Deloitte.

Deloitte regulatory news alert

Data Transfers: Managing Uncertainty – EU-US Privacy

10 February 2016

Since the Court of Justice of the EU nullified the EU-US Safe Harbor Framework on 6 October 2015, the European Commission and the US Department of Commerce have worked to establish **a new legal framework to govern transfers of personal data** from the EU to the US. On 2 February, negotiators from both sides announced a political agreement on a new arrangement called "EU-US Privacy Shield" to replace the invalidated Safe Harbor.

The EU's Data Protection Authorities (DPAs) will analyse in the next months whether the EU-US Privacy Shield sufficiently addresses the issues raised by the Court and whether it offers sufficient protection of EU citizens' fundamental rights. In light of the Court's ruling, the **regulators are also questioning the robustness of alternative data transfer mechanisms** such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs). For now however, these alternative mechanisms remain valid for transfers to the US.

The **legal uncertainty** surrounding EU-US personal data transfers **is hence set to continue** until the Data Protection Authorities have completed their assessment of the EU-US Privacy Shield, on which they are expected to communicate in **April 2016**. This article provides a state of play of the remaining options for transferring personal data to the US, as well as recommended next steps to manage the current legal uncertainty surrounding data transfer strategies.

The EU-US Privacy Shield

On 2 February 2016, the European Commission announced a **political agreement** with the US Department of Commerce on a new transatlantic data transfer arrangement to replace the invalidated Safe Harbor framework. The new framework, called "**EU-US Privacy Shield**", will provide EU citizens with several options to exercise their right of redress in the US, including with regards to the use of their data by US national intelligence authorities. The US has reportedly also given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to "clear limitations, safeguards and oversight mechanisms". To ensure that this arrangement is not simply a one-off decision like Safe Harbor, an annual review process will also be established.

Deloitte.

Core points of the agreement

- Strong obligations on companies handling EU citizens' personal data, and robust enforcement and monitoring by the US Department of Commerce and the US Federal Trade Commission.
- Clear safeguards and transparency obligations on US government access to personal data and assurance for the respect of the principles of necessity and proportionality.
- Effective protection of EU citizens' rights with several redress possibilities in front of the Department of Commerce, the Federal Trade Commission, an independent Ombudsperson and the installation of an alternative dispute resolution mechanism that is free of charge. Furthermore, companies will be given deadlines to respond to complaints.

An overview of your options

The EU's Data Protection Authorities issued a statement on 3 February to stress that further analysis of the new Privacy Shield deal is needed to assess whether the arrangement sufficiently addresses the issues raised by the Court of Justice of the EU in the Schrems case. The Article 29 Working Party hopes to receive the official documents related to the EU-US Privacy Shield by the end of February, and is scheduled to analyse the deal in the first weeks of March 2016.

While alternative transfer mechanisms such as **Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) remain valid options** for personal data transfers to the US, the regulators announced that they are assessing "the robustness" of these mechanisms as well in light of the Schrems ruling. **By April 2016**, the Working Party will provide **clarity on the validity of all three options**: BCRs, SCCs and the new EU-US Privacy Shield. The tables below give a general overview of the possible ways to transfer personal data from the EU to the US, with their respective common advantages and drawbacks.

Safe Harbor

Advantages	Disadvantages
- Minimal certification cost - Compliance implies integration of the Safe Harbor privacy principles in the organisation's policies & procedures	- Invalidated by the Court of Justice of the EU ruling - Only covers data transfers from EU/Switzerland to the US Safe Harbor certified company - Provides the US FTC with enforcement powers

Accepted by DPAs?

No. Invalidated by the CJEU in the Schrems v. Data Protection Commissioner case (C-362/14). DPAs consider it illegal to rely on Safe Harbor and will handle cases and complaints about organisations on a case-by-case basis.

Binding Corporate Rules

Advantages	Disadvantages
- Compliance integrates EU privacy requirements into the core policies & procedures of a corporate group - One solution for all data transfers outside the EU within the corporate group (not just to the USA)	- Long approval process, requires extensive documentation and resources - Strong privacy governance (responsibilities) required - The EU headquarters can be held accountable for BCR non-compliance of non-EU group entities who received EU data

Accepted by DPAs?

Yes. Accepted by all DPAs until Art. 29 Working Party has completed analysis of EU-US Privacy Shield (expected in April 2016). However Germany, Hungary and Portugal are not currently accepting new BCR applications.

Standard Contractual Clauses (EU Model Contracts)

Advantages	Disadvantages
- Requires no drafting of contractual clauses – mandatory contractual clauses are available online - Pre-approved by DPAs, so far never challenged	- Only useable for well-defined transfers - Contractual administration challenges at time of signature and in case an update is needed - Risk of creating a paper tiger: Strong contractual guarantees, without compliance in practice

Accepted by DPAs?
Yes. Accepted by all DPAs until Art. 29 Working Party has completed analysis of EU-US Privacy Shield (expected in April 2016).

Ad-hoc data transfer agreements

Advantages	Disadvantages
- More drafting flexibility than EU Model Contracts - Easier to adapt to changing transfers	- More drafting time and resources needed - Approval of DPAs needed and not guaranteed

Accepted by DPAs?
Yes. By all DPAs except Germany's, until Art. 29 Working Party has completed analysis of EU-US Privacy Shield (expected in April 2016).

Derogations in the law (e.g. consent)

Advantages	Disadvantages
- Clear exceptions provided in EU Data Protection Directive (EC/95/46)	- Derogations interpreted restrictively, not a stable solution - Likely only accepted if the transfer is neither massive nor frequent - Consent needs to be informed, specific and freely given, which is in many cases very hard if not impossible to obtain

Accepted by DPAs?
Only if strict conditions (informed, specific and freely given) are fully met, and not for repeated, mass or structural transfers.

Recommendations

Stay Calm

For now, we strongly recommend to verify whether any personal data transfers to the US in your organisation are still based on the invalidated Safe Harbor framework. To that **end,gather existing documentation on your data processing operations and transfers** to evaluate internal and third party Safe Harbor risk exposure and prepare for potential inquiries from DPAs, clients, employees, and/or Works Councils. In addition, it may be a good idea to identify and empower an individual within your organisation to be the contact point (internal and external) on Safe Harbor issues.

Evaluate

Based on this information, assess whether using any of the **remaining options for transferring data to the US** would be viable in your specific situation, and develop a road map to implement changes to your privacy program accordingly. In addition, verify whether Safe Harbor-reliant third parties with whom your organisation shares personal data have taken action as well. Finally, verify whether you need to update any registrations of processing activities towards the Data Protection Authorities. This demonstrates that you are taking a proactive approach and can prevent unwanted queries from regulators.

Deloitte.

Prepare

As for the long-term viability of alternative transfer mechanisms, beyond April 2016, the future remains uncertain. We recommend therefore to focus on elements that can show to DPAs that the CJEU's message was taken into account in your organisation. Assess whether you are able to justify why the cross-border transfer is necessary, and if possible even whether the transfer benefits the data subject. Transparent privacy policies and procedures, well-documented Privacy Impact Assessments and data retention policies as well as IT security measures such as end-to-end encryption can help build your case for sustained transatlantic data transfers in the future.

Your contacts

Roland Bastin
Partner | *Information & Technology Risk*
Tel: +352 451 452 213
rbastin@deloitte.lu

Laurent de la Vaissière
Director | *Information & Technology Risk*
Tel: +352 451 452 010
ldelavaissiere@deloitte.lu

Irina Hedea
Director | *Information & Technology Risk*
Tel: +352 451 452 944
ighedea@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg