

**Position Paper on the EU Court of Justice Ruling in Case C-311/18
("Schrems II")**

European Federation of Data Protection Officers
September 2020

Schrems II: DPOs left alone with unsolvable dilemmas

EFDPPO welcomes the increased attention paid to the major issue of personal data protection, especially when related to recent international data transfers. We believe that the protection of personal data, as a fundamental right, requires rigorous attention from the competent administrative authorities, as well as from courts dealing with relevant cases. Any court decision concerning personal data protection issues, particularly by the CJEU, evokes great interest and discussion by the professional public, as well as the controllers and processors. For the DPOs, such a court decision usually provides guidance and important information of practical relevance. Moreover, the interpretation given to the relevant legal texts, as well as the principles expressed and adopted in such court decisions, helps DPOs perform their duties more effectively.

Recently, great attention has been given to the “Schrems II” case, which invalidated the “Privacy Shield” agreement between the EU and the USA on data transfers, and has brought a significant change to the field of data protection. Suddenly, following the Schrems II decision, international data processing has to deal with a whole new situation. In our opinion the main points to be considered as possible causes for this are the following:

- With the Privacy Shield, the EU commission had not negotiated an ideal scheme as the basis for an adequacy decision between EU and US. Furthermore, the standard contractual clauses were basically left for quite a long time.
- International companies that are not redirecting their data processing practices with respect to European law
- DPAs without a position imposing enough powers to create practical changes at international enterprises
- Lack of sufficient information exchange between all stakeholders

Without any intention of contradicting the CJEU's conclusions on the state of personal data protection in the US and the shortcomings regarding Privacy Shield, we would also like to draw attention to some aspects of this decision and the subsequent actions of public authorities that European DPOs have to deal with.

We would like to point out that a court decision that intervenes with immediate effect with the processing of personal data in such an extensive and diverse way is almost impossible to be translated into practice. This is especially true for small and medium-sized businesses, which often do not have sufficient resources for rapid response

and are in principle dependent on large providers of cloud solutions. In fact, there are just not enough alternatives for them. All companies use software and platform contractors which are affected by Schrems II. Moving to alternatives, if there were any available, would take years.

In such cases, we, as DPOs, find ourselves in a very difficult situation when providing the right advice to controllers and processors. We would like to respectfully emphasise that from our point of view it is always important to consider whether it is appropriate to issue judgments setting out “with immediate effect” obligations which, in principle, cannot in the short term be effectively complied with by the addressees. Considering the deferred effectiveness of the judgment could be an appropriate solution. For now, the DPOs are asked for guidance in this case. The judgment creates pressure on DPOs to deal with the necessity to stop data transfers immediately, while knowing at the same time that their companies have almost no options for practical action. Currently, most companies ask their contractors for additional measures making SCC applicable. The DPOs have to explain the complex circumstances and mistakes, which led to this situation, whereas it is obvious that many companies do not share the same interest regarding data protection. The trouble it brings, which is made even worse due to the Schrems II decision, goes far beyond its benefits. And it puts the DPO in the above-mentioned rather awkward position.

From the point of view of EFDPO, we would therefore very much appreciate quick and specific steps to clarify the situation, for example:

1. Supervisory authorities or the EDPB to provide controllers and processors with clear guidance on how to proceed in assessing the "appropriate safeguards" associated with preventing unauthorised access to personal data by US authorities. This is especially important for the possibility of using SCC. It is of course also necessary to take the specific circumstances of the processing in question into account. We very much welcome the recent announcement made by EDPB that it is working intensively on this topic.
2. US data processors to provide the required technical and organisational measures for processing required under European legislation.
3. Supervisory authorities to address the international processors directly. The GDPR provides this option, where processor responsibilities can be addressed directly.
4. European Commission to negotiate as soon as possible a new tool that will replace the invalidated Privacy Shield so that cooperation between the EU and the US can continue and at the same time the rights of data subjects can be properly protected.

5. The European Commission has to provide updated Standard Contractual Clauses which can be practically applied. We very much welcome the recent announcement made by Commissioner Reynders that the European Commission plans to prepare the new version of SCC by the end of this year.
6. The US Administration to respect the privacy and data protection rights of all people, irrespective of their origin.

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, email: office@efdpo.eu,

President: Thomas Spaeing (Germany)

Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira (Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDP) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The new association is based in Brussels.

Founding members:

- Austria: privacyofficers.at – Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter
- Czech Republic: Spolek pro ochranu osobních údajů
- France: UDPO, Union des Data Protection Officer - DPO
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov