How can we transfer personal data to companies outside EU? 1/40/20

By passing a landmark ruling (C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems of 16 July 2020) which emphasises the basic right to privacy when personal data is transferred to third countries, the Court of Justice of the European Union ("CJEU") has again confirmed how important it is to maintain a high level of protection of personal data being transferred from the EEA to third countries. The ruling has raised a number of questions about the legal basis for personal data transfers to third countries. As the ruling focuses on transfers to the US, this article explores some of the steps companies should take with the ruling in force.

Rules that require secure processing and adequate protection of personal data consistent with the General Data Protection Regulation ("GDPR") apply to any dealings with personal data. Companies planning to transfer data outside the EEA should expect more requirements this kind of data processing will have to meet before data can be processed at all.

The European Commission had so far found that the EU-US privacy shield provided an adequate level of protection for personal data transferred from the EU to US entities. With the CJEU ruling in force, it is now clear that matters have changed. Although the privacy shield aims to protect any personal data transferred from the EU to US entities for commercial purposes, the guarantees provided by the privacy shield might no longer be sufficient to transfer personal data lawfully.

First of all, the company needs to understand what personal data is to be transferred to a US entity and for what purpose. Personal data is basically transferred for business purposes after being collected for further processing in the US (e.g. a customer's or employee's name, phone number, email address or any other details that help identify the individual). This is how an EU company or, say, a US entity's affiliate or partner in Europe transfers personal data to the US entity for further processing in the US. Such transactions usually occur when people buy goods and services over the Internet, use social media and cloud services, or work for EU companies that acquire, say, services related to personnel management from a US entity (e.g. the US parent).

Companies transferring data in this way so far believed that the privacy shield provides a high level of protection. They were not afraid of committing personal data protection breaches and processed personal data by transferring it to US entities on condition that the data recipient will process it (e.g. store it or pass it on) according to tight data protection rules and measures adopted by the privacy shield. The CJEU has now invalidated Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield, but still upholds Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries.

Although standard contractual clauses still stand, the CJEU finds that we need to maintain a level of data protection which is substantially equivalent to that guaranteed by the GDPR. The company that transfers personal data to a third country (including the US) is responsible for making sure that the recipient country provides adequate protection through measures consistent with the GDPR.

Secondly, once the company understands what kind of data is involved and whether it can be transferred to a third country (including the US), the company needs to consider ways of ensuring that requirements arising from the GDPR and the CJEU ruling will be met in the future:

- The parties involved in the transfer and further processing of personal data should mitigate risks by adopting additional security measures, such as data encryption and in certain cases anonymisation or pseudonymisation, to ensure that the data can be accessed only by the company having transferred it to the US;
- An EU company transferring personal data to a third-country company should assess how the recipient meets requirements consistent with the GDPR and should make sure that the data enjoys the rights granted by the GDPR;
- The company should evaluate its business partners in third countries, as well as assessing and documenting the need to transfer personal data, relying on reasonable data transfer mechanisms, and choosing service providers that mitigate risks associated with data transfers.

The US authorities have already announced that as a result of the CJEU ruling more than 5,300 large and small European and US companies can no longer rely on the privacy shield as a basis for transferring personal data from Europe to the US. Companies should expect that the supervisory authorities will be running checks to make sure that the companies have adopted even more stringent measures when it comes to data protection and transfers to third countries. What we also need to understand is that doing business as usual and waiting to see whether the authorities will take any action can have unpredictable consequences, with fines reaching 4% of the company’s annual turnover.