



711.424.1

17 July 2020

After “Schrems II”: Europe needs digital independence

After the adequacy of the “EU-US Privacy Shield” was invalidated by a recent decision issued by the Court of Justice of the European Union (CJEU), the Berlin Commissioner for Data Protection and the Freedom of Information, Maja Smolczyk, is now calling on data processors in Berlin to move any personal data stored in the USA to Europe.

In its decision of 16 July 2020 (“Schrems II”, C-311/18), the CJEU stated that the US authorities’ access to data belonging to European citizens is too extensive. As a result, personal data may generally no longer be transferred to the USA until the legal situation changes. There are some exceptions, especially in special cases stipulated by law, such as when booking a hotel room in the USA.

One of the findings noted in the CJEU decision concerns the government surveillance measures in the USA, which involve the mass collection of personal data with no clear limitations. This contradicts the Charter of Fundamental Rights of the European Union (Paragraph 180 *et seq.* of the Decision). The CJEU also indicates that European citizens are unable to request a judicial review of the surveillance measures carried out by the US authorities. This violates the European fundamental right to effective legal protection.

Personal data may only be transferred to third countries that ensure a level of data protection that is equivalent to the essence of the European fundamental rights. As the findings of the highest European court suggest that is not the case in the USA, the decision issued by the CJEU has invalidated the adequacy of the “EU-US Privacy Shield”, which was previously the basis for many personal data transfers to the USA. By contrast, the CJEU has ruled that “standard contractual clauses” are admissible under certain conditions; standard contractual clauses can be established between European companies and providers in third countries to ensure the European level of data protection abroad. Before the first data transfer, however, the CJEU emphasises that both European data exporters and third-country data importers are obliged to check whether the data could potentially be accessed by government authorities in the third country in a manner that goes beyond the access rights granted under European law (Paragraphs 134 *et seq.* & 142 of the Decision). If such rights of access are enjoyed by the government authorities, data may not even be exported on the basis of standard contractual clauses. Any data that has already been transferred to any such third countries must be retrieved. Contrary to the prevalent practice to date, data cannot be exported merely on the basis of standard contractual clauses (Paragraph 126 *et seq.* of the Decision).

The CJEU emphasises that the data protection supervisory authorities must prohibit unlawful data exports according to these new standards (Paragraphs 135 & 146 of the Decision), and that data subjects may claim damages for the unlawful exportation of personal data (Paragraph 143 of the Decision). This may especially include non-material damage (solatia); the amount of compensation must act as a deterrent in accordance with European law.

The Berlin Commissioner for Data Protection and the Freedom of Information calls on all controllers under her supervision to observe the CJEU's decision. Controllers who transfer personal data to the USA, especially when using cloud-based services, are now required to switch immediately to service providers based in the European Union or a country that can ensure an adequate level of data protection.

Maja Smolczyk:

“The CJEU has made it refreshingly clear that data exports are not just financial decisions, as people's fundamental rights must also be considered as a matter of priority. This ruling will put an end to the transfer of personal data to the USA for the sake of convenience or to cut costs. Now is the time for Europe to become digitally independent.

The CJEU has explicitly obliged the supervisory authorities to prohibit all unlawful data transfers, and we gladly accept the challenge. Of course, that not only applies to data transfers to the USA, which have already been outlawed by the CJEU; we must also check whether similar or perhaps even greater problems are involved in data transfers to other countries, such as China, Russia or India”.