Welcome

Brexit and the EU-UK Trade Deal: what now for Privacy and Data Protection?

SHOOSMITHS

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Nick Holland, Co-Head of Privacy
Nick.Holland@shoosmiths.co.uk
+44 (0) 777 497 5559
+44 (0) 118 965 8754

Sarah Tedstone, Principal Associate
Sarah.Tedstone@shoosmiths.co.uk
+44 (0) 756 295 0800
+44 (0) 121 625 4277

Today’s session

An update on Brexit and data protection

Presenters:

Nick Holland and Sarah Tedstone

4 March 2021

Brexit and privacy timescales

← We are here

31 January 2020: UK left the EU

31 December 2020: transition period ends and UK leaves EU single market and customs union

30 June 2021 UK "third country" if no final adequacy decision

1 January 2021 EU-UK Trade and Cooperation Agreement

19 February 2021 European Commission draft UK adequacy decision

June 2021: UK out in the cold?

"The UK has left the EU, but not the European privacy family"
Věra Jourová, Vice-President for Values and Transparency European Commission 19 February 2021

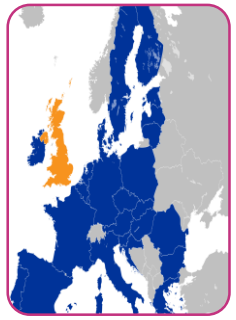
Process and deadlines

It was concluded on 24 December 2020.

It addresses the arrangements following the end of the transition period from 1 January 2021.

Data protection is not dealt with in detail so more is needed (see adequacy later)

It applies for four months and can be extended by two months unless one party objects, or, if earlier, until there is an adequacy finding for the UK



What does it mean for data protection?

It gives a commitment to high data protection standards

It is a “temporary bridge” mechanism for personal data transfers from the EU to the UK, provided that the UK's applicable data protection regime continues.

It provides that cross-border data flows shall not be restricted by implementing data localisation requirements, for example by requiring or prohibiting data storage or processing within either territory

What does the UK say?

The UK regulator, the ICO, has stated that the temporary bridge is "the best possible outcome for UK organisations processing personal data from the EU".

Nevertheless, the ICO recommends that, as a sensible precaution, organisations work with EU and EEA organisations who transfer personal data to them, to put in place alternative data transfer mechanisms, such as standard contractual clauses (SCCs) or Binding Corporate Rules (BCRs), in case there is no adequacy finding by the end of the temporary bridge.

BREXIT INSIGHT WEBINAR

EU-UK Trade and Cooperation Agreement

BREXIT INSIGHT WEBINAR

UK National Data Strategy a different approach in future?

UK as a data haven?

The new strategy is out for consultation so may change before it is finalised. It says:

" Under this strategy, data and data use are seen as opportunities to be embraced, rather than threats against which to be guarded"

but Oliver Dowden Sec State for DCMS writing for the FT on 27 February 2021 said

"We fully intend to maintain those world-class standards. But to do so, we do not need to copy and paste the EU's rule book, the General Data Protection Regulation, word-for-word. Countries as diverse as Israel and Uruguay have successfully secured adequacy with Brussels despite having their own data regimes. Not all of those were identical to GDPR, but equal doesn't have to mean the same. The EU doesn't hold the monopoly on data protection"

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'

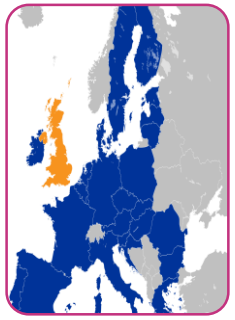
The ICO will not be the supervisory authority

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 2020

There is some debate about whether this is a "frozen" GDPR or not

BREXIT INSIGHT WEBINAR

What does the new UK data protection regime look like?

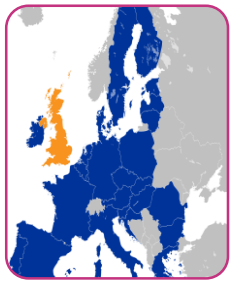
There are two regimes, and possibly temporarily three regimes depending on whether UK adequacy is achieved

Emarketing

PECR rules cover marketing, 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) with the latest draft dated 5 January 2021. The new ePR is not yet agreed. It remains to be seen if and how it will be applied in the UK. The territoriality provisions are likely to mean that the UK will still need to comply

NIS Directive



The NIS Regulations in the UK cover network and information systems and implements the NIS Directive (often called the Cybersecurity Directive). They derive from EU law but are set out in UK law. **They 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 (e.g. SaaS provider), from the end of the transition period you will 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.

