СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

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)

In Case C-311/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings

Data Protection Commissioner

v

Facebook Ireland Ltd,

Maximillian Schrems,

intervening parties:

* Language of the case: English.

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi and I. Jarukaitis, Presidents of Chambers, M. Ilešič, T. von Danwitz (Rapporteur), and D. Šváby, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2019,

after considering the observations submitted on behalf of:

– the Data Protection Commissioner, by D. Young, Solicitor, B. Murray and M. Collins, Senior Counsel, and C. Donnelly, Barrister-at-Law,

– Facebook Ireland Ltd, by P. Gallagher and N. Hyland, Senior Counsel, A. Mulligan and F. Kieran, Barristers-at-Law, and P. Nolan, C. Monaghan, C. O'Neill and R. Woulfe, Solicitors,

– Mr Schrems, by H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty and S. O'Sullivan, Senior Counsel, and G. Rudden, Solicitor,

– the United States of America, by E. Barrington, Senior Counsel, S. Kingston, Barrister-at-Law, S. Barton and B. Walsh, Solicitors,

– the Electronic Privacy Information Centre, by S. Lucey, Solicitor, G. Gilmore and A. Butler, Barristers-at-Law, and C. O'Dwyer, Senior Counsel,

– BSA Business Software Alliance Inc., by B. Van Vooren and K. Van Quathem, advocaten,

– Digitaleurope, by N. Cahill, Barrister, J. Cahir, Solicitor, and M. Cush, Senior Counsel,

– Ireland, by A. Joyce and M. Browne, acting as Agents, and D. Fennelly, Barrister-at-Law,

– the Belgian Government, by J.-C. Halleux and P. Cottin, acting as Agents,

– the Czech Government, by M. Smolek, J. Vláčil, O. Serdula and A. Kasalická, acting as Agents,

– the German Government, by J. Möller, D. Klebs and T. Henze, acting as Agents,

– the French Government, by A.-L. Desjonquères, acting as Agent,

– the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and M. Noort, acting as Agents,

– the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,

– the Polish Government, by B. Majczyna, acting as Agent,

– the Portuguese Government, by L. Inez Fernandes, A. Pimenta and C. Vieira Guerra, acting as Agents,

– the United Kingdom Government, by S. Brandon, acting as Agent, and J. Holmes QC, and C. Knight, Barrister,

– the European Parliament, by M.J. Martínez Iglesias and A. Caiola, acting as Agents,

– the European Commission, by D. Nardi, H. Krämer and H. Kranenborg, acting as Agents,

– the European Data Protection Board (EDPB), by A. Jelinek and K. Behn, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 19 December 2019,

gives the following

Judgment

1 This reference for a preliminary ruling, in essence, concerns:

– the interpretation of the first indent of Article 3(2), Articles 25 and 26 and Article 28(3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), read in the light of Article 4(2) TEU and of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’);

– the interpretation and validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (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) ('the SCC Decision'); and

– the interpretation and validity of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1; 'the Privacy Shield Decision').

2 The request has been made in proceedings between the Data Protection Commissioner (Ireland) ('the Commissioner'), on the one hand, and Facebook Ireland Ltd and Maximillian Schrems, on the other, concerning a complaint brought by Mr Schrems concerning the transfer of his personal data by Facebook Ireland to Facebook Inc. in the United States.

Legal context

Directive 95/46

3 Article 3 of Directive 95/46, under the heading 'Scope', stated, in paragraph 2:

'This Directive shall not apply to the processing of personal data:

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

– …'

4 Article 25 of that directive provided:

'1. The Member States shall provide that the transfer to a third country of personal data … may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; …

…

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's Decision.'

5 Article 26(2) and (4) of the directive provided:

'2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

…

4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.'

6 Pursuant to Article 28(3) of that directive:

'Each authority shall in particular be endowed with:

– investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

– the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been infringed or to bring those infringements to the attention of the judicial authorities.

…'

The GDPR

7 Directive 95/46 was repealed and replaced by 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR').

8 Recitals 6, 10, 101, 103, 104, 107 to 109, 114, 116 and 141 of the GDPR state:

'(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

…

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ("sensitive data"). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

…

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in these flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

…

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects

should be provided with effective and enforceable rights and effective administrative and judicial redress.

…

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. …

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

…

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

…

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. …

…

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. …'

9 Article 2(1) and (2) of the GDPR provides:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

penalties, including the safeguarding against and the prevention of threats to public security.'

10 Article 4 of the GDPR provides:

'For the purposes of this Regulation:

…

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) "processor", means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) "recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

…'

11 Article 23 of the GDPR states:

'1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

…

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'

12 Chapter V of the GDPR, under the heading 'Transfers of personal data to third countries or international organisations', contains Articles 44 to 50 of that regulation. According to Article 44 thereof, under the heading 'General principle for transfers':

'Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.'

13 Article 45 of the GDPR, under the heading ‘Transfers on the basis of an adequacy decision’, provides, in paragraphs 1 to 3:

‘1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).’

14 Article 46 of the GDPR, under the heading ‘Transfers subject to appropriate safeguards’, provides, in paragraphs 1 to 3:

‘1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.’

15 Article 49 of the GDPR, under the heading ‘Derogations for specific situations’, states:

‘1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.'

16 Under Article 51(1) of the GDPR:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

17 In accordance with Article 55(1) of the GDPR, 'each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State'.

18 Article 57(1) of that regulation states as follows:

'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

(f) handle complaints lodged by a data subject … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable

period, in particular if further investigation or coordination with another supervisory authority is necessary;

…’

19 According to Article 58(2) and (4) of the GDPR:

‘2. Each supervisory authority shall have all of the following corrective powers:

…

(f) to impose a temporary or definitive limitation including a ban on processing;

…

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

…

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.’

20 Article 64(2) of the GDPR states:

‘Any supervisory authority, the Chair of the [European Data Protection Board (EDPB)] or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.’

21 Under Article 65(1) of the GDPR:

‘In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

…

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.’

