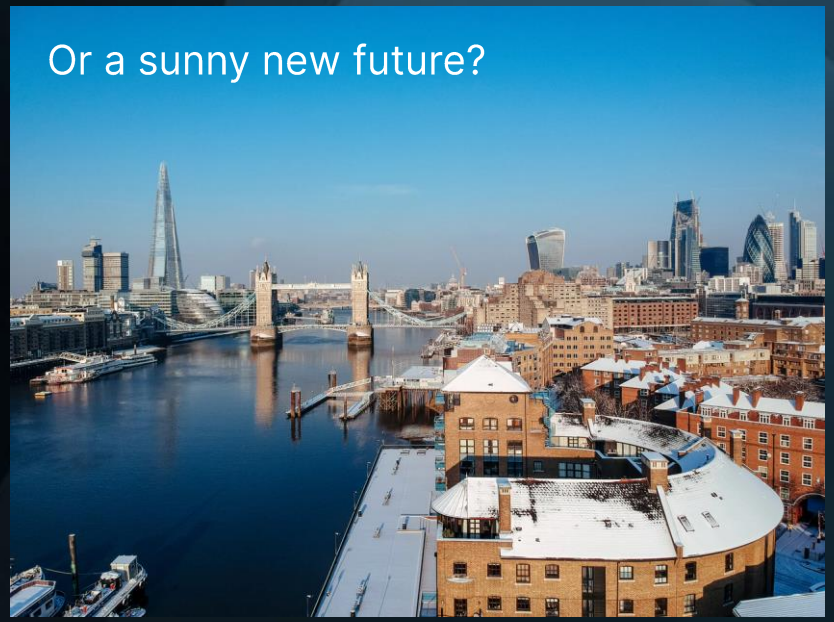
Nick Holland and Sarah Tedstone

5 November 2020

2020: Brexit 1.0 → Brexit 2.0



January 2021: UK out in the cold?

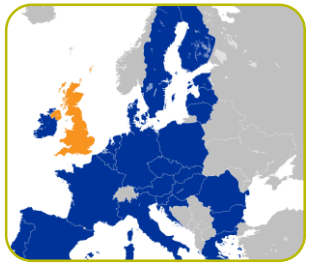


What does the new UK data protection regime look like?

There will be two regimes, and possibly three regimes depending on whether the European Commission grants UK adequacy

Regime 1: the 'UK GDPR': the UK's new bespoke version + the DPA 2018

- The 'UK GDPR' will be the UK data protection regime based on the 'EU GDPR'
- It will enter 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 would no longer be binding on the UK so the UK and EU regime would 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



Regime 2: the 'adequacy gap' or 'legacy' regime: the specific regime for 'non-UK personal data'

- This 'legacy data' 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 adequacy decision (if any)
- It will enter into force at 11pm on 31 December 2020 or until the date of an adequacy decision is made (if any).
- Scope:
  - Personal data of EEA data subjects outside the UK but processed in the UK subject to EU GDPR before the transition period which must remain subject to EU GDPR post 31 December 2020
  - This may be called a "frozen" GDPR

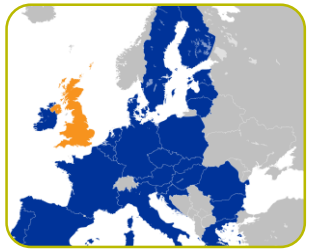
Regime 3: the 'EU GDPR': the original GDPR

- The 'EU GDPR' is the current 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 or elsewhere

What about emarketing, NIS Directive, FOIA and EIR?

PECR

- PECR rules cover emarketing, cookies and electronic communications. They derive from EU law but are set out in UK law. They will continue to apply in the UK at the end of the transition period.
- The EU is replacing the current e-privacy law with a new e-privacy Regulation (ePR). The new ePR is not yet agreed. It remains to be seen if and how it will be applied in the UK



NIS Directive

Covers network and information systems. It derives from EU law but is set out in UK law. It will continue to apply at the end of the transition period.

If you are a UK-based digital service provider offering services in the EU (eg SaaS provider), from the end of the transition period you may need to appoint a representative in one of the EU member states in which you offer services. You will need to comply with the local NIS rules in that member state.

If you also offer services in the UK, you will also need to continue to comply with the UK rules regarding your UK services.

FOIA and EIR

The FOIA 2000 forms part of UK law and will continue to apply.

The EIR derive from EU law but are set out in UK law. The UK has also independently signed up to the underlying international treaty on access to environmental information (the Aarhus Convention).