For organisations based in the EU offering services in the UK by the end of March 2021 you must appoint a representative in the UK, confirm this with the ICO, and comply with the UK NIS Regulations as well as any local EU interpretations of the Cybersecurity Directive

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 and **will continue to apply.** The UK has also independently signed up to the underlying international treaty on access to environmental information (the Aarhus Convention).

BREXIT INSIGHT WEBINAR

What about Emarketing, NIS Directive, FOIA and EIR?

BREXIT INSIGHT WEBINAR

What about cookies and consent?

- *In situations where the EU GDPR applies, organisations will be bound by EU Member State Laws and ongoing guidance. Local rules may also apply. The European Data Protection Board "EDPB" has issued guidance on consent, and CNIL, the French regulator, has updated its guidance on cookies with a deadline of 31 March 2021 to comply. The ICO has yet to clarify its position.*
- *In situations where sites can be accessed around the world, this can be a complex legal area to navigate. The status of EDPB guidance will vary depending on location.*
- *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.*

"CONCLUSION

(266) The Commission considers that the UK GDPR and the DPA 2018 ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(267) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in United Kingdom law enable infringements to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.

(268) Finally, on the basis of the available information about the United Kingdom legal order, the Commission considers that any interference with the fundamental rights of the individuals whose personal data are transferred from the European Union to the United Kingdom by United Kingdom public authorities for public interest purposes, in particular law enforcement and national security purposes, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

(269) Therefore, in the light of the findings of this Decision, it should be decided that the UK ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union.

(270) This conclusion is based on both the relevant UK domestic regime and its international commitments, in particular adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights. Continued adherence to such international obligations is therefore a particularly important element of the assessment on which this Decision is based."

SHOOSMITHS

BREXIT INSIGHT WEBINAR

European Commission draft UK adequacy decision

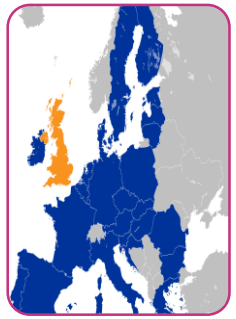
Adequacy means a decision that the jurisdiction offers an essentially equivalent level of data protection

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)

BREXIT INSIGHT WEBINAR

UK Adequacy

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.”

What are some of the risk factors against a final UK adequacy decision?:

- UK use of mass surveillance techniques
- UK membership of the Five Eyes intelligence sharing community
- UK potentially diverging from the EU on data protection
- 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

BREXIT INSIGHT WEBINAR

UK No Adequacy

Adequacy decisions are subject to periodic review, revocation by the European Commission or challenge in the European Court of Justice

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

BREXIT INSIGHT WEBINAR

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 in 2021. It has produced an amended version of the existing EU SCCs to make sense in a UK context

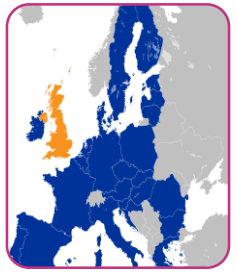
At some point EU SCCs may be invalid for transfers from the UK

NEW EU SCCs

The European Commission is consulting on draft amended SCCs proposed in November 2020. 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 decision is awaited (possibly in March). 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

