EU regulators express their take on Safe Harbor ruling

The Article 29 Working Party (WP29) issued on 16 October 2015 what it called a "robust, collective and common position" on the consequences of the recent decision of the European Court of Justice that declared Safe Harbor mechanism for transfers of personal data to the US invalid. The WP29 suggested that the EU and the US reach agreement before the end of January 2016 on an appropriate "political, legal and technical solution" for data transfers to the US.
The WP29's statement follows in the aftermath of the European Court of Justice's decision in *Maximillian Schrems v Data Protection Commissioner*. Our Legal alert of 7 October 2015 discussed the ramifications of this judgment and suggested EU model contracts as a temporary and Binding Corporate Rules (BCR) as a more permanent basis for structural data transfers between the EU, the US and elsewhere. The WP29's statement confirms that both EU model contracts and Binding Corporate Rules can indeed continue to be used.
The WP29's statement warns about the potential of coordinated enforcement by data protection authorities (DPAs) after the end of January 2016. This coordinated enforcement would likely initially focus on Safe Harbor based transfers. Because of the differences in individual statements of various national DPAs, the extent of actual enforcement will likely vary from country to country. The WP29's statement further indicates that also the use of alternatives for Safe Harbor, such as model contracts and BCR discussed above, will become subject to more scrutiny and potential enforcement. When employing these instruments, it is therefore important to ensure that their use results in actual data privacy compliance and not just the signing of documents.
Given the broad scope of the WP29 post-Safe Harbor guidance, we advise corporates to map and assess the compliance of both their internal and external data transfers globally.
See also the full text of the statement by the WP29.

Highlights of the WP29's conclusions

- The question of massive and indiscriminate surveillance is a key element of the ECJ's analysis. This surveillance is incompatible with the EU legal framework. Transfers to third countries where the powers of state authorities to access information go beyond what is necessary in a democratic society will not be considered as safe destinations for transfers
- The WP29 is urgently calling on EU member states and European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the US with the assurance that fundamental rights will be respected. According to the WP29, an intergovernmental agreement providing stronger guarantees to EU data subjects, such as a new Safe Harbor agreement, can be part of a solution
- Transfers that are still taking place under the current Safe Harbor framework after the ECJ's judgment are unlawful. EU DPAs might investigate data transfers on a case-by-case basis, for instance on the basis of complaints or on their own initiative
- If by the end of January 2016 no appropriate solution is agreed between EU and US authorities, the DPAs will take action, which may include coordinated enforcement action
- The WP29 will continue to analyse the impact of the ECJ's judgment on other transfer tools. The WP29's statement makes clear that EU Model Contract Clauses and Binding Corporate Rules may continue to be used
- According to the WP29's statement, businesses should reflect on any potential risks they may be taking when transferring data and should consider putting legal and technical solutions in place in a timely manner to mitigate those risks and which also respect EU data protection laws.

Will EU DPAs give businesses a grace period to align their processes with the ECJ's ruling?

The WP29's statement indicates that until the end of January 2016 national DPAs may investigate and enforce any specific data transfers to the US or elsewhere based on any adequacy mechanisms. At least one European DPA (UK's Information Commissioner) recognised that companies would need time to align their data transfers with law. On the other hand, the German DPA in Schleswig-Holstein has already suggested that companies which fall under its jurisdiction terminate contracts (also using EU Model Contract Clauses) for data transfers to the US. The Schleswig-Holstein DPA backs this guidance up by referring to potential enforcement actions.

Beyond Safe Harbor: real compliance is the key

Following the ECJ's decision, we advised companies in our previous Legal Alert to analyse which of their personal 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, which can temporarily be based on the EU Model Contract Clauses, and
- intra-group data transfers, which can be based on BCR or the EU Model Contract Clauses for simple intra-group transfers.
- In addition to due diligence on data transfers based on Safe Harbor previously advised, we recommend that companies extend their efforts and assess material data flows to other non-adequate countries. More specifically, we recommend that companies:
- analyse data flows to non-adequate countries, both intra-group and to third parties, and investigate the ways to bring those in line with data protection laws
- elaborate short-term strategies for achieving compliant transfers on a case-by-case basis
- review and regularly update data processing policies and practices to ensure that these policies are robustly implemented in practice.

The above adds agility if there are changes to the adequacy status of other data transfer mechanisms or adequate countries. And we recommend staying abreast of developments in this area, monitoring national DPAs relevant for your business operations

and engaging in conversations with them in case of uncertainty.

Some additional background

The EU is currently working on a general data protection regulation (GDPR) that will harmonise data protection laws throughout the EU, have extra-territorial effect and introduce strong mechanisms for protecting personal data. The final text of the GDPR is expected to be adopted in 2015 and to come into force within 2 years. In anticipation of the GDPR, EU DPAs have been taking an increasingly active role in enforcing data protection law and pursuing violators.

The ECJ has followed this trend by a string of groundbreaking cases. In 2014, the ECJ invalidated the EU Data Retention Directive for massive and unjustified collection and storage of personal telecom data. The same year the ECJ extended European jurisdiction over Google Inc. and gave a new dimension to the right to be forgotten. Less than a month ago, in *Weltimmo* (C230/14), the ECJ recognised a right – and a duty – of national DPAs to investigate claims of individuals regarding violation of their rights under data protection law regardless of the applicability of the national law. In *Schrems*, the national DPAs were reinstated in their authority to investigate and act on the claims on non-compliant data transfers outside the EU, even if there is an adequacy mechanism established by the European Commission.

For an overview of frequently asked questions about *Schrems* and its consequences, please see our Legal alert of 7 October 2015.