

Case C-311/18**Data Protection Commissioner**

v

**Facebook Ireland Ltd
and
Maximillian Schrems**

(Request for a preliminary ruling from the High Court (Ireland))

Judgment of the Court (Grand Chamber), 16 July 2020

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfers of personal data to third countries for commercial purposes — Article 45 — Commission adequacy decision — Article 46 — Transfers subject to appropriate safeguards — Article 58 — Powers of the supervisory authorities — Processing of the data transferred by the public authorities of a third country for national security purposes — Assessment of the adequacy of the level of protection in the third country — Decision 2010/87/EU — Protective standard clauses on the transfer of personal data to third countries — Suitable safeguards provided by the data controller — Validity — Implementing Decision (EU) 2016/1250 — Adequacy of the protection provided by the EU-US Privacy Shield — Validity — Complaint by a natural person whose data was transferred from the European Union to the United States)

1. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Scope — Concept of personal data processing — Transfers of personal data for commercial purposes by an economic operator established in a Member State to another operator established in a third country — Included — Data liable to be processed by the authorities of the third country in question for the purposes of national security — Irrelevant (European Parliament and Council Regulation 2016/679, Art. 2(1) and Art. 2(2)(a), (b) and (d), and Art. 4(2))*

(see paragraphs 82, 83, 85-89, operative part 1)

2. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Transfers of personal data to third countries — Transfers subject to appropriate safeguards pursuant to standard contractual data protection clauses — Concept of adequate level of protection to be ensured by the third country in question at the time of such transfers — Interpretation in the light of EU law — Criteria for assessment (Charter of Fundamental Rights of the European Union, Art. 52(3); European Parliament and Council Regulation 2016/679, Art. 46(1) and (2)(c))*

(see paragraphs 92-96, 98-101, 103-105, operative part 2)

3. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Transfers of personal data to third countries — Transfers subject to appropriate safeguards pursuant to standard contractual data protection clauses — National supervisory authorities — Powers — Monitoring of transfers of personal data to third countries — Requirement to suspend or prohibit such transfers in the event of the breach of an adequate level of protection in the third country in question — Conditions*

(Charter of Fundamental Rights of the European Union, Art. 8(3); European Parliament and Council Regulation 2016/679, Arts 45 and 46, Art. 51(1), Art. 57(1)(a) and (f), and Art. 58(1), (2)(f) and (j))

(see paragraphs 107, 108, 112-121, operative part 3)

4. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Transfers of personal data to third countries — Transfers subject to appropriate safeguards pursuant to standard contractual data protection clauses — Decision 2010/87 introducing standard contractual clauses for the transfer of personal data to third countries — Appropriate guarantees offered by data controllers and processors established in the EU and by supervisory authorities — Obligation for those authorities to prohibit or suspend such transfers in the event of infringement of those clauses — Rights to privacy, personal data protection and effective judicial protection — No infringement — Validity of the decision*
(Charter of Fundamental Rights of the European Union, Arts 7, 8 and 47; European Parliament and Council Regulation 2016/679, Art. 46(1) and (2)(c); Commission Decision 2010/87, annex)

(see paragraphs 128-130, 133-145, 148, 149, operative part 4)

5. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Transfer of personal data to third countries — Adoption by the Commission of a decision finding an adequate level of protection in a third country — Decision 2016/1250 finding an adequate level of protection provided by the EU-US Privacy Shield — National authority dealing with an application challenging the adequacy of the level of protection provided by that third country — Obligation for that authority to examine the application — Examination of the validity of Decision 2016/1250*
(Art. 288, para. 4, TFEU; European Parliament and Council Regulation 2016/679, Art. 45(3) and Art. 77(1); Commission Decision 2016/1250, Annex II)

(see paragraphs 151-161)

6. *Fundamental rights — Charter of Fundamental Rights of the European Union — Respect for private life — Protection of personal data — Retention of and access to personal data with a view to their use by public authorities — Interference in those fundamental rights — Limitations on the exercise of those rights — Observance of the principle of proportionality*
(Charter of Fundamental Rights of the European Union, Arts 7 and 8, Art. 52(1), second sentence; European Parliament and Council Regulation 2016/679)

(see paragraphs 170-176)

7. *Protection of individuals with regard to the processing of personal data — Regulation 2016/679 — Transfer of personal data to third countries — Adoption by the Commission of a decision finding an adequate level of protection in a third country — Decision 2016/1250 finding an adequate level of protection provided by the EU-US Privacy Shield — Absence of a level of protection essentially equivalent to that provided under EU law — Infringement of the rights to privacy, personal data protection and effective judicial protection of the persons concerned by those transfers — Establishment of a mediation mechanism under the EU-US Privacy Shield — No effect on the infringement of the right to effective judicial protection — Invalidity of the decision*
(Charter of Fundamental Rights of the European Union, Arts 7, 8 and 47, Art. 52(1), second sentence; European Parliament and Council Regulation 2016/679, Art. 45(2)(a) and (3); Commission Decision 2016/1250, Annex II)

(see paragraphs 180-185, 187-192, 195-201, operative part 5)

8. *Questions referred for a preliminary ruling — Assessment of validity — Declaration of invalidity of an EU act — Decision 2016/1250 finding an adequate level of protection provided by the EU-US Privacy Shield — Effects — No temporal limitation*
(Art. 267 TFEU; European Parliament and Council Regulation 2016/679, Art. 49; Commission Decision 2016/1250)

Résumé

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield

However, it considers that Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries is valid.

The General Data Protection Regulation (1) ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. (2) In the absence of an adequacy decision, such a transfer may take place only if the personal data exporter established in the European Union has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies. (3) Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards. (4)

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data are transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where they undergo processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520 (5) ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment'). (6)

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the European Union to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 2010/87. (7) Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield (8) ('the Privacy Shield Decision').

By its request for a preliminary ruling, the referring court asks the Court whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raises the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

In today's judgment, the Court finds that examination of Decision 2010/87 in the light of the Charter of

Fundamental Rights has disclosed nothing to affect the validity of that decision. However, the Court declares Decision 2016/1250 invalid.

The Court considers, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court adds that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR.

Regarding the level of protection required in respect of such a transfer, the Court holds that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter. In those circumstances, the Court specifies that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.

Regarding the supervisory authorities' obligations in connection with such a transfer, the Court holds that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the European Union has not itself suspended or put an end to such a transfer.

Next, the Court examines the validity of Decision 2010/87. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court adds, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court finds that Decision 2010/87 establishes such mechanisms. In that regard, the Court points out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

Lastly, the Court examines the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court notes that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a

way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

As regards the requirement of judicial protection, the Court holds that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declares Decision 2016/1250 invalid.

[1](#) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

[2](#) Article 45 of the GDPR.

[3](#) Article 46(1) and (2)(c) of the GDPR.

[4](#) Article 49 of the GDPR.

[5](#) Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 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 (OJ 2000 L 215, p. 7).

[6](#) Judgment of the Court of 6 October 2015, *Schrems*, C-362/14 (see, also, CP No 117/15).

[7](#) Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

[8](#) Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1).