UK National Data Strategy

'The National Data Strategy (NDS) is an ambitious, pro-growth strategy that aims to drive the UK in building a world-leading data economy while ensuring public trust in data use.'

- *Published 9 September 2020; out to consultation until 2 December 2020*
- *'We want the data revolution to benefit businesses large and small. That means maintaining a data regime in the UK that is not too burdensome for the average company; one that helps innovators and entrepreneurs to use data responsibly and securely, without undue regulatory uncertainty or risk, to drive growth across the economy.'*
- *'We will seek EU 'data adequacy' to maintain the free flow of personal data from the EEA, and we will pursue UK 'data adequacy' with global partners to promote the free flow of data to and from the UK and ensure that it will be properly protected.'*
- *There is a commitment to review the use of alternative cross-border transfer mechanisms*

Adequacy ⟺

- *It is unclear whether the UK will obtain an adequacy finding from the EU before 31 December 2020. This will have a major impact on EEA to UK transfers in particular.*
- *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.*
- *In October 2020, the Department for Culture, Media & Sport (DCMS) indicated it was confident that the UK's data protection standards will gain a finding of adequacy status from the EC before 1 January 2021. The process involves assessment, a draft decision, an opinion from the EDPB, a vote by the EC and adoption. Progress has not been publicised. The UK government in March 2020 published its own view of its data protection regime and protections from intelligence surveillance as a basis for discussions.*
- *DCMS has advised UK-based organisations to be prepared to adopt appropriate safeguards to legitimise transfers of data from the EEA.*
- *DCMS notes 11 of the 12 third countries deemed adequate by the EU have currently informed the UK government they will maintain unrestricted personal data flows with the UK.*

Adequacy ⟺

Potential risk factors for a UK adequacy finding:

- *UK's use of mass surveillance techniques*
- *UK membership of the Five Eyes intelligence sharing community*
- *UK potentially diverging from the EU on data protection after Brexit 2.0*
- *UK deeming third countries to be adequate (and thus allowing for onward data transfers) which the EU doesn't deem to be adequate*
- *UK no longer being part of the Charter of Fundamental Rights of the European Union*
- *Politicians threatening to leave all or part of the European Convention on Human Rights*
- *The Schrems 2.0 judgment*
- *The immigration exemption in the Data Protection Act 2018*

Issues	Actions
Transfer of data UK → EEA	Some impact may occur Bear in mind regimes (which may diverge) The intention is that the UK will deem the EU/EEA 'adequate' for data transfers although this needs implementing.

Transfer of data
EEA → UK
	Act now to protect and maintain your data flows in anticipation of no UK adequacy by 31 December 2020
	
	• determine what data transfer solution works best for your business to miminise the legal and commercial risk to your operations if there is no adequacy agreement
	• strategise how you use and protect your data generally
	• options if there is no adequacy:
	  • BCRs
	  • Hybrid DTA
	  • SCC+
	  • narrow list of derogations in the GDPR

Transfer of data UK → the countries the EU has deemed adequate	Some impact may occur Bear in mind regimes (which may diverge) The intention is that the UK will deem them 'adequate' for data transfers although this needs implementing.
Transfer of data the countries the EU has deemed adequate → UK	Some impact may occur Bear in mind regimes (which may diverge) and whether there is UK adequacy if EU GDPR and Legacy data regimes apply (see EEA → UK above). Most have confirmed they intend business as usual otherwise for transfers into the UK although this needs implementing.
Transfer of data UK → rest of the world	Bear in mind regimes (which may diverge) UK government intends business as usual. It is possible that new cross border regimes are created
Transfer of data rest of the world → UK	Bear in mind regimes (which may diverge) and whether there is UK adequacy if EU GDPR and Legacy data regimes apply (see EEA → UK above). It is possible that new cross border regimes are created

No UK adequacy? BCRs

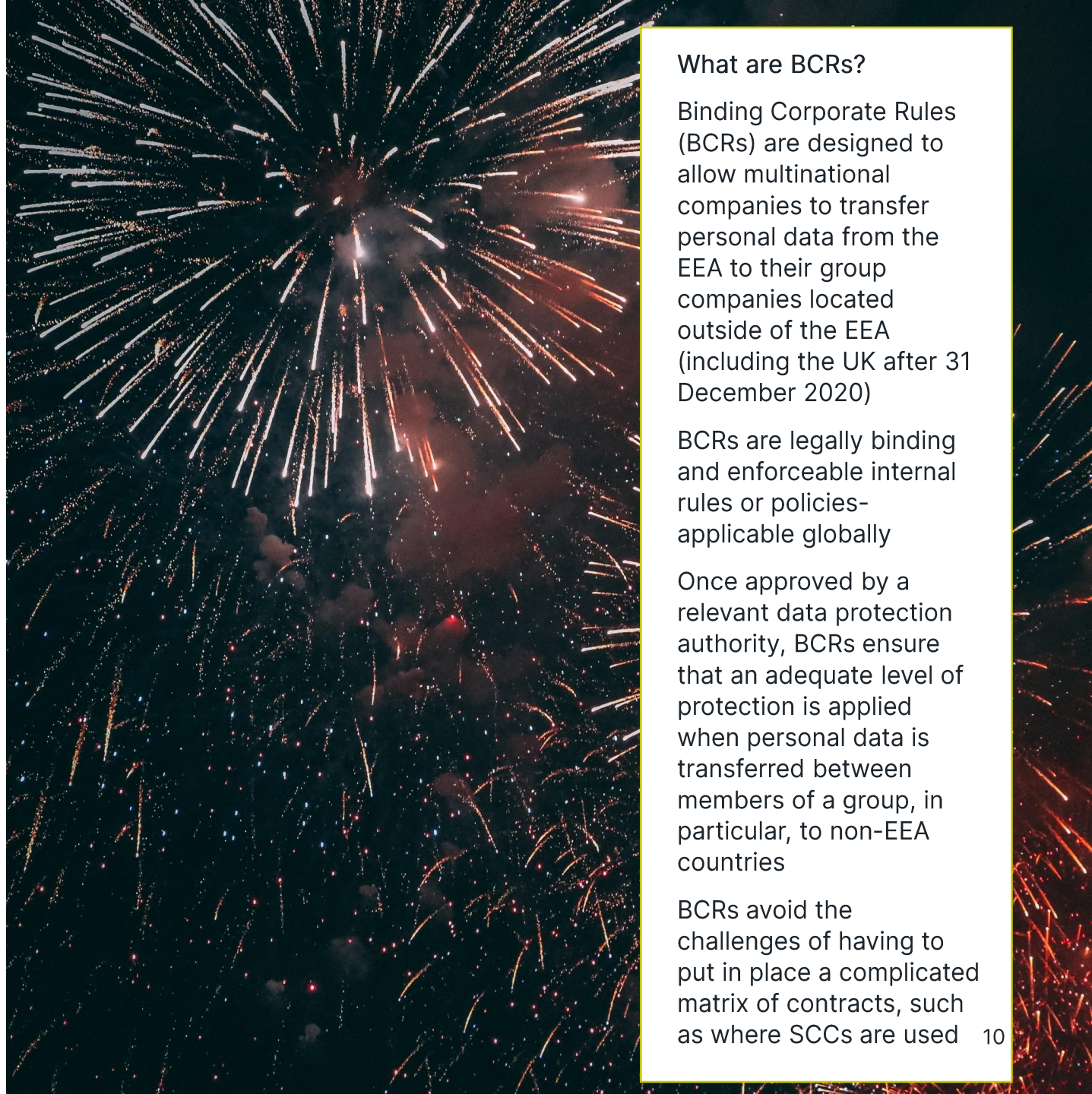
Check
- Are BCRs sensible for your business? For smaller businesses they are unlikely to be feasible (Hybrid DTAs are a good alternative). For multinationals they are by far the safest option

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 transfer to a new lead
- Changes will be needed as per EDPB checklist 22 July 2020

SHOOSMITHS



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 after 31 December 2020)

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

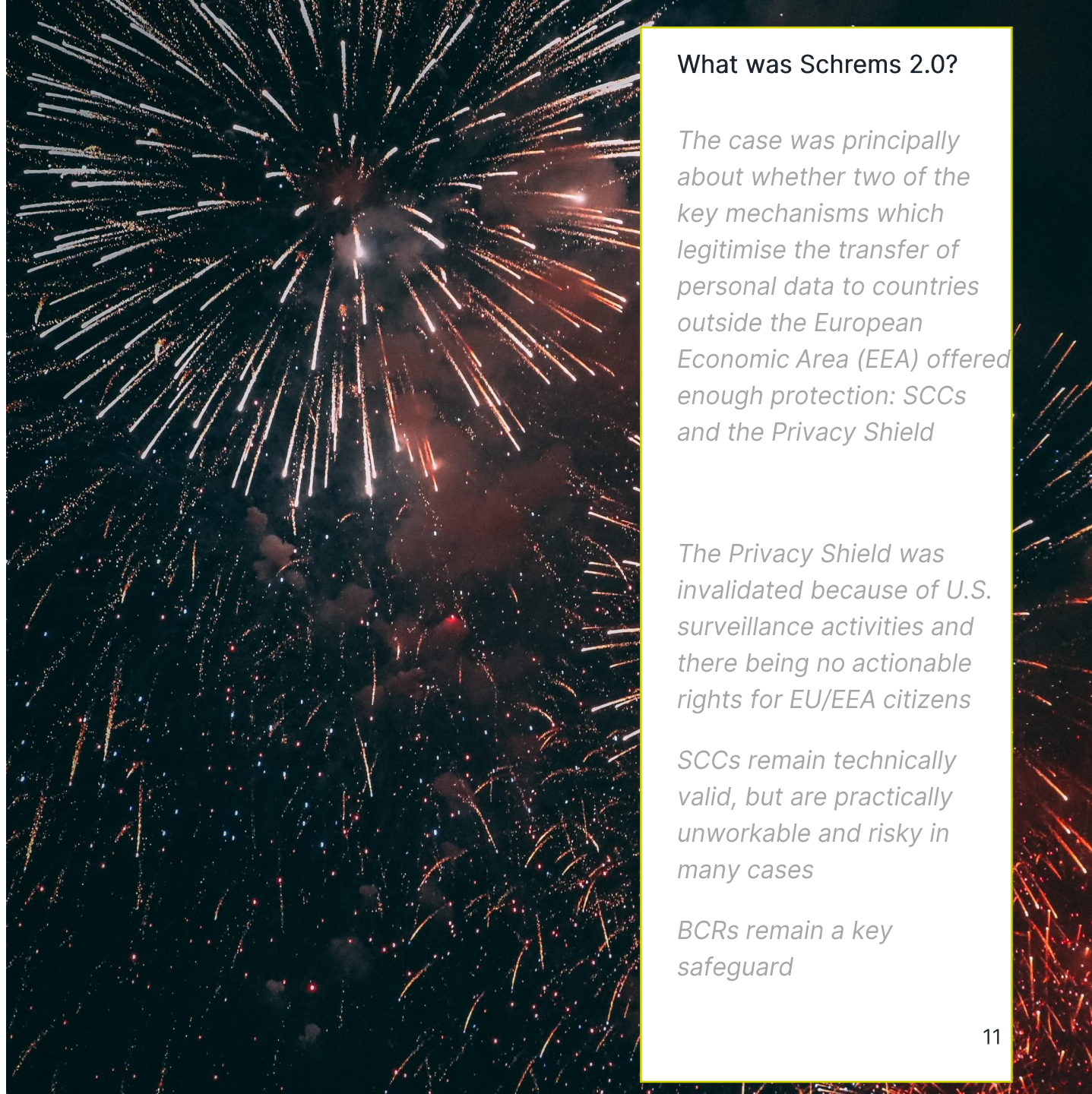
Once approved by a relevant data protection authority, BCRs ensure that an adequate level of protection is applied when personal data is transferred between members of a group, in particular, to non-EEA countries

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

Schrems 2.0 and Brexit 2.0

The Schrems 2.0 risks add potential complications for Brexit for two key reasons:

- SCCs are likely to be a key safeguard for transfers of personal data into the UK after 31 December 2020 in the absence of UK adequacy
- The criticisms of the US surveillance regime in the case raise doubts about the UK's own regime which may impact a UK adequacy decision



What was Schrems 2.0?

The case was principally about whether two of the key mechanisms which legitimise the transfer of personal data to countries outside the European Economic Area (EEA) offered enough protection: SCCs and the Privacy Shield

The Privacy Shield was invalidated because of U.S. surveillance activities and there being no actionable rights for EU/EEA citizens

