



## Navigating the Safe Harbor storm EU-US Privacy

Since the [Court of Justice of the EU nullified the EU-US Safe Harbor Framework](#) on October 6<sup>th</sup>, businesses, regulators and European rule makers have been working hard to put together an appropriate response.

This article aims to summarize the events of the past month and assesses the different remaining options for transferring personal data from the EU to the US.

## European Commission: Working towards Safe Harbor 2.0

Immediately after the ruling, the European Commission, which has the power to declare other countries safe enough to transfer personal data into, emphasized that it has been working with the US on a new Safe Harbor framework since 2013. At the same time, Justice Commissioner Vera Jourová stressed that **alternative transfer mechanisms** for data exports to the US, such

as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (i.e. EU Model Contracts), were **still valid** and would remain viable options. In addition, the Commissioner called upon the EU's 28 data protection regulators to work together on a uniform interpretation of the ruling, to ensure business certainty and the continuation of Transatlantic data flows, which she called "the backbone of the European economy".

On November 6<sup>th</sup>, the Commission issued its [announced guidance](#) on how to transfer data to the EU after the invalidation of Safe Harbor, in which it again confirmed that the alternative data transfer mechanisms remain valid options. The guidance document however also stressed that data exporters using BCRs or Model Contracts are responsible for ensuring that transfers take place with sufficient safeguards. This may entail taking technical, organizational, business-model related or legal measures, or suspending the transfer altogether. Ultimately, the Data Protection Authorities (DPAs) have to assess, in full independence and on a case-by-case basis, whether sufficient safeguards are in place to approve a transfer based on alternative transfer mechanisms. The European Commission will however work with the DPAs to ensure a uniform application of data protection law across the EU.

The Commission further stated that its objective is to conclude the negotiations with the US on a **new framework** to replace Safe Harbor **within 3 months**. In a [statement to the European Parliament](#) on October 26<sup>th</sup>, Commissioner Jourová had already revealed that the EU and US had reached agreement in principle on key elements of the new Safe Harbour framework, but admitted that provisions regarding the possible access of data by public authorities for law enforcement and national security purposes remains the biggest challenge in the negotiations.

## Regulators set January 2016 deadline for negotiations; accept alternative transfer options for now

According to the EU's privacy regulators (Data Protection Authorities or DPAs), the accessing of European personal data by US intelligence services which Commissioner Jourová alluded to, is key to understanding the CJEU's ruling. In a [common statement](#) on October 16<sup>th</sup>, the DPAs called upon the EU Member States and the European Commission to find "political, technical and legal solutions" that enable data transfers to the US, whilst respecting fundamental rights. The DPAs acknowledged that a new Safe Harbor framework could be a part of the solution, but set strict requirements for it to be acceptable as well as a clear deadline for the negotiations. If by January 31<sup>st</sup> 2016 no solution is found, the regulators will take "all **necessary and appropriate actions**, which may include coordinated enforcement actions".

The DPAs also called into question whether alternative transfer mechanisms will still be valid in the future, as BCRs or EU Model Contracts do not protect European data subjects from "massive and indiscriminate surveillance" either. In their common statement, the DPAs

committed to accepting these alternatives at least until the end of January 2016. However, the **DPAs of Germany** have [unilaterally deviated](#) from this standpoint, announcing that they will **no longer issue new authorizations for data transfers to the United States** that are based on BCRs or ad-hoc data transfer agreements.

## An overview of your options

In an attempt to provide clarity, the following tables 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.

The below list provides an overview of how things stand as of November 11<sup>th</sup> 2015. Due to the volatile legal climate, this assessment may change quickly, following for example guidance issued by the European Commission, the evolution of the negotiations on a new Safe Harbor framework, or a re-assessment of BCRs and Model Contracts by the data protection authorities (DPAs). The Safe Harbor ruling will be a key topic during a meeting that Commissioner Jourova will have with her US counterpart in Washington DC in the week of **November 17<sup>th</sup>**. In addition, the Article 29 Working Party, which convenes all the DPAs of EU Member States, will discuss the Safe Harbor fall-out again at the **end of November**.

### Safe Harbor

Advantages	Disadvantages
<ul style="list-style-type: none"><li>• Minimal certification cost</li><li>• Compliance implies integration of the Safe Harbor privacy principles in the organization's policies &amp; procedures</li></ul>	<ul style="list-style-type: none"><li>• Invalidated by the Court of Justice of the EU ruling</li><li>• Only covers data transfers from EU/Switzerland to the US Safe Harbor certified company</li><li>• Provides the US FTC with enforcement powers</li></ul>

### Accepted by DPAs?

No. Invalidated by the CJEU in the Schrems v. Data Protection Commissioner case (C-362/14).

---

## Binding Corporate Rules

### Advantages

- Compliance integrates EU privacy requirements into the core policies & procedures of the group
- 1 solution usable for all data transfers outside the EU (not just to the USA)

### Disadvantages

- 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. By all DPAs except Germany's, until at least January 31<sup>st</sup> 2016.

## Standard Contractual Clauses (EU Model Contracts)

### Advantages

- Requires no drafting of contractual clauses – mandatory contractual clauses are available online
- Pre-approved by DPAs, so far never challenged

### Disadvantages

- 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 at least January 31<sup>st</sup> 2016.

## Ad-hoc data transfer agreements

### Advantages

- More drafting flexibility than EU Model Contracts
- Easier to adapt to changing transfers

### Disadvantages

- More drafting time and resources needed
- Approval of DPAs needed and not guaranteed

### Accepted by DPAs?

Yes. By all DPAs except Germany's, until at least January 31<sup>st</sup> 2016.

## Derogations in the law (e.g. consent)

### Advantages

- Clear exceptions provided in EU Data Protection Directive (EC/95/46)

### Disadvantages

- 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

For now, we strongly recommend to verify whether any personal data transfers to the US in your organization are still based on the invalidated Safe Harbor framework. If this is the case, you should consider reviewing your overall data transfer strategy and assess whether any of the remaining options for transferring data to the US would be viable in your specific situation.

As for the long-term viability of alternative transfer mechanisms, beyond January 2016, the future is uncertain. We recommend therefore to focus on elements that can show to DPAs that the CJEU's message was taken into account in your organization. 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 data minimization strategies and data retention policies as well as IT security measures such as end-to-end encryption should help build your case for sustained transatlantic data transfers in the future.

## Contact us

For data transfer strategy advice tailored to the needs of your organization, please contact [Erik Luysterborg](#) or [Georgia Skouma](#).

[Homepage](#)



[Deloitte Belgium](#)

Berkenlaan 8A, 8B, 8C  
1831 Diegem  
Belgium

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 200,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015. For information, contact Deloitte Belgium.

To no longer receive emails about this topic please send a return email to the sender with the word "Unsubscribe" in the subject line.