
DPPC 2024
EMPOWERING YOU
THROUGH INFORMATION
ico.
Information Commissioner's Office
#DPPC24
ico.org.uk/DPPC

Going stateside: transferring data to the US

DPPC 2024

ico.
Information Commissioner's Office

Agenda

1. The UK-US Data Bridge

   What is the UK-US Data Bridge and how is it used in practice?

2. Transferring data to entities not registered under the UK-US Data Bridge

   What are the article 46 transfer methods, how can you streamline the TRA process when using them, and when can you rely on article 49 derogations?

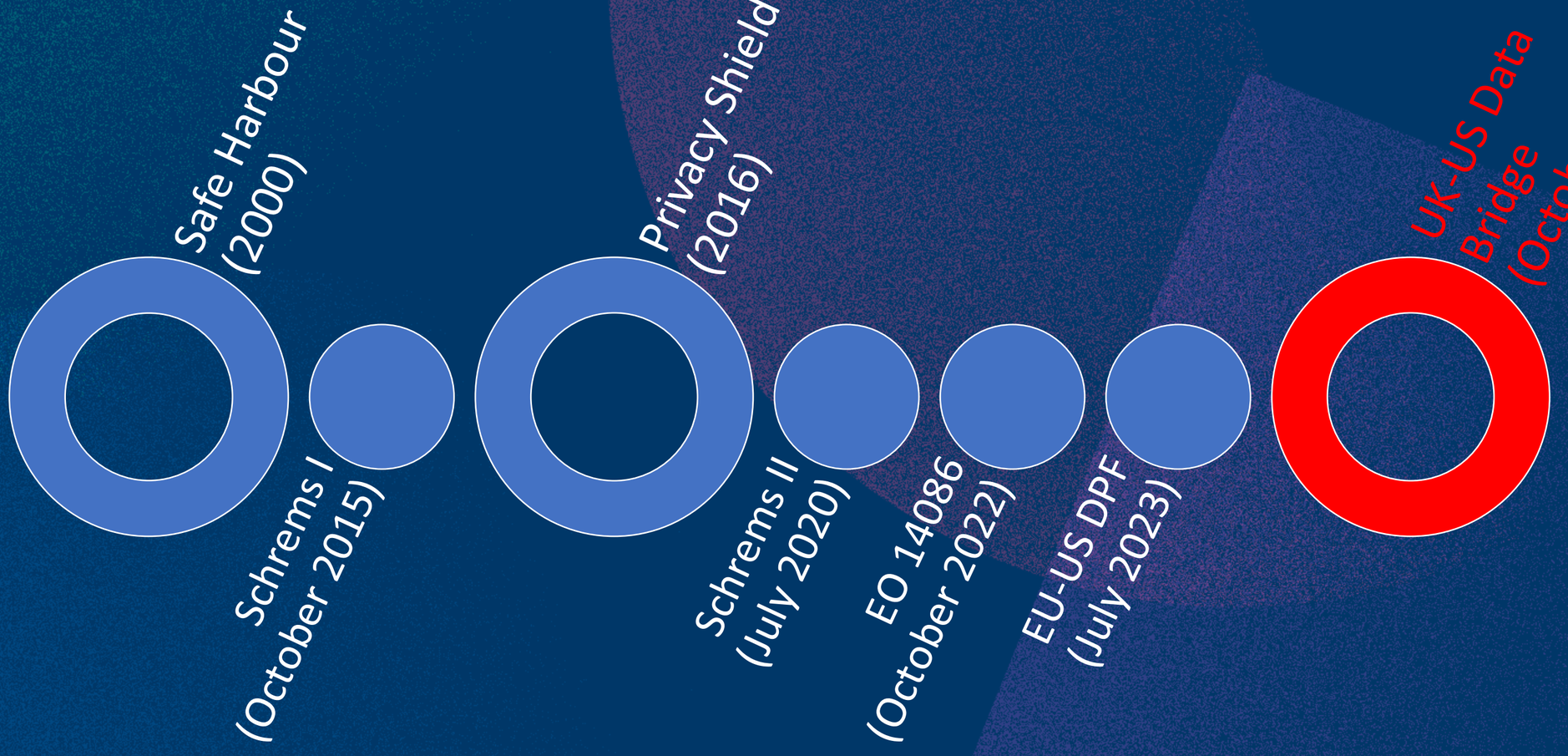
3. Q & A

Your presenters

Emma Bate Director of Legal Service

Kitty Rosser Principal Lawyer (Data Privacy Advice)

Background to the UK-US Data Bridge



Poll 1

Have you used the UK-US Data Bridge to send personal data to the US?

- ❑ Yes
- ❑ No – we use other transfer mechanisms
- ❑ N/A – we do not transfer data to the US

The UK-US Data Bridge – a (partial) adequacy decision

- The *Data Protection (Adequacy) (United States of America) Regulations 2023* came into force 12 October 2023 creating the UK-US Data Bridge
- AKA UK Extension to the EU-US Data Protection Framework
- The *Regulations* were made under s17A DPA 18 and are a **partial** adequacy decision under article 45 UK GDPR
- Only applies to US organisations that have self-certified under the EU-US DPF and the UK Extension
- Only US entities subject to the jurisdiction of the US FTC or DoT can certify – excludes eg banks, telecommunication companies, non-profits, public bodies
- Search at https://www.dataprivacyframework.gov/list

How is PD protected under the UK-US Data Bridge?

