Welcome

Charities and data protection: Brexit, the new EU SCCs and guidance, what do we do now?

This webinar will begin at 10:30

SHOOSMITHS

Your host

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

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

Today’s session

- The new data protection regimes
- International data transfers
- Legacy managers’ work
- What else is new?

Presenter:

Sarah Tedstone

8 July 2021

Brexit impact on Legacy Managers' work

What does the new UK data protection regime look like?

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

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

UK representative needed

The 'EU GDPR': the original GDPR

The ICO will not be the supervisory authority

EU representative needed

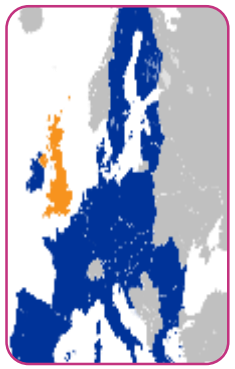
Scope:

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

Brexit and International Data Transfers

UK Adequacy



What does it mean?

Data flows between the EEA and the UK can flow freely and are safeguarded

The decision will last for up to 4 years and will be reviewed

International Data Transfers

Safeguards: New SCCs

Safeguards may be needed for international personal data transfers depending on the locations involved

List of countries deemed already adequate by the EU and UK and not needing safeguards: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK and Uruguay.

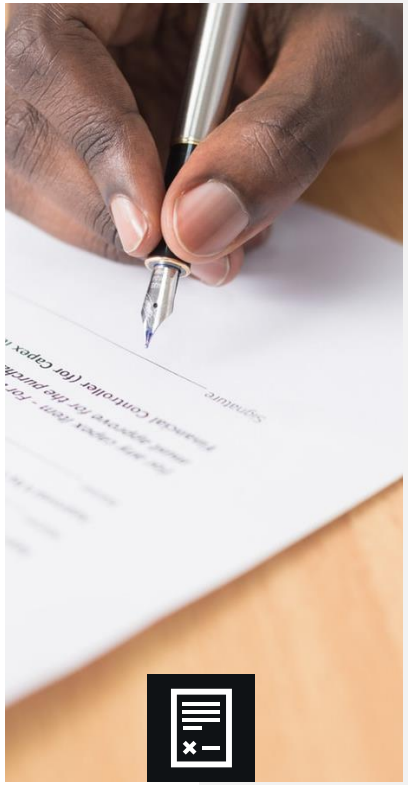
BCRs are the gold standard

Privacy Shield was critical for EU-US transfers but is invalidated

SCCs are EU-approved template terms which ensure GDPR standards are met provided the terms are respected. New EU SCCs with guidance require significant work by 27 September. New UK SCCs are awaited

SCCs: the new versions and guidance: pros and cons

New final SCCs were published on 7 June 2021 New final guidance is now available



Standard Contractual Clauses (SCCs)

- Now modular multi-party possibilities to cover combinations of four scenarios:
  - controller-controller
  - controller-processor
  - processor-processor
  - processor to controller
- Suitable for data exporters not located within the EU but caught by the GDPR terms.
- Processor mandatory terms under Art 28
- Schrems 2.0 risks covered
- Time periods: 27 September 2021 for all new contacts and amendments. 27 December 2022 for all existing contracts
- Wider responsibilities to understand the chain of processing from the ultimate controller to the last sub-processor
- Tougher notification requirements to parties in the processing chain and EU data protection authorities
- They involve creating a contract from relevant choices and an assessment of wider risks and laws involved. Inserting them by reference into a contract will no longer be possible
- Data protection authorities are expected to 'up their game' on enforcement and there are indications that this is happening
- We are seeing stakeholders take a much keener interest in the detail as we predicted in July 2020
- The parties give warranties that they have no reason to believe that local laws and practices in the data importer's country prevent compliance. There is now additional guidance about this
- The EU guidance has further clarified the SCC+ assessment exercise. Understand the SCC obligations. They require significant vigilance, legal advice, ongoing monitoring and action
- There are also new SCCs for controller to processor contracts generally giving some certainty about these common terms

Brexit and International Data Transfers

What about Marketing and eMarketing?

Marketing

UK GDPR

ICO guidance

Code of Fundraising Practice

ILM guidance

Draft Direct Marketing Code of Practice

eMarketing

PECR rules cover eMarketing, cookies and electronic communications. They derive from EU law but are set out in UK law. **They continue to apply in the UK**

The EU is replacing the current e-privacy law with a new e-privacy Regulation (ePR) 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

Brexit and International Data Transfers

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 trackers 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.*

No specific ICO rules for charities

Charity Commission (OSCR/CCNI)

Fundraising Regulator

Other Supervisory Authorities

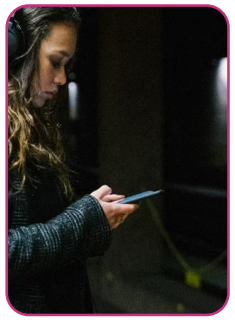
Communications and data processing

Where PECR requires consent, consent must be obtained and used as the lawful basis under GDPR and to a GDPR standard (positive specific opt in consent)

Where PECR does not require consent, another lawful basis under GDPR can be used such as legitimate interests

If legitimate interests is being relied on as the lawful basis for processing a Legitimate Interests Assessment should be undertaken and recorded

When does PECR require consent for marketing individuals?



Text

Email

Recorded calls

Legacy managers' work

Legitimate interests or consent?

5

- Specifically requested
- Post
- Live calls
- Researching prospects/legacy profiling and bought in lists
- Individual v corporate
- Marketing v service and other admin messages
- Encouraging professionally written legacies in wills v encouraging professionals to include legacies in wills
- Testator v prospective testator
- Sharing with other charities and fighting fraud
- Estate family members
- Renewing consent
- Sensitive personal data

Legacy managers' work

Legitimate interests or consent?

5

What do you do now?

- Understand what GDPR regime applies 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. **Shoosmiths has an Automated Privacy Compliance digital data mapping tool to make this painless**
- Appoint EU and UK representatives if necessary- **this is mandatory**
- Assess your appropriate lead supervisory authority
- Update your BCRs and apply for UK BCRs as needed
- Keep track of privacy law changes – existing EU SCCs, new EU SCCs and UK SCCs. **Contracts may need to be renewed.**
- Review your privacy notices, DPIAs, contracts 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?

Between the EEA and the UK and all other “adequate” locations:

Data likely to flow freely but some review is needed

Between the rest of the world and the EEA and UK where safeguards are needed:

- Likely options medium to large charities:
    - BCRs controller and processor which address processing internally and with others
    - Hybrid DTA, and
    - SCC+ : Shoosmiths has a Transfer Risk Assessment solution
- Likely options smaller charities:
    - Hybrid DTA, and
    - SCC+: Shoosmiths has a Transfer Risk Assessment solution

What else is new?

- Data Sharing Code: organisations both using personal data for their own different purposes now should include details of the agreements about data sharing
- Children's Code: from September 2021 new rules about websites and online services that may be used by children. 15 new standards
- Updated Criminal Conviction Guidance: wider than previously thought
- Updated Data Subject Access Rights Guidance
- Updated controllers and processors guidance: contracts with third parties may need a review

Watch out for these webinars as things develop:

- Brexit, SCCs and Global Data Protection August 2021

  UK Children's Code September 2021

  Data Protection contracts: controllers and processors October 2021

Any questions?

Your host

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

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