BREXIT INSIGHT WEBINAR

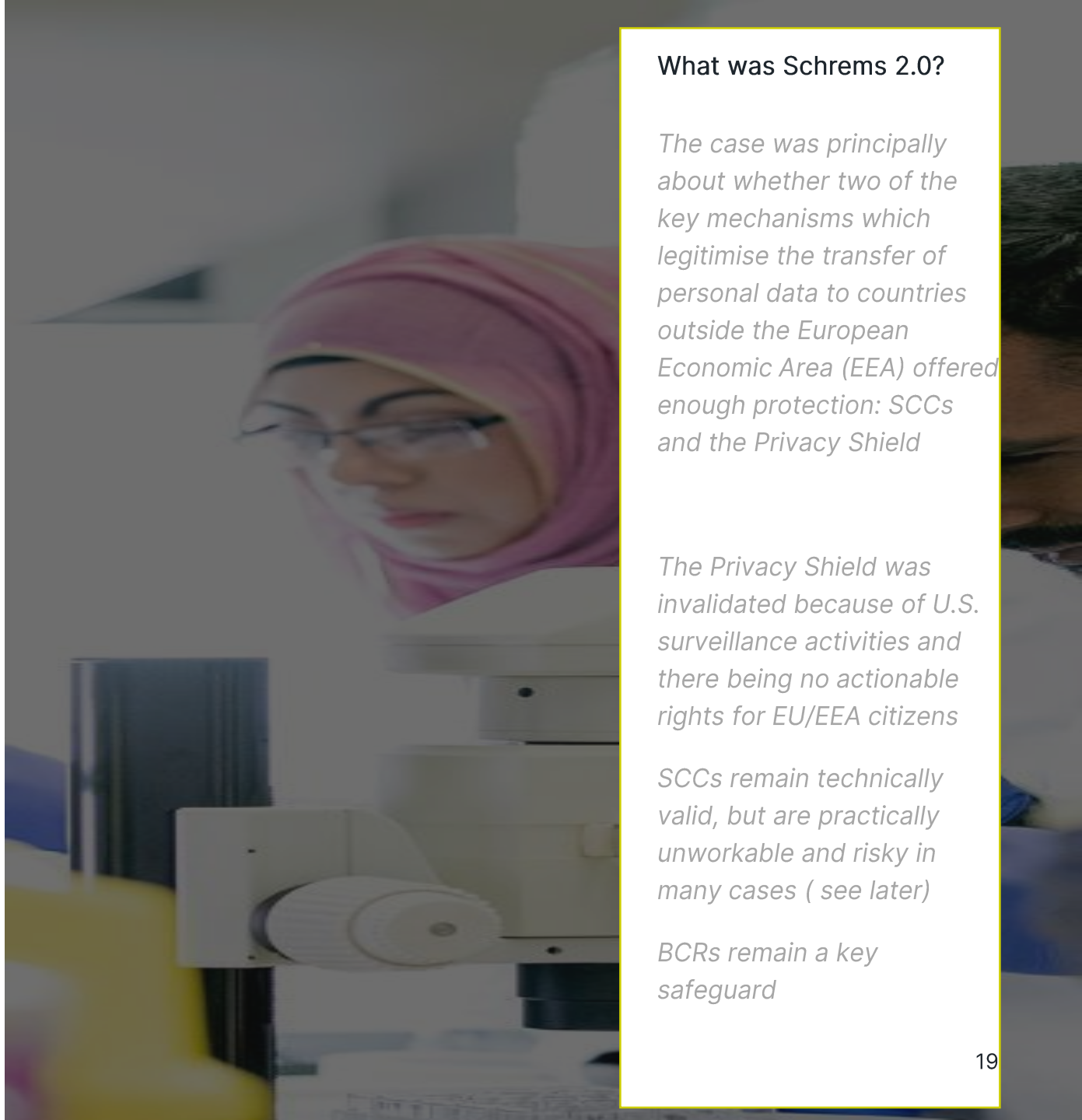
Transfers needing safeguards

See later especially SCC+

Schrems 2.0 and Brexit

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
- See later SCC+



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 (see later)