- Administered by the International Trade Administration (ITA), part of the US DoC
- Participation is voluntary but effective compliance once certified is compulsory
- Certified organisations must adhere to 7 core principles and 16 supplemental principles
- Must publicise certification in privacy policy
- Multi-layer recourse and enforcement mechanism:
  - Direct engagement
  - Use of Independent Recourse Mechanism
  - complaint to ICO
  - binding arbitration
  - government enforcement by FTC or DoT

Exiting the UK-US Data Bridge

	Withdrawn/lapsed certification	Removed by DoC
Retain data, continue to apply principles, make annual affirmation to ITA	✓	✗
Retain data, provide protection by other authorised means	✓	✗
Return or delete all data transferred under the UK-US Data Bridge	✓	✓

Using the UK-US Data Bridge in practice

1. Check the register at https://www.dataprivacyframework.gov/list:
    - Does your recipient appear on the register?
    - Is your recipient registered under the UK Extension?
    - Is the registration status active?
    - Does the registration cover HR data (if relevant)?
2. Confirm that no journalistic data is being transferred
3. Identify and clearly flag any special category data/criminal records data to your recipient
4. Ensure an Article 28 DPA or a data sharing agreement is in place where needed
5. Ensure you update relevant records, policies, DPIAs, and privacy notices as needed to comply with your accountability and transparency obligations

The ICO's role

- During the implementation process…
  - The ICO provided advice to Government during its assessment of the UK-US Data Bridge and published its formal opinion once the implementing Regulations were laid (available on the ICO website www.ico.org.uk)
  - The ICO considered that it was reasonable to conclude that the UK-US Data Bridge provides an adequate level of protection but identified 4 areas of potential concern requiring ongoing monitoring
- Following implementation…
  - The ICO provides a specific complaints service and publishes accompanying guidance
- In the future…
  - The ICO will provide advice to Government during its review of the UK-US Data Bridge (to take place not less than once each 4 years)

Will the UK-US Data Bridge last?

- Subject to review every 4 years under s17B DPA 18
- No legal challenges in the UK or complaints to the ICO to date
- Potential impact of a challenge to the EU-US DPF on the UK-US Data Bridge?
- Note US presidential elections

Case study – part 1

A UK retail company is purchased by a large US corporate group. The UK retail company is required to provide monthly sales reports to its new US parent company. These reports include a small amount of personal data.

The UK retail company checks the DPF register and sees that the US parent company is certified to the EU-US DPF and the UK Extension. It is not registered to accept HR data. The UK retail company confirms that no HR data is included in the monthly sales report and decides that it can rely on the UK-US Data Bridge to make the transfer.

The UK retail company updates its article 30 ROPA and its customer privacy notice to record that it is relying on the UK-US Data Bridge.

Poll 2

What mechanism do you most commonly use when transferring personal data to the US?

- ❑ UK-US Data Bridge
- ❑ IDTA
- ❑ SCCs with Addendum
- ❑ Other article 46 appropriate safeguards
- ❑ Article 49 derogations
- ❑ N/A – we don’t transfer personal data to the US

Article 46 appropriate safeguards

If you cannot use/do not wish to use the UK-US Data Bridge, consider whether you can use an article 46 appropriate safeguard mechanism

The most used mechanisms are the IDTA and EU SCCs with Addendum

You **must** complete a TRA

Poll 3

What is your approach when completing a TRA?

- ❑ We follow the EDPB guidelines
- ❑ We use the ICO’s TRA Tool
- ❑ We outsource to external DPO or lawyers
- ❑ Other
- ❑ N/A – we don’t transfer personal data/use article 46 appropriate safeguards

Using the DSIT analysis when completing the TRA

- DSIT undertook a detailed analysis to assess whether the UK-US Data Bridge together with other relevant laws and practices in the US would provide an adequate level of protection for UK personal data
- The DSIT analysis addresses application of US laws and practices more generally and mirrors the issues to be addressed as part of a transfer risk assessment (TRA)
- The ICO considers that organisations can incorporate the DSIT analysis into their own transfer risk assessments (TRAs) by reference rather than repeating the analysis themselves
- Organisations must still record that they have completed a TRA and keep it under review
- Detailed guidance can be found on the international transfers guidance page on our website

Relying on derogations under article 49

- It may be particularly relevant to consider derogations if:
  - You cannot use/do not wish to use the UK-US Data Bridge
  - It is not possible to implement an article 46 mechanism
  - Your TRA contains unmitigated high risks for some data
- There are 8 derogations set out at article 49 UK GDPR
- 6 of the exemptions require that you conduct a necessity assessment
- See the guidance on the international transfers page of our website

Case study – part 2

The UK retail company wishes to take advantage of the centralised HR services offered by its new US parent company. It cannot transfer HR data under the UK-US data Bridge because the US parent company's DPF certification does not cover HR data.

The UK retail company completes a TRA, relying on the DSIT Analysis, and enters into the IDTA with its US parent company. These cover the transfer of HR data only as the UK retail company continues to rely on the UK-US Data Bridge to send its monthly sales reports.

The UK retail company updates its article 30 ROPA and its employee privacy notice.

Questions?

ico.org.uk/DPPC

#DPPC24

Keep in touch

Subscribe to our e-newsletter at ico.org.uk or find us on...

#DPPC24

ico.org.uk/DPPC

DPPC 2024

ico.
Information Commissioner's Office