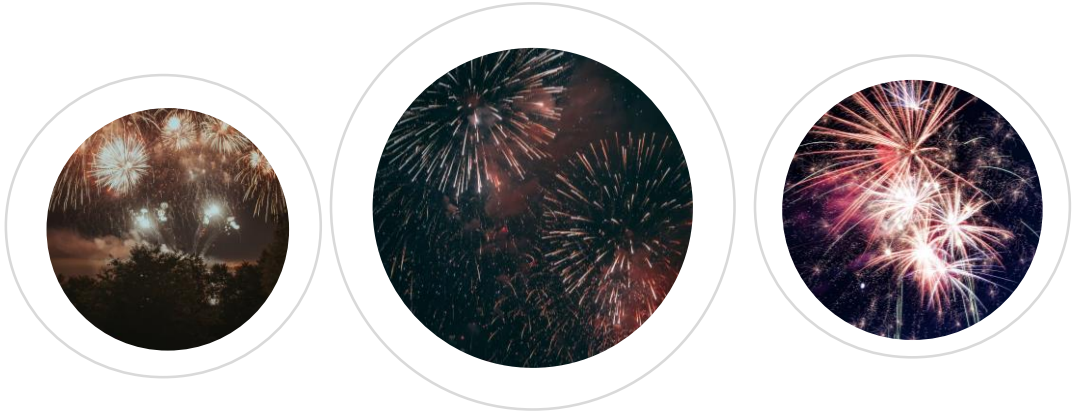
SCCs remain technically valid, but are practically unworkable and risky in many cases

BCRs remain a key safeguard

No UK adequacy: SCC+

- Update ROPA- understanding your data flows and locations is key
- Assess what safeguards are needed
- Remember: No contract will achieve compliance on its own
- Understand the existing SCC obligations. The UK government intends for the existing SCCs to remain valid for UK use. They require significant vigilance, legal advice, ongoing monitoring and action and formal decisions about whether transfers can take place
- Undertake and record a mini-DPIA to justify the adequacy internally, externally about any specific transfer:
    - Map out the transfer locations involved
    - Risk assess locations both within the company group but also externally with existing third-party vendors and suppliers for:
        - specific prohibitions on transfers or particular guidance by location. We have tracked this globally;
        - law enforcement implications and processes- to verify the rules for disclosure to and access by governmental agencies and in the US specifically, the FISA requirements. Our location analysis questionnaire can be used;
        - conflicts with GDPR data protection standards;
        - assessment of enforceability of rights and claims including in a court or tribunal;
        - 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;

No UK adequacy: SCC+



- any potential amendment to privacy notices to data subjects needed;
- assessment of your ability to comply with the standard SCC obligations; and
- assessment of whether additional terms will be needed.

- Create additional clauses within your Hybrid DTA or GDPR-compliant contract to supplement the SCCs to address specific risks
- 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 and update risk priorities to adopt and evidence basic principles including accountability and baking in privacy by design and default, and considering technical and organisational methods such as minimisation, anonymisation, pseudonomysation, encryption. This will all assist with the justification of processing and transferring. Our compliance plans have always been created with these basic principles in mind and these will be even more important ongoing potentially.
- Monitor developments. Updated SCCs and guidance from the EDPB is expected, but organisations should have realistic expectations that obligations remain on them to take steps by themselves to comply with privacy laws.
- Any new SCCs will NOT obviate from the need to undertake the work above!

UK Representative

- Analogous to EU Representative requirement
- Applies to any business outside the UK, which must appoint a UK Representative if it is caught by extra-territorial rules, namely which:
  - has no UK physical footprint
  - either monitors UK individuals or targets goods/services in UK
- Excludes public sector entities, and excludes occasional processing
- *Whether or not an adequacy decision is made*

The role of the UK Rep

Key responsibilities:

- maintaining the Record of Processing Activities (ROPA) as required under Art 30 – as provided to it by the appointing controller/processor
- facilitating communications between individuals and the controller/processor, and between the ICO and the controller/processor
- cooperating with & providing information (including the Art 30 ROPA) to ICO
- named as point of contact for UK data subjects on privacy notices

Does not include:

- fulfilling data subject rights
- advising the controller/processor on commercial strategies, or legal rights or obligations

Announcing the UK Representative Service

- In response to demand, Shoosmiths will be launching a UK Representative Service next week.
- This will be a fixed price, platform-based service, and available to any business.
- It will be provided by Shoosmiths Privacy Services (a subsidiary of Shoosmiths LLP).
- We are also likely to be launching an EU Representative Service within the next month for clients based in the UK which offer goods and services to, or monitor the behaviour of, individuals in the EEA, after 31 December 2020.
- Watch this space!

DPOs

If you are currently required to have a DPO, that requirement will continue, whether under the UK GDPR, EU GDPR or Legacy data regime. You may continue to have a DPO who covers the UK and EEA.

The DPO can continue to be located in the UK.

The UK and EU GDPRs will both require that your DPO is easily accessible from each establishment in the EEA and UK, and, has expert knowledge of both regimes.