22 Article 77 of the GDPR, under the heading ‘Right to lodge a complaint with a supervisory authority’, states:

‘1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’

23 Article 78 of the GDPR, under the heading ‘Right to an effective judicial remedy against a supervisory authority’, provides, in paragraphs 1 and 2:

‘1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to [an] effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.’

24 Article 94 of the GDPR provides:

‘1. Directive [95/46] is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.’

25 Pursuant to Article 99 of the GDPR:

‘1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.’

The SCC Decision

26 Recital 11 of the SCC Decision reads as follows:

‘Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data

subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.'

27 Article 1 of the SCC Decision states:

'The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive [95/46].'

28 In accordance with the second paragraph of Article 2 of the SCC Decision, that decision 'shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as data processors'.

29 Article 3 of the SCC Decision provides:

'For the purposes of this Decision, the following definitions shall apply:

…

(c) "data exporter" means the controller who transfers the personal data;

(d) "data importer" means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive [95/46];

…

(f) "applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

…'

30 According to its original wording, prior to the entry into force of Implementing Decision 2016/2297, Article 4 of Decision 2010/87 provided:

‘1. ‘Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive [95/46], the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive [95/46] where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.’

31 Recital 5 of Implementing Decision 2016/2297, adopted after the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650) was handed down, reads as follows:

‘*Mutatis mutandis*, a Commission decision adopted pursuant to Article 26(4) of Directive [95/46] is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities, in so far as it has the effect of recognising that transfers taking place on the basis of standard contractual clauses set out therein offer sufficient safeguards as required by Article 26(2) of that Directive. This does not prevent a national supervisory authority from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses.’

32 According to its current wording, resulting from Implementing Decision 2016/2297, Article 4 of the SCC Decision states:

‘Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive [95/46] leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission which will forward the information to the other Member States.’

33 The annex to the SCC Decision, under the heading ‘Standard Contractual Clauses (Processors)’, is comprised of 12 standard clauses. Clause 3 thereof, itself under the heading ‘Third-party beneficiary clause’, provides:

‘1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

…’

34 According to Clause 4 in that annex, under the heading ‘Obligations of the data exporter’:

‘The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

…

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive [95/46];

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

…'

35 Clause 5 in that annex, under the heading 'Obligations of the data importer …', provides:

'The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

…

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

…'

36 The footnote to the heading of Clause 5 states:

'Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive [95/46], that is, if they

constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. …'

37 Clause 6 in the annex to the SCC Decision, under the heading 'Liability', provides:

'1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter …

…'

38 Clause 8 in that annex, under the heading 'Cooperation with supervisory authorities', stipulates, in paragraph 2 thereof:

'The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.'

39 Clause 9 in that annex, under the heading 'Governing law', specifies that the clauses are to be governed by the law of the Member State in which the data exporter is established.

40 According to Clause 11 in that annex, under the heading 'Sub-processing':

'1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses …

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for

cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

…'

41 Clause 12 in the annex to the SCC Decision, under the heading 'Obligation after the termination of personal data-processing services', states, in paragraph 1 thereof:

'The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. …'

The Privacy Shield Decision

42 In the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650), the Court declared Commission Decision 2000/520/EC 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), in which the Commission had found that that third country ensured an adequate level of protection, invalid.

43 Following the delivery of that judgment, the Commission adopted the Privacy Shield Decision, after having, for the purposes of adopting that decision, assessed the US legislation, as stated in recital 65 of the decision:

'The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence (ODNI) …, has provided the Commission with detailed representations and commitments that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of

data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.'

44 The Commission's assessment of those limitations and guarantees is summarised in recitals 67 to 135 of the Privacy Shield Decision, while the Commission's conclusions on the adequate level of protection in the context of the EU-US Privacy Shield are set out in recitals 136 to 141 thereof.

45 In particular, Recitals 68, 69, 76, 77, 109, 112 to 116, 120, 136 and 140 of the Privacy Shield Decision state:

'(68) Under the U.S. Constitution, ensuring national security falls within the President's authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs … While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. … At present, the two central legal instruments in this regard are Executive Order 12333 ("E.O. 12333") … and Presidential Policy Directive 28.

(69) Presidential Policy Directive 28 ("PPD-28"), issued on 17 January 2014, imposes a number of limitations for "signals intelligence" operations … This presidential directive has binding force for U.S. intelligence authorities … and remains effective upon change in the U.S. Administration … PPD-28 is of particular importance for non-US persons, including EU data subjects. …

…

(76) Although not phrased in … legal terms, [the] principles [of PPD-28] capture the essence of the principles of necessity and proportionality. …

(77) As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. …

…

(109) Conversely, under Section 702 [of the Foreign Intelligence Surveillance Act (FISA)], the [United States Foreign Intelligence Surveillance Court (FISC)] does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the [US] Attorney General and the Director of National Intelligence [(DNI)]. … As indicated, the certifications to be approved by the FISC contain no information about the individual persons to

be targeted but rather identify categories of foreign intelligence information … While the FISC does not assess — under a probable cause or any other standard — that individuals are properly targeted to acquire foreign intelligence information …, its control extends to the condition that "a significant purpose of the acquisition is to obtain foreign intelligence information" …

…

(112) First, the [FISA] provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance … This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed …; to sue U.S. government officials in their personal capacity ("under colour of law") for money damages …; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States …

(113) Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes …

(114) Finally, the U.S. government has pointed to the [Freedom of Information Act (FOIA)] as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual's personal data … Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. …

(115) While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited … and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing" …, which restricts access to ordinary courts …

(116) In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision.

This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond this original concept.

…

(120) … the U.S. government commits to ensure that, in carrying out its functions, the Privacy Shield Ombudsperson will be able to rely on the cooperation from other oversight and compliance review mechanisms existing in U.S. law. … Where any non-compliance has been found by one of these oversight bodies, the Intelligence Community element (e.g. an intelligence agency) concerned will have to remedy the non-compliance as only this will allow the Ombudsperson to provide a "positive" response to the individual (i.e. that any non-compliance has been remedied) to which the U.S. government has committed. …

…

(136) In the light of [those] findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.

…

(140) Finally, on the basis of the available information about the U.S. legal order, including the representations and commitments from the U.S. government, the Commission considers that any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference.'

