The CJEU Schrems decision: What you should know as a business and as an individual

On 6 October 2015, the CJEU issued the much-awaited decision in the *Schrems* case (Case C-362/14). In this case, the CJEU ruled that the Commission's EU-US Safe Harbour Decision 2000/520 on data transfer to the United States is invalid. The Safe Harbour Decision held that the level of data protection in the United States is adequate.

The background of this case are Edward Snowden's revelations concerning transfers of data on European citizens to the United States. Internet companies, such as Facebook, store much of their data on servers in the United States, which means that the US National Security Agency (the NSA) could get hold of data protected information on European citizens through its PRISM surveillance programme.

Schrems, an Austrian campaigner, initially filed a complaint with the Irish Data Protection Commissioner to investigate this practice. When the Data Protection Commissioner decided not to investigate the matter because of the existing Safe Harbour Decision, compelling national data protection agencies to transfer data falling under the decision, Schrems took the Data Protection Commissioner to the Irish High Court. The High Court asked the CJEU for a preliminary ruling – the question being whether the national data protection agencies are bound by the Commission's decision.

The central topic was whether the US rules on data protection could be considered 'adequate', i.e. up to European standards (the Data Protection Directive 95/46/EC and the Charter of Fundamental Rights of the EU). Recital 57 of this Directive reads as follows, 'The transfers of personal data to a third country which does not ensure an adequate level of protection must be prohibited'.

The CJEU came to the following conclusion

That the EU-US Safe Harbour Decision is invalid for the following reasons;

- Firstly, it does not offer an adequate level of protection, because it requires 'clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.'
- Secondly, 'data subjects [individuals] had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.'

Consequently, the decision not only held the current EU-US Safe Harbour Decision to be invalid, but also that national supervisory authorities are not prevented from examining the claim of a person on personal data rights – even though a Commission decision allows such transfers.

What is the current legal status?

Data transfers, which are merely based on the Safe Harbour Decision, are considered invalid. The Commission is undergoing the establishment of a Safe Harbour II, but its time of publication is currently unknown. Neither is it known whether such can be considered as compliant with the new decision. The Working Group 29, which is a co-operation between the Commission and the data protection agencies, is said to publish guidelines within the next two weeks.

Another factor to take into consideration is whether the national data protection agencies will immediately move forward and seek enforcement of these rules against the businesses. For businesses to safeguard themselves, they should take steps to adapt.

What this means for businesses

The decision will mainly affect companies transferring personal data to servers in the US. These companies are usually US-established, such as Facebook. Other types of businesses affected are those storing data in the cloud and online retailers. Pharmaceutical companies and HR companies that store sensitive data on European individuals on US servers will also need to look into their practices.

What are the immediately available solutions?

The most convenient solution will be for businesses to implement a consent function in their online activities, e.g. in the terms & conditions for social media companies, or at checkout for online retailers. This practice, however, may not be accepted by national data protection agencies, especially not if it concerns large transfers of personal data. The Danish Data Protection Agency has not issued any guidelines as of yet.

A safer solution would be the EU Commission model clauses. The purpose of these model clauses is to allow national data protection agencies to suspend data transfers to countries where the national rules do not follow EU standards.

What this means for private individuals

At the moment, the CJEU decision may be regarded as a victory for individuals from the point of view of data protection. Businesses are, however, likely to await guidelines by the Working Party 29 – which may be published at any time – before changing their practices.

The CJEU finds that although there is a Commission decision stating that the level of protection is adequate, private individuals may now challenge the validity of a particular data protection matter before the national data protection agencies. This possibility for individuals might also be of relevance for businesses, as it means that although the data protection agencies might await an enforcement of the decision, private individuals may not.

—

If you have any questions about this decision in relation to your particular business or personal concerns, please do not hesitate to contact us.