One-stop shop

- *If your business carries out any cross-border processing involving the EU/EEA, it currently benefits from the One-Stop-Shop system under the GDPR. This means a single data protection authority acts as the lead on behalf of the other EEA data protection authorities.*
- *During the transition period, the One-Stop-Shop system has continued. However, you should start preparing now for what happens once this period ends. If you continue any cross-border processing, you lead authority will need to change if it is currently the ICO.*
- *The ICO will not be the regulator for any European-specific activities caught by the EU GDPR, although cooperation is still anticipated.*

Cookies and consent

- *In situations where the EU GDPR applies, organisations will be bound by EU Member State Laws and ongoing guidance. The EDPB has recently issued guidance on consent, and CNIL has updated its guidance on cookies. The ICO has yet to clarify its position.*
- *In situations where sites can be accessed around the world, this could be a complex legal area to navigate after 31 December 2020.*
- *CNIL: User consent: The mere continuation of browsing a site can no longer be considered a valid expression of the user's consent*
- *people must consent to the filing of tracers by a clear positive act (such as clicking "I accept" in a cookie banner). If they do not, no tracers that are not essential to the operation of the service will be able to be deposited on their device.*
- *A strict interpretation of the EDPB guidelines would be that separate consents are required for direct marketing and sharing of the information for marketing by group companies.*

For UK government to do now

- To achieve a lot of what the government says it intends to happen, a lot of work and changes to the law still need to take place. We are tracking what is being implemented. Areas include:
- UK GDPR
- Legacy data
- Adopting existing SCCs for use by the UK
- Transfers out of the UK to the EEA and rest of the world
- UK recognising adequacy arrangements both for the EEA and for non EEA third countries deemed adequate by the EU
- UK adequacy
- EU deemed adequate countries recognising the UK

For you to do now

(* is if there is no UK adequacy)

- Comply with the GDPR
- Understand what GDPR regime applies to your business (UK GDPR, EU GDPR, *Legacy data regime) and which supervisory authorities are involved
- Understand your data flows (ROPA) and locations involved
- *For Legacy data regime, distinguish between personal data collected before 31 December 2020, and also whether it is of UK data subjects or not, and whether processed in the UK or not
- Appoint EU and UK representatives if necessary
- Check whether the UK has recognised the adequacy of the EEA and relevant global locations
- Review your privacy notices, DPIAs and other documentation to update references to EU law, UK-EU transfers and your UK and/or EU representative (if you need one)
- Ensure your DPO will be easily accessible from both your UK and any EEA establishments and has expertise in all regimes
- Consider international data flows (*including from EEA to UK) : medium to large companies:
    - BCRs controller and processor which address processing internally and with customers
    - Hybrid DTA, and
    - SCC+
- Consider international data flows (*including from EEA to UK) : smaller companies:
    - Hybrid DTA, and
    - SCC+

ABOUT CAREERS OUR RESPONSIBILITY MEDIA & PR CLIENT LOGIN

SHOOSMITHS

PEOPLE EXPERTISE INSIGHTS EVENTS CONTACT

Brexit hub

The result of the December 2019 general election has ended the Brexit stalemate in Parliament. The UK's departure from the EU on 31 January 2020 (and end of the transition period only 11 months later on 31 December 2020) means that businesses now have greater clarity on the Brexit timeline, after three and a half years of uncertainty.

However there is still much that remains unknown and preparing for the changes ahead remains challenging for businesses. The detail of a long-term UK-EU trade deal needs to be negotiated and we don't know how comprehensive it will be or if agreement can even be reached, leaving the prospect of a 'no deal' scenario at the end of the year still very much a possibility. The result? While 2020 will see significant milestones in the Brexit process, businesses will still have to monitor developments closely. It is only when

Key contacts

Tony Randle ›

Next webinars:

- The New Immigration Rules – Is your Business prepared for the end of free movement? (11 November)
- Sponsoring EU and non EU nationals post Brexit (25 November 2020)
- Right to Work check changes (9 December 2020)
- Data Protection update TBA in December or early 2021

Any questions?

Brexit and data protection

Thank you and do get in touch

Nick Holland, Co- Head of Privacy

+ 44 (0)7774 975559

+ 44 (0)118 965 8754

nick.holland@shoosmiths.co.uk

Sarah Tedstone, Principal Associate

+ 44 (0)7562 950800

+ 44 (0)121 625 4277

sarah.tedstone@shoosmiths.co.uk