46 Under Article 1 of the Privacy Shield Decision:

'1. For the purposes of Article 25(2) of [Directive 95/46], the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.

2. The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I [and] III to VII.

3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the "Privacy Shield List", maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.'

47 Under the heading 'EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce', Annex II to the Privacy Shield Decision, provides, in paragraph I.5 thereof, that adherence to those principles may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement requirements'.

48 Annex III to that decision contains a letter from Mr John Kerry, then Secretary of State (United States), to the Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, to which a memorandum, Annex A, was attached, entitled 'EU-U.S. Privacy Shield Ombudsperson mechanism regarding signals intelligence', the latter of which contains the following passage:

'In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with [PPD-28], regarding signals intelligence …

… President Obama announced the issuance of a new presidential directive — PPD-28 — to "clearly prescribe what we do, and do not do, when it comes to our overseas surveillance."

Section 4(d) of PPD-28 directs the Secretary of State to designate a "Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) "to […] serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States." …

…

1. … The Senior Coordinator will serve as the Privacy Shield Ombudsperson and … will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.

…'

49 Annex VI to the Privacy Shield Decision contains a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, in which it is

stated that PPD-28 allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection'.

The dispute in the main proceedings and the questions referred for a preliminary ruling

50 Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

51 Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his or her 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.

52 On 25 June 2013, Mr Schrems filed a complaint with the Commissioner whereby he requested, in essence, that Facebook Ireland be prohibited from transferring his personal data to the United States, on the ground that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities in which the public authorities were engaged. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520, the Commission had found that the United States ensured an adequate level of protection.

53 The High Court (Ireland), before which Mr Schrems had brought judicial review proceedings against the rejection of his complaint, made a request to the Court for a preliminary ruling on the interpretation and validity of Decision 2000/520. In a judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650), the Court declared that decision invalid.

54 Following that judgment, the referring court annulled the rejection of Mr Schrems's complaint and referred that decision back to the Commissioner. In the course of the Commissioner's investigation, Facebook Ireland explained that a large part of personal data was transferred to Facebook Inc. pursuant to the standard data protection clauses set out in the annex to the SCC Decision. On that basis, the Commissioner asked Mr Schrems to reformulate his complaint.

55 In his reformulated complaint lodged on 1 December 2015, Mr Schrems claimed, inter alia, that United States law requires Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). He submitted that, since that data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, the SCC Decision cannot justify the transfer of that data to the United States. In those

circumstances, Mr Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.

56 On 24 May 2016, the Commissioner published a 'draft decision' summarising the provisional findings of her investigation. In that draft decision, she took the provisional view that the personal data of EU citizens transferred to the United States were likely to be consulted and processed by the US authorities in a manner incompatible with Articles 7 and 8 of the Charter and that US law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner found that the standard data protection clauses in the annex to the SCC Decision are not capable of remedying that defect, since they confer only contractual rights on data subjects against the data exporter and importer, without, however, binding the United States authorities.

57 Taking the view that, in those circumstances, Mr Schrems's reformulated complaint raised the issue of the validity of the SCC Decision, on 31 May 2016, the Commissioner brought an action before the High Court, relying on the case-law arising from the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 65), in order for the High Court to refer a question on that issue to the Court. By order of 4 May 2018, the High Court made the present reference for a preliminary ruling to the Court.

58 In an annex to the order for reference, the High Court provided a copy of a judgment handed down on 3 October 2017, in which it had set out the results of an examination of the evidence produced before it in the national proceedings, in which the US Government had participated.

59 In that judgment, to which the request for a preliminary ruling refers on several occasions, the referring court stated that, as a matter of principle, it is not only entitled, but is obliged, to consider all of the facts and arguments presented to it and to decide on the basis of those facts and arguments whether or not a reference is required. The High Court considers that, in any event, it is required to take into account any amendments that may have occurred in the interval between the institution of the proceedings and the hearing which it held. That court stated that, in the main proceedings, its own assessment is not confined to the grounds of invalidity put forward by the Commissioner, as a result of which it may of its own motion decide that there are other well-founded grounds of invalidity and, on those grounds, refer questions for a preliminary ruling.

60 According to the findings in that judgment, the US authorities' intelligence activities concerning the personal data transferred to the United States are based, inter alia, on Section 702 of the FISA and on E.O. 12333.

61 In its judgment, the referring court specifies that Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain 'foreign

intelligence information', and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes. In the context of the PRISM programme, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA).

62 As regards the UPSTREAM programme, that court found that, in the context of that programme, telecommunications undertakings operating the 'backbone' of the Internet — that is to say, the network of cables, switches and routers — are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a 'selector'. Under that programme, the NSA has, according to the findings of that court, access both to the metadata and to the content of the communications concerned.

63 The referring court found that E.O. 12333 allows the NSA to access data 'in transit' to the United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. It adds that activities conducted pursuant to E.O. 12333 are not governed by statute.

64 As regards the limits on intelligence activities, the referring court emphasises the fact that non-US persons are covered only by PPD-28, which merely states that intelligence activities should be 'as tailored as feasible'. On the basis of those findings, the referring court considers that the United States carries out mass processing of personal data without ensuring a level of protection essentially equivalent to that guaranteed by Articles 7 and 8 of the Charter.

65 As regards judicial protection, the referring court states that EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the Constitution of the United States, which constitutes, in United States law, the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens. In that regard, the referring court states that there are substantial obstacles in respect of the causes of action open to EU citizens, in particular that of *locus standi*, which it considers to be excessively difficult to satisfy. Furthermore, according to the findings of the referring court, the NSA's activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable. Lastly, the referring court considers that, in so far as, in its view, the Privacy Shield Ombudsperson is not a tribunal within the meaning of Article 47 of the Charter, US law does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right enshrined in that article.

66 In its request for reference preliminary ruling, the referring court also states that the parties to the main proceedings disagree, inter alia, on the applicability of EU law to transfers to a third country of personal data which are likely to be processed by the authorities of that country, inter alia, for purposes of national security and

on the factors to be taken into consideration for the purposes of assessing whether that country ensures an adequate level of protection. In particular, that court notes that, according to Facebook Ireland, the Commission's findings on the adequacy of the level of protection ensured by a third country, such as those set out in the Privacy Shield Decision, are also binding on the supervisory authorities in the context of a transfer of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.

