



Key Issues: Personal data

Case: Maximillian Schrems v Data Protection Commissioner

Reference: Case C-362/14, CJEU (Grand Chamber), 6 October 2015

Legislation: Council Directive 1995/46/EC

Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ("Facebook") since 2008. Any person residing in the EU who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

On 25 June 2013, Mr Schrems made a complaint to the Data Protection Commissioner (Ireland) and asked the Commissioner to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in the United States did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Commission Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection. Commission Decision 2000/520 contains, at Annex 1, the "Safe Harbour Privacy Principles".

Mr Schrems brought an action before the High Court (Ireland) challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a "significant over-reach" on the part of the NSA and other federal agencies.

According to the High Court, EU citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.

The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law. The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter of Fundamental Rights of the EU ("the Charter"), and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice (CJEU) in the judgment in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238).

The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

The High Court further observes that, in his action, Mr Schrems raises the legality of the "safe harbour" regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether

Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

In those circumstances the High Court decided to stay the proceedings and to refer a question to the CJEU for a preliminary ruling.

Consideration by CJEU

Commission Decision 2000/520 lays down that “national security, public interest, or law enforcement requirements” have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

That decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference.

In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security. Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind.

As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the CJEU’s settled case-law, lay down 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. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data.

Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary.

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 European Union to the United States 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 which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.

Likewise, 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 fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.

In order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment. However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

The CJEU held that:

- 1. Article 25(6) of Directive 95/46/EC must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC on the adequacy of the protection provided by the "safe harbour" privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country, when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

2. Decision 2000/520 is invalid.

Why is this decision important?

The use of personal data by businesses is likely to attract more attention in future as the public begin to realise the extent to which their personal information, on social networks and elsewhere, can be transferred and analysed by third parties. Businesses which store and share personal data will need to consider the consequences of this judgment.

The material on these pages is for information purposes only. You should not act or rely on this information without seeking professional advice.

CLfE (12/2015)

Elliott Duffy Garrett | Royston House | 34 Upper Queen Street | Belfast | BT1 6FD

W: www.edglegal.com

E: kevin.mcveigh@edglegal.com

T: +44 (0) 28 9024 5034

F: +44 (0) 28 9024 1337