COVINGTON

The EU's Highest Court Invalidates Safe Harbor with Immediate Effect

October 6, 2015

Data Privacy and Cybersecurity

Today, the Court of Justice of the European Union (the "CJEU") invalidated the European Commission's Decision on the EU-U.S. Safe Harbor arrangement (Commission Decision 2000/520 - see here). The Court responded to pre-judicial questions put forward by the Irish High Court in the so-called *Schrems* case. More specifically, the High Court had enquired, in particular, about the powers of European data protection authorities ("DPAs") to suspend transfers of personal data that take place under the existing Safe Harbor arrangement. The CJEU ruled both on the DPAs' powers and the validity of the Safe Harbor, finding that national data protection authorities do have the power to investigate in these circumstances, and further, that the Commission decision finding Safe Harbor adequate is invalid.

This judgment affects all companies that rely on Safe Harbor. They now need to consider alternative data transfer mechanisms.

The Powers of the DPAs

First, the CJEU emphasized that the DPAs cannot invalidate a Commission adequacy decision themselves; only the CJEU has this power. However, the DPAs must have the power to examine complaints brought by data subjects against transfers on the basis of Safe Harbor or other adequacy decisions of the European Commission based on Article 25 (6) of the EU Data Protection Directive and be able to engage in legal proceedings to make a reference for a preliminary ruling by the CJEU with the aim of examining the decision's validity. In addition, the European Commission struck out the provision in the Safe Harbor decision which allows the DPAs to suspend data flows, subject to restrictive conditions establishing a high threshold for intervention. According to the CJEU, this provision denies the DPAs the powers which they have under the EU Data Protection Directive and the Commission has no competence under Article 25(6) to restrict the DPAs' powers under Article 28 of the Directive.

Safe Harbor

Second, the CJEU declared the Safe Harbor decision invalid, without providing for a transitional period, based on the following reasoning:

- Article 25 (6) of the EU Data Protection Directive empowers the Commission to find that a third country ensures an adequate level of protection. The CJEU held that, once the Commission has made such a finding, it must check periodically whether the finding is still factually and legally justified, especially when evidence gives rise to doubt.
- The CJEU further held that, although Article 25 (6) cannot be interpreted as requiring a level of protection *identical* to that guaranteed in the EU legal order, the level of protection must be **essentially equivalent**, by reason of the third country's domestic

laws or its international commitments. In other words, the legal order of the third country must prove to be effective, in practice, to meet this level of protection.

- In the present case, the Court decided that the standard of "essentially equivalent" is not met by the United States, in particular, because:
  - The United States public authorities are not required to comply with the Safe Harbor Principles.
  - Where U.S. law imposes an obligation conflicting with the Safe Harbor Principles, certified U.S. organizations must comply with the law.
  - The applicability of the Safe Harbor Principles may be limited on the basis of a broad "national security, public interest or law enforcement requirements" exemption contained in the Safe Harbor decision.

    The general nature of this derogation interferes with the fundamental rights of the individuals concerned, and the Safe Harbor decision does not contain any reference to rules adopted by the U.S. which would limit such interference. In fact, the Commission itself had found that the U.S. authorities were able to access and use transferred personal data for purposes that go beyond what is strictly necessary and proportionate to the protection of national security. In the CJEU's view:

    "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the EU to the U.S. without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes for which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."

    The CJEU further found that the Safe Harbor decision also does not refer to the existence of effective remedies against interference of this kind. "*Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data does not respect the essence of the fundament right to effective judicial protection.*"

What Does It Mean in Practice?

The judgment applies to everyone (*erga omnes*), not only to the parties in the case. It is definitive without possibility of appeal and has immediate effect.

The judgment will have an important impact on organizations and the broader political discussions regarding EU-U.S. data flows.

- Organizations relying on Safe Harbor to transfer personal data to the U.S. will have to consider alternative transfer mechanisms in order to transfer personal data lawfully to the U.S. Immediate short-term alternatives are likely to include standard contractual clauses and, in more limited instances, consent and possibly other statutory derogations (Article 26 (1) of the EU Data Protection Directive). Binding Corporate Rules are another alternative, but would require more time to put in place.

- Negotiations on the revised EU-U.S. Safe Harbor framework are still under way (see our earlier posts here and here). It will be interesting to observe the impact that the CJEU's findings have on these negotiations. The European Commission is determined to continue these negotiations, as Commissioner for Justice, Consumers and Gender Equality Věra Jourová confirmed in a press conference today (the full statement is available here).

Interestingly, the CJEU does not consider a system of self-certification in itself to be contrary to Article 25 (6) of the EU Data Protection Directive; however, it seems that such a system may be open to challenge unless the domestic law or international commitments of the third country ensure a level of protection which is essentially equivalent to that guaranteed in the EU legal order.

A working group of the Article 29 Data Protection Working Party—an EU advisory body, comprised of representatives of the DPAs of all EU Member States, the European Data Protection Supervisor and the European Commission—is meeting later this week to discuss the implications of this ruling. Moreover, the European Commission will release guidance shortly.

It is hoped that the DPAs will come up with pragmatic solutions as thousands of companies will be struggling to put in place alternative data transfer mechanisms which, in many cases, cannot be done overnight.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice group:

Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Monika Kuschewsky	+32 2 549 52 49	mkuschewsky@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com