BCRs remain a key safeguard

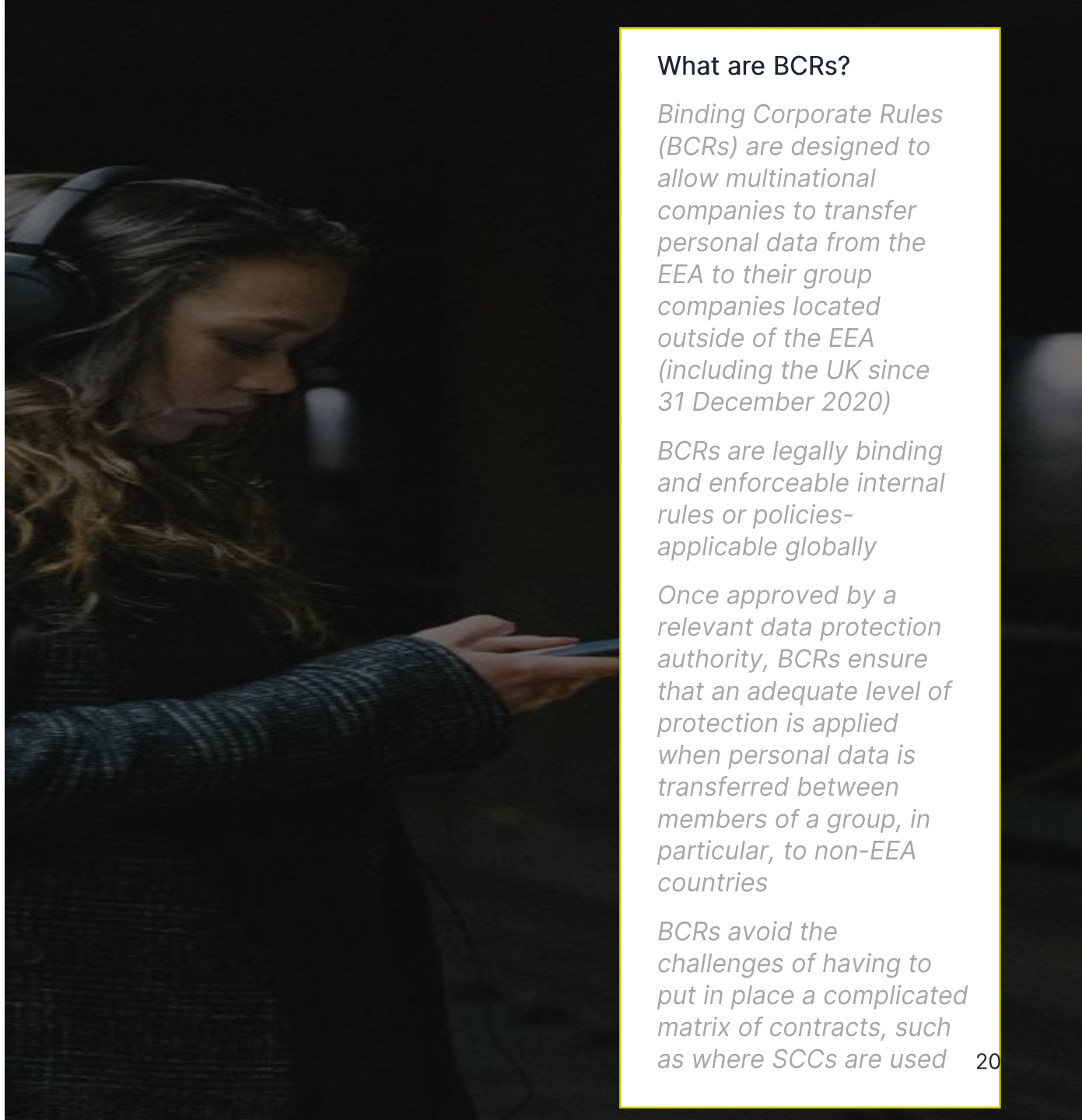
BCRs

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 may 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

UK Representative

- Analogous to EU Representative requirement

- Applies from 1 January 2021 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

- Applies whether or not a UK 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

Shoosmiths' UK Representative Service

- This is a fixed price, platform-based service, and available to any business.
- It is provided by Shoosmiths Privacy Services (a subsidiary of Shoosmiths LLP).
- Visit www.shoosmiths.co.uk/dataprivacyrep

SHOOSMITHS

BREXIT INSIGHT WEBINAR

DPOs

If you are currently required to have a DPO, that requirement will continue, whether under the UK GDPR, or EU GDPR. 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.

BREXIT INSIGHT WEBINAR

One-stop shop and enforcement

- If your UK business carries out any cross-border processing involving the EU/EEA, it used to benefit 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.
- If you continue any cross-border processing, your 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 version of the GDPR, although cooperation is still anticipated. It remains to be seen how this will work
- Companies can face investigation by EU and UK regulators and potential fines from each of them

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

Watch out for these webinars as things develop:

- International transfers: the new EU SCCs
  End of March/April
- Global privacy program: practical tips
  May /June2021
- Brexit and Data Protection: the Finale?
  July 2021 (depending on UK adequacy decision)

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Nick Holland, Co-Head of Privacy
Nick.Holland@shoosmiths.co.uk
+44 (0) 777 497 5559
+44 (0) 118 965 8754

Sarah Tedstone, Principal Associate
Sarah.Tedstone@shoosmiths.co.uk
+44 (0) 756 295 0800
+44 (0) 121 625 4277

Thank you

Visit our events page:
https://www.shoosmiths.co.uk/insights/events

SHOOSMITHS