Safe Harbor agreement is dead. What now?

October 7, 2015

On 6 October 2015, the European Court of Justice ruled on the case *Maximillian Schrems v Data Protection Commissioner*. This ruling has two important parts.

- The Court declared the EU Commission's decision on the adequacy of the EU-US Safe Harbor arrangement invalid with immediate effect.
- The Court underlined the greater powers of national data protection authorities in supervising outbound transfers of personal data, even if based on adequacy decisions of the European Commission.

As a consequence of the ruling, the Safe Harbor arrangement is rendered ineffective. Also, other mechanisms for transferring personal data to non-adequate countries, such as the EU model contractual clauses or binding corporate rules, will likely become subject to a higher level of scrutiny of European data protection authorities, in particular if they are used for transfers to the US. Following the Court's ruling, companies are advised to analyse which of their data transfers are based on Safe Harbor and distinguish between data transfers through US based cloud and outsourcing providers, and internal data transfers. We also advise not entering into any new contracts that refer to Safe Harbor.

Background

EU data protection law prohibits transfers of personal data to countries outside the EU where protection of personal data does not comply with EU standards – including the US. Those transfers may only take place if one of the transfer mechanisms set out in data protection law is used. For data transfers to the US, the EU-US Safe Harbor Framework was agreed in 2000 and formalised by the European Commission's (EC) decision 2000/520/EC. This EC decision 2000/520/EC was declared invalid by the ECJ.

Guidance expected in mid-October

The EC will shortly issue guidance for those businesses affected on how to proceed. The EC also confirmed it will speed up the negotiations with the US on the renewed Safe Harbor agreement. In the meantime, it is up to the European data protection authorities to investigate individual claims about unlawful data transfers and impose sanctions.

The Court's decision reiterated the investigatory and enforcement powers of national DPAs in ensuring protection of personal data on their territories and overseeing outbound data transfers. The first reactions of the national data protection authorities are very mixed – from a relaxed "it will take time to comply" by the UK's Information Commissioner to the German DPAs' self-pronounced readiness to enforce strictly.

To avoid fragmented application of law by national data protection authorities, the Article 29 Working Party (that includes all EU data protection authorities) will meet on 8 October 2015 to analyse the consequences of the ECJ's decision. The Article 29 Working Party will also outline a common position regarding investigating and suspending transfers that are non-compliant with the adequacy requirements.

Analyse your transatlantic data flows

Following the ECJ's ruling, companies are advised to analyse which of their data transfers are based on Safe Harbor. In doing so, a distinction can be made between

- data transfers through US based cloud and outsourcing providers and
- internal data transfers.

Data processing by US cloud and outsourcing providers

Many US based cloud and outsourcing providers rely on Safe Harbor as a basis for transfer of data from the EU to the US. Following the ECJ's ruling, this is no longer allowed. We advise companies to review their existing US cloud and outsourcing contracts in view of the ECJ's decision. If Safe Harbor is being relied on, we recommend discussing potential alternatives with the respective service providers and renegotiating contractual terms where necessary.

For obvious reasons, we do not recommend entering into any new contracts that refer to Safe Harbor as a basis for transfer of personal data from the EU to the US.

Internal processing of personal data

Following the ECJ's ruling, companies may no longer use Safe Harbor for inter-group transfers of personal data between the EU and the US.

As Safe Harbor fulfilled a clear economic need, we expect that the EU and the US will continue their discussions on an updated Safe Harbor framework. Although companies can choose to wait a few months and see what these negotiations on an updated Safe Harbor framework bring, it means accepting a risk of non-compliance. Also, a new Safe Harbor framework will likely be subject to criticism similar to that which led to the ECJ's decision.

The use of EU model contracts can provide a temporary solution for non-compliance. EU model contracts, as sanctioned by the EC, contractually impose a level of data protection on the recipient of the personal data. If adopted in unmodified form, the clauses generally permit transfers to a non-EEA country without further approval by a national data protection authority.

For the longer term, companies can in practice rely only on Binding Corporate Rules (BCR) as a basis for structural data transfers between the EU, the US and elsewhere. BCR create a "safe haven" within a company for personal data and facilitates intra-group transfers of personal data. They are fully accepted and supported by the EU DPAs.

Some questions and answers

What is the Safe Harbor Framework?

EU data protection law prohibits transfers of personal data to countries outside the EU where protection of personal data does not comply with the EU standards – including to the US. The EU-

US Safe Harbor Framework was agreed in 2000 and formalised by the EC decision 2000/520/EC. It permits the transfer of personal data of Europeans to US companies that are self-certified under the Safe Harbor Privacy Principles and registered with the US Department of Commerce. Compliance is monitored and enforced by the Federal Trade Commission (FTC).

The scheme has frequently faced pressure from the European Parliament, the EU data protection authorities, and human rights activists for its failure to provide sufficient safeguards to protect the personal data of Europeans. In March 2014, the European Parliament adopted a resolution calling on the European Commission to immediately suspend the Safe Harbor agreement, which was not followed by the EC following the Snowden revelations.

Can companies still rely on Safe Harbor?

No. The ECJ declared the EC Decision 2000/520/EC on Safe Harbor invalid with direct effect. Companies can no longer rely on the Safe Harbor arrangement.

This might change if the EU and the US reach a new agreement on Safe Harbor. The negotiations have been progressing very slowly. The amended Safe Harbor is expected to address, among other things, the national security access issues that have raised concerns.

What is the background?

Following the Snowden revelations, an Austrian PhD student Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner (**Irish DPA**) against Facebook Ireland, objecting to the fact that its servers with personal data are located in the US. He argued that there is no protection of the personal data of EU citizens against state surveillance in the US. The Irish DPA rejected the claim, stating that EC Decision 2000/520/EC about adequacy of Safe Harbor was binding and it had no authority to review the claim. Schrems appealed to the Irish High Court, which then referred the case to the ECJ. For further details, please read our previous legal alert.

What did the Advocate General advise?

On 23 September 2015, Advocate General Bot of the ECJ delivered a non-binding but highly influential opinion. The ECJ generally followed the main conclusions and reasoning of the Advocate General. For further details, please read our legal alert "*ECJ Advocate General suggests striking down Safe Harbor – Questions & Answers*".

Read also the full text of the decision on *Maximillian Schrems v Data Protection Commissioner* (C362/14) and press release by the ECJ.