67 As regards those standard data protection clauses, that court asks whether the SCC Decision may be considered to be valid, despite the fact that, according to that court, those clauses are not binding on the State authorities of the third country concerned and, therefore, are not capable of remedying a possible lack of an adequate level of protection in that country. In that regard, it considers that the possibility, afforded to the competent authorities in the Member States by Article 4(1)(a) of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, of prohibiting transfers of personal data to a third country that imposes requirements on the importer that are incompatible with the guarantees contained in those clauses, demonstrates that the state of the law in the third country can justify prohibiting the transfer of data, even when carried out pursuant to the standard data protection clauses in the annex to the SCC Decision, and therefore makes clear that those requirements may be insufficient in ensuring an adequate level of protection. Nonetheless, the referring court harbours doubts as to the extent of the Commissioner's power to prohibit a transfer of data based on those clauses, despite taking the view that discretion cannot be sufficient to ensure adequate protection.

68 In those circumstances, the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) In circumstances in which personal data is transferred by a private company from a European Union (EU) Member State to a private company in a third country for a commercial purpose pursuant to [the SCC Decision] and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter) apply to the transfer of the data notwithstanding the provisions of Article 4(2) TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive [95/46] in relation to public security, defence and State security?

(2) (a) In determining whether there is a violation of the rights of an individual through the transfer of data from the [European Union] to a third country under the [SCC Decision] where it may be further processed for national security purposes, is the relevant comparator for the purposes of [Directive 95/46]:

(i) the Charter, the EU Treaty, the FEU Treaty, [Directive 95/46], the [European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950] (or any other provision of EU law); or

(ii) the national laws of one or more Member States?

(b) If the relevant comparator is (ii), are the practices in the context of national security in one or more Member States also to be included in the comparator?

(3) When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of [Directive 95/46], ought the level of protection in the third country be assessed by reference to:

(a) the applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules and security measures which are complied with in the third country;

or

(b) the rules referred to in (a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non-judicial remedies as are in place in the third country?

(4) Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision] does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?

(5) Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision]:

(a) does the level of protection afforded by the United States respect the essence of an individual's right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?

If the answer to Question 5(a) is in the affirmative:

(b) are the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?

(6) (a) What is the level of protection required to be afforded to personal data transferred to a third country pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26(4) [of Directive 95/46] in light of the provisions of [Directive 95/46] and in particular Articles 25 and 26 read in the light of the Charter?

(b) What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under [the SCC Decision] satisfies the requirements of [Directive 95/46] and the Charter?

(7) Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in [the SCC Decision] preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of [Directive 95/46]?

(8) If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the [standard contractual clauses] or Article 25 and 26 of [Directive 95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of [Directive 95/46] to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [the SCC Decision], or can a data protection authority use its discretion not to suspend data flows?

(9) (a) For the purposes of Article 25(6) of [Directive 95/46], does [the Privacy Shield Decision] constitute a finding of general application binding on data protection authorities and the courts of the Member States to the effect that the United States ensures an adequate level of protection within the meaning of Article 25(2) of [Directive 95/46] by reason of its domestic law or of the international commitments it has entered into?

(b) If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the [SCC Decision]?

(10) Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III to the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data

subjects whose personal data is transferred to the United States under the [SCC Decision] that is compatible with Article 47 of the Charter]?

(11) Does the [SCC Decision] violate Articles 7, 8 and/or 47 of the Charter?'

Admissibility of the request for a preliminary ruling

69 Facebook Ireland and the German and United Kingdom Governments claim that the request for a preliminary ruling is inadmissible.

70 With regard to the objection raised by Facebook Ireland, that company observes that the provisions of Directive 95/46, on which the questions referred for a preliminary ruling are based, were repealed by the GDPR.

71 In that regard, although Directive 95/46 was, under Article 94(1) of the GDPR, repealed with effect from 25 May 2018, that directive was still in force when, on 4 May 2018, the present request for a preliminary ruling, received at the Court on 9 May 2018, was made. In addition, the first indent of Article 3(2) and Articles 25, 26 and 28(3) of Directive 95/46 cited in the questions referred, were, in essence, reproduced in Article 2(2) and Articles 45, 46 and 58 of the GDPR, respectively. Furthermore, it must be borne in mind that the Court has a duty to interpret all provisions of EU law which national courts require in order to decide the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court of Justice by those courts (judgment of 2 April 2020, *Ruska Federacija*, C-897/19 PPU, EU:C:2020:262, paragraph 43 and the case-law cited). On those grounds, the fact that the referring court referred its questions by reference solely to the provisions of Directive 95/46 cannot render the present request for a preliminary ruling inadmissible.

72 For its part, the German Government bases its objection of inadmissibility on the fact, first, that the Commissioner merely expressed doubts, and not a definitive opinion, as to the validity of the SCC Decision and, second, that the referring court failed to ascertain whether Mr Schrems had unambiguously given his consent to the transfers of data at issue in the main proceedings, which, if that had been the case, would have the effect of rendering an answer to that question redundant. Lastly, the United Kingdom Government maintains that the questions referred for a preliminary ruling are hypothetical since that court did not find that that data had actually been transferred on the basis of that decision.

73 It follows from settled case-law of the Court that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions referred concern the interpretation or the validity of a rule of EU law, the Court is in principle bound to give a ruling. It follows that questions referred by national courts enjoy a presumption of

relevance. The Court may refuse to rule on a question referred by a national court only where it appears that the interpretation sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgments of 16 June 2015, *Gauweiler and Others*, C-62/14, EU:C:2015:400, paragraphs 24 and 25; of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 45; and of 19 December 2019, *Dobersberger*, C-16/18, EU:C:2019:1110, paragraphs 18 and 19).

74 In the present case, the request for a preliminary ruling contains sufficient factual and legal material to understand the significance of the questions referred. Furthermore, and most importantly, nothing in the file before the Court leads to the conclusion that the interpretation of EU law that is requested is unrelated to the actual facts of the main action or its object, or that the problem is hypothetical, inter alia, on the basis that the transfer of the personal data at issue in the main proceedings may have been based on the express consent of the data subject of that transfer rather than based on the SCC Decision. As indicated in the request for a preliminary ruling, Facebook Ireland has acknowledged that it transfers the personal data of its subscribers residing in the European Union to Facebook Inc. and that those transfers, the lawfulness of which Mr Schrems disputes, were in large part carried out pursuant to the standard data protection clauses in the annex to the SCC Decision.

75 Moreover, it is irrelevant to the admissibility of the present request for a preliminary ruling that the Commissioner did not express a definitive opinion on the validity of that decision in so far as the referring court considers that an answer to the questions referred for a preliminary ruling concerning the interpretation and validity of rules of EU law is necessary in order to dispose of the case in the main proceedings.

76 It follows that the request for a preliminary ruling is admissible.

Consideration of the questions referred

77 As a preliminary matter, it must be borne in mind that the present request for a preliminary ruling has arisen following a complaint made by Mr Schrems requesting that the Commissioner order the suspension or prohibition, in the future, of the transfer by Facebook Ireland of his personal data to Facebook Inc. Although the questions referred for a preliminary ruling refer to the provisions of Directive 95/46, it is common ground that the Commissioner had not yet adopted a final decision on that complaint when that directive was repealed and replaced by the GDPR with effect from 25 May 2018.

78 That absence of a national decision distinguishes the situation at issue in the main proceedings from those which gave rise to the judgments of 24 September 2019, *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:772), and of

1 October 2019, *Planet49* (C-673/17, EU:C:2019:801), in which decisions adopted prior to the repeal of that directive were at issue.

79 The questions referred for a preliminary ruling must therefore be answered in the light of the provisions of the GDPR rather than those of Directive 95/46.

The first question

80 By its first question, the referring court wishes to know, in essence, whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2) TEU, must be interpreted as meaning that that regulation applies to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third country, in circumstances where, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of that third country for the purposes of public security, defence and State security.

81 In that regard, it should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR.

82 Under Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Article 4(2) of that regulation defines ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’ and mentions, by way of example, ‘disclosure by transmission, dissemination or otherwise making available’, but does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V thereof, entitled ‘Transfers of personal data to third countries or international organisations’, and also confers specific powers on the supervisory authorities for that purpose, which are set out in Article 58(2)(j) of that regulation.

83 It follows that the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR, carried out in a Member State, and falls within the scope of that regulation under Article 2(1) thereof (see, by analogy, as regards Article 2(b) and Article 3(1) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 45 and the case-law cited).

84 As to whether such an operation may be regarded as being excluded from the scope of the GDPR under Article 2(2) thereof, it should be noted that that

provision lays down exceptions to the scope of that regulation, as defined in Article 2(1) thereof, which must be interpreted strictly (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 37 and the case-law cited).

85 In the present case, since the transfer of personal data at issue in the main proceedings is from Facebook Ireland to Facebook Inc., namely between two legal persons, that transfer does not fall within Article 2(2)(c) of the GDPR, which refers to the processing of data by a natural person in the course of a purely personal or household activity. Such a transfer also does not fall within the exceptions laid down in Article 2(2)(a), (b) and (d) of that regulation, since the activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 38 and the case-law cited).

86 The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.

87 Indeed, by expressly requiring the Commission, when assessing the adequacy of the level of protection afforded by a third country, to take account, inter alia, of 'relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation', it is patent from the very wording of Article 45(2)(a) of that regulation that no processing by a third country of personal data for the purposes of public security, defence and State security excludes the transfer at issue from the application of the regulation.

88 It follows that such a transfer cannot fall outside the scope of the GDPR on the ground that the data at issue is liable to be processed, at the time of that transfer or thereafter, by the authorities of the third country concerned, for the purposes of public security, defence and State security.

89 Therefore, the answer to the first question is that Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation 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, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

The second, third and sixth questions

90 By its second, third and sixth questions, the referring court seeks clarification from the Court, in essence, on the level of protection required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country based on standard data protection clauses. In particular, the referring court asks the Court to specify which factors need to be taken into consideration for the purpose of determining whether that level of protection is ensured in the context of such a transfer.

91 As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country only if the controller or processor has provided 'appropriate safeguards', and on condition that 'enforceable data subject rights and effective legal remedies for data subjects' are available, such safeguards being able to be provided, inter alia, by the standard data protection clauses adopted by the Commission.

92 Although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to 'appropriate safeguards', 'enforceable rights' and 'effective legal remedies', it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled 'General principle for transfers', which lays down that 'all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined'. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.

93 As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country, in accordance with the objective set out in recital 6 thereof.

94 The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph would be undermined (see, by

analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 73).

95 In that context, recital 107 of the GDPR states that, where 'a third country, a territory or a specified sector within a third country … no longer ensures an adequate level of data protection. … the transfer of personal data to that third country … should be prohibited, unless the requirements [of that regulation] relating to transfers subject to appropriate safeguards … are fulfilled'. To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the regulation must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union'.

96 It follows, as the Advocate General stated in point 115 of his Opinion, that such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union.

97 The referring court also asks whether the level of protection essentially equivalent to that guaranteed within the European Union must be determined in the light of EU law, in particular the rights guaranteed by the Charter and/or the fundamental rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR'), or in the light of the national law of the Member States.

98 In that regard, it should be noted that, although, as Article 6(3) TEU confirms, the fundamental rights enshrined in the ECHR constitute general principles of EU law and although Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that convention, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (judgments of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 44 and the case-law cited, and of 20 March 2018, *Menci*, C-524/15, EU:C:2018:197, paragraph 22).

99 In those circumstances, the Court has held that the interpretation of EU law and examination of the legality of EU legislation must be undertaken in the light of the fundamental rights guaranteed by the Charter (see, by analogy, judgment of 20 March 2018, *Menci*, C-524/15, EU:C:2018:197, paragraph 24).

100 Furthermore, the Court has consistently held that the validity of provisions of EU law and, in the absence of an express reference to the national law of the Member

States, their interpretation, cannot be construed in the light of national law, even national law of constitutional status, in particular fundamental rights as formulated in the national constitutions (see, to that effect, judgments of 17 December 1970, *Internationale Handelsgesellschaft*, 11/70, EU:C:1970:114, paragraph 3; of 13 December 1979, *Hauer*, 44/79, EU:C:1979:290, paragraph 14; and of 18 October 2016, *Nikiforidis*, C-135/15, EU:C:2016:774, paragraph 28 and the case-law cited).

101 It follows that, since, first, a transfer of personal data, such as that at issue in the main proceedings, for commercial purposes by an economic operator established in one Member State to another economic operator established in a third country, falls, as is apparent from the answer to the first question, within the scope of the GDPR and, second, the purpose of that regulation is, inter alia, as is apparent from recital 10 thereof, to ensure a consistent and high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union, the level of protection of fundamental rights required by Article 46(1) of that regulation must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter.

102 The referring court also seeks to ascertain what factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses adopted under Article 46(2)(c) of the GDPR.

103 In that regard, although that provision does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies.

104 The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor 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 personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

105 Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are

transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor 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 personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

The eighth question

106 By its eighth question, the referring court wishes to know, in essence, whether Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that the competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured, or as meaning that the exercise of those powers is limited to exceptional cases.

107 In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data. Each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in that regulation (see, by analogy, as regards Article 28 of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 47).

108 It follows from those provisions that the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is clear from recital 116 of that regulation, 'when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information'. In such cases, as is stated in that recital, 'supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders'.

109 In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that

data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 63).

110 Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that 'right to an effective judicial remedy in accordance with Article 47 of the Charter' in circumstances where that supervisory authority 'does not act where such action is necessary to protect the rights of the data subject'.

111 In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.

112 Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.

113 In that regard, as the Advocate General also stated in point 148 of his Opinion, the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

114 The interpretation in the previous paragraph is not undermined by the Commissioner's reasoning that Article 4 of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, read in the light of recital 11 of that decision, confined the power of supervisory authorities to suspend or prohibit a transfer of personal data to a third country to certain exceptional circumstances. As amended by Implementing Decision 2016/2297, Article 4 of the SCC Decision refers to the power of the supervisory authorities, now under Article 58(2)(f) and (j) of the GDPR, to suspend or ban such a transfer, without confining the exercise of that power to exceptional circumstances.

115 In any event, the implementing power which Article 46(2)(c) of the GDPR grants to the Commission for the purposes of adopting standard data protection clauses does not confer upon it competence to restrict the national supervisory authorities' powers on the basis of Article 58(2) of that regulation (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraphs 102 and 103). Moreover, as stated in recital 5 of Implementing Decision 2016/2297, the SCC Decision 'does not prevent a [supervisory authority] from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law'.

116 It should, however, be pointed out that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In such a case, it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.

117 Under the fourth paragraph of Article 288 TFEU, a Commission adequacy decision is, in its entirety, binding on all the Member States to which it is addressed and is therefore binding on all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 51 and the case-law cited).

118 Thus, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection (judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 52 and the case-law cited) and, as a result, to suspend or prohibit transfers of personal data to that third country.

119 However, a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data. Similarly, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 53).

120 Thus, even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraphs 57 and 65).

121 In the light of the foregoing considerations, the answer to the eighth question is that Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

The7th and 11th questions

122 By its 7th and 11th questions, which it is appropriate to consider together, the referring court seeks clarification from the Court, in essence, on the validity of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter.

123 In particular, as is clear from the wording of the seventh question and the corresponding explanations in the request for a preliminary ruling, the referring court asks whether the SCC Decision is capable of ensuring an adequate level of protection of the personal data transferred to third countries given that the standard data protection clauses provided for in that decision do not bind the supervisory authorities of those third countries.

124 Article 1 of the SCC Decision provides that the standard data protection clauses set out in its annex are considered to offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals in accordance with the requirements of Article 26(2) of Directive 95/46. The latter provision was, in essence, reproduced in Article 46(1) and Article 46(2)(c) of the GDPR.

125 However, although those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a

third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract.

126 Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.

127 Thus, the question arises whether a Commission decision concerning standard data protection clauses, adopted pursuant to Article 46(2)(c) of the GDPR, is invalid in the absence, in that decision, of guarantees which can be enforced against the public authorities of the third countries to which personal data is or could be transferred pursuant to those clauses.

128 Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission. However, those provisions do not state that all safeguards must necessarily be provided for in a Commission decision such as the SCC Decision.

129 It should be noted in that regard that such a standard clauses decision differs from an adequacy decision adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, inter alia, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection.

130 By contrast, in the case of a Commission decision adopting standard data protection clauses, such as the SCC Decision, in so far as such a decision does not refer to a third country, a territory or one or more specific sectors in a third country, it cannot be inferred from Article 46(1) and Article 46(2)(c) of the GDPR

that the Commission is required, before adopting such a decision, to assess the adequacy of the level of protection ensured by the third countries to which personal data could be transferred pursuant to such clauses.

131 In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject' and that 'those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country'.

132 Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that 'the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses'.

133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

134 In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data,

whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135 Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.

136 Therefore, the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision.

137 That validity depends, however, on whether, in accordance with the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, such a standard clauses decision incorporates 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 the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

138 As regards the guarantees contained in the standard data protection clauses in the annex to the SCC Decision, it is clear from Clause 4(a) and (b), Clause 5(a), Clause 9 and Clause 11(1) thereof that a data controller established in the European Union, the recipient of the personal data and any processor thereof mutually undertake to ensure that the processing of that data, including the transfer thereof, has been and will continue to be carried out in accordance with 'the applicable data protection law', namely, according to the definition set out in Article 3(f) of that decision, 'the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established'. The provisions of the GDPR, read in the light of the Charter, form part of that legislation.

139 In addition, a recipient of personal data established in a third country undertakes, pursuant to Clause 5(a), to inform the controller established in the European Union promptly of any inability to comply with its obligations under the contract concluded. In particular, according to Clause 5(b), the recipient certifies that it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the contract entered into and undertakes to notify the data

controller about any change in the national legislation applicable to it which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses in the annex to the SCC Decision, promptly upon notice thereof. Furthermore, although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses.

140 Clause 5(a) and (b), in both cases to which it refers, confers on the controller established in the European Union the right to suspend the transfer of data and/or to terminate the contract. In the light of the requirements of Article 46(1) and (2)(c) of the GDPR, read in the light of Articles 7 and 8 of the Charter, the controller is bound to suspend the transfer of data and/or to terminate the contract where the recipient is not, or is no longer, able to comply with the standard data protection clauses. Unless the controller does so, it will be in breach of its obligations under Clause 4(a) in the annex to the SCC Decision as interpreted in the light of the GDPR and of the Charter.

141 It follows that Clause 4(a) and Clause 5(a) and (b) in that annex oblige the controller established in the European Union and the recipient of personal data to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses in the annex to the SCC Decision, before transferring personal data to that third country. As regards that verification, the footnote to Clause 5 states that mandatory requirements of that legislation which do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security are not in contradiction with those standard data protection clauses. Conversely, as stated by the Advocate General in point 131 of his Opinion, compliance with an obligation prescribed by the law of the third country of destination which goes beyond what is necessary for those purposes must be treated as a breach of those clauses. Operators' assessments of the necessity of such an obligation must, where relevant, take into account a finding that the level of protection ensured by the third country in a Commission adequacy decision, adopted under Article 45(3) of the GDPR, is appropriate.

142 It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.

143 If the recipient of personal data to a third country has notified the controller, pursuant to Clause 5(b) in the annex to the SCC Decision, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses in that annex, it follows from Clause 12 in that annex that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety. In any event, under Clause 6 in that annex, breach of those standard clauses will result in a right for the person concerned to receive compensation for the damage suffered.

144 It should be added that, under Clause 4(f) in the annex to the SCC Decision, a controller established in the European Union undertakes, where special categories of data could be transferred to a third country not providing adequate protection, to inform the data subject before, or as soon as possible after, the transfer. That notice enables the data subject to be in a position to bring legal action against the controller pursuant to Clause 3(1) in that annex so that the controller suspends the proposed transfer, terminates the contract concluded with the recipient of the personal data or, where appropriate, requires the recipient to return or destroy the data transferred.

145 Lastly, under Clause 4(g) in that annex, the controller established in the European Union is required, when the recipient of personal data notifies him or her, pursuant to Clause 5(b), in the event of a change in the relevant legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses, to forward any notification to the competent supervisory authority if the controller established in the European Union decides, notwithstanding that notification, to continue the transfer or to lift the suspension. The forwarding of such a notification to that supervisory authority and its right to conduct an audit of the recipient of personal data pursuant to Clause 8(2) in that annex enable that supervisory authority to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.

146 In that context, Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

147 As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on each supervisory authority on the territory of its own Member State. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued.

148 It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.

149 In the light of all of the foregoing considerations, the answer to the 7th and 11th questions is that examination of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter has disclosed nothing to affect the validity of that decision.

The 4th, 5th, 9th and 10th questions

150 By its ninth question, the referring court wishes to know, in essence, whether and to what extent findings in the Privacy Shield Decision to the effect that the United States ensures an adequate level of protection are binding on the supervisory authority of a Member State. By its 4th, 5th and 10th questions, that court asks, in essence, whether, in view of its own findings on US law, the transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision breaches the rights enshrined in Articles 7, 8 and 47 of the Charter and asks the Court, in particular, whether the introduction of the ombudsperson referred to in Annex III to the Privacy Shield Decision is compatible with Article 47 of the Charter.

151 As a preliminary matter, it should be noted that, although the Commissioner's action in the main proceedings only calls into question the SCC Decision, that action was brought before the referring court prior to the adoption of the Privacy Shield Decision. In so far as, by its fourth and fifth questions, that court asks the Court, at a general level, what protection must be ensured, under Articles 7, 8 and 47 of the Charter, in the context of such a transfer, the Court's analysis must take into consideration the consequences arising from the subsequent adoption of the Privacy Shield Decision. A fortiori that is the case in so far as the referring court asks expressly, by its 10th question, whether the protection required by Article 47 of the Charter is ensured by the offices of the ombudsperson to which the Privacy Shield Decision refers.

152 In addition, it is clear from the information provided in the order for reference that, in the main proceedings, Facebook Ireland claims that the Privacy Shield Decision is binding on the Commissioner in respect of the finding on the adequacy of the level of protection ensured by the United States and therefore in respect of the lawfulness of a transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.

153 As appears from paragraph 59 above, in its judgment of 3 October 2017, provided in an annex to the order for reference, the referring court stated that it was obliged to take account of amendments to the law that may have occurred in the interval between the institution of the proceedings and the hearing of the action before it. Thus, that court would appear to be obliged to take into account, in order to dispose of the case in the main proceedings, the change in circumstances brought about by the adoption of the Privacy Shield Decision and any binding force it may have.

154 In particular, the question whether the finding in the Privacy Shield Decision that the United States ensures an adequate level of protection is binding is relevant for the purposes of assessing both the obligations, set out in paragraphs 141 and 142 above, of the controller and recipient of personal data transferred to a third country pursuant to the standard data protection clauses in the annex to the SCC Decision and also any obligations to which the supervisory authority may be subject to suspend or prohibit such a transfer.

155 As to whether the Privacy Shield Decision has binding effects, Article 1(1) of that decision provides that, for the purposes of Article 45(1) of the GDPR, 'the United States ensures an adequate level of protection for personal data transferred from the [European] Union to organisations in the United States under the EU-U.S. Privacy Shield'. In accordance with Article 1(3) of the decision, personal data are regarded as transferred under the EU-US Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the 'Privacy Shield List', maintained and made publicly available by the US Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II to that decision.

156 As follows from the case-law set out in paragraphs 117 and 118 above, the Privacy Shield Decision is binding on the supervisory authorities in so far as it finds that the United States ensures an adequate level of protection and, therefore, has the effect of authorising personal data transferred under the EU-US Privacy Shield. Therefore, until the Court should declare that decision invalid, the competent supervisory authority cannot suspend or prohibit a transfer of personal data to an organisation that abides by that privacy shield on the ground that it considers, contrary to the finding made by the Commission in that decision, that the US legislation governing the access to personal data transferred under that privacy shield and the use of that data by the public authorities of that third country for national security, law enforcement and other public interest purposes does not ensure an adequate level of protection.

157 The fact remains that, in accordance with the case-law set out in paragraphs 119 and 120 above, when a person lodges a complaint with the competent supervisory authority, that authority must examine, with complete independence, whether the transfer of personal data at issue complies with the requirements laid down by the GDPR and, if, in its view, the arguments put forward by that person with a view to challenging the validity of an adequacy decision are well founded, bring an action before the national courts in order for them to make a reference to the Court for a preliminary ruling for the purpose of examining the validity of that decision.

158 A complaint lodged under Article 77(1) of the GDPR, by which a person whose personal data has been or could be transferred to a third country contends that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 45(3) of the GDPR, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, the issue of whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (see, by analogy, as regards Article 25(6) and Article 28(4) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 59).

159 In the present case, in essence, Mr Schrems requested the Commissioner to prohibit or suspend the transfer by Facebook Ireland of his personal data to Facebook Inc., established in the United States, on the ground that that third country did not ensure an adequate level of protection. Following an investigation into Mr Schrems's claims, the Commissioner brought the matter before the referring court and that court appears, in the light of the evidence adduced and of the competing arguments put by the parties before it, to be unsure whether Mr Schrems's doubts as to the adequacy of the level of protection ensured in that third country are well founded, despite the subsequent findings of the Commission in the Privacy Shield Decision, and that has led that court to refer the 4th, 5th and 10th questions to the Court for a preliminary ruling.

160 As the Advocate General observed in point 175 of his Opinion, those questions must therefore be regarded, in essence, as calling into question the Commission's finding, in the Privacy Shield Decision, that the United States ensures an adequate level of protection of personal data transferred from the European Union to that third country, and, therefore, as calling into question the validity of that decision.

161 In the light of the considerations set out in paragraphs 121 and 157 to 160 above and in order to give the referring court a full answer, it should therefore be examined whether the Privacy Shield Decision complies with the requirements stemming from the GDPR read in the light of the Charter (see, by analogy, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 67).

162 In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, 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 (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 96).

The Privacy Shield Decision

163 The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-US Privacy Shield, the latter being comprised, inter alia, under Article 1(2) of that decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision.

164 However, the Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading 'EU-U.S. Privacy Shield Framework Principles', that adherence to those principles may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement requirements'. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 86).

165 In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision thus enables interference, based 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 (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 87). More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333.

166 In that context, in recitals 67 to 135 of the Privacy Shield Decision, the Commission assessed the limitations and safeguards available in US law, inter alia under Section 702 of the FISA, E.O. 12333 and PPD-28, as regards access to, and use of, personal data transferred under the EU-US Privacy Shield by US public authorities for national security, law enforcement and other public interest purposes.

167 Following that assessment, the Commission found, in recital 136 of that decision, that 'the United States ensures an adequate level of protection for personal data

transferred from the [European] Union to self-certified organisations in the United States', and, in recital 140 of the decision, it considered that, 'on the basis of the available information about the U.S. legal order, … any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the [European] Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference'.

The finding of an adequate level of protection

168 In the light of the factors mentioned by the Commission in the Privacy Shield Decision and the referring court's findings in the main proceedings, the referring court harbours doubts as to whether US law in fact ensures the adequate level of protection required under Article 45 of the GDPR, read in the light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the Charter. In particular, that court considers that the law of that third country does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences. As far as concerns effective judicial protection, it adds that the introduction of a Privacy Shield Ombudsperson cannot, in its view, remedy those deficiencies since an ombudsperson cannot be regarded as a tribunal within the meaning of Article 47 of the Charter.

169 As regards, in the first place, Articles 7 and 8 of the Charter, which contribute to the level of protection required within the European Union, compliance with which must be established by the Commission before it adopts an adequacy decision under Article 45(1) of the GDPR, it must be borne in mind that Article 7 of the Charter states that everyone has the right to respect for his or her private and family life, home and communications. Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.

170 Thus, access to a natural person's personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter, which concerns any information relating to an identified or identifiable individual. Such processing of data also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 49 and 52, and of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 29; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 122 and 123).

171 The Court has held that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, judgments of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 74 and 75, and of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 33 to 36; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126).

172 However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48 and the case-law cited, and of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 33 and the case-law cited; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136).

173 In this connection, it should also be observed that, under Article 8(2) of the Charter, personal data must, inter alia, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

174 Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

175 Following from the previous point, it should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case-law cited).

176 Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that

the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited).

177 To that effect, Article 45(2)(a) of the GDPR states that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of 'effective and enforceable data subject rights' for data subjects whose personal data are transferred.

178 In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the Charter, has been called into question, inter alia, on the ground that the interference arising from the surveillance programmes based on Section 702 of the FISA and on E.O. 12333 are not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter. It is therefore necessary to examine whether the implementation of those surveillance programmes is subject to such requirements, and it is not necessary to ascertain beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter.

179 In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)'. As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'.

180 It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental

rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

181 According to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 of the FISA is, indeed, subject to the requirements of PPD-28. However, although the Commission stated, in recitals 69 and 77 of the Privacy Shield Decision, that such requirements are binding on the US intelligence authorities, the US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.

182 As regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.

183 It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.

184 It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.

185 In those circumstances, 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 the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent

to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

186 In the second place, as regards Article 47 of the Charter, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR, it should be noted that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.

187 According to settled case-law, 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. Thus, 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 her, 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 (judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95 and the case-law cited).

188 To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'. Recital 104 of the GDPR states, in that regard, that the third country 'should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress'.

189 The existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.

190 In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter has been called into question on the ground, inter alia, that the introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies which the Commission itself found in connection with the

judicial protection of persons whose personal data is transferred to that third country.

191 In that regard, the Commission found, in recital 115 of the Privacy Shield Decision, that 'while individuals, including EU data subjects, … have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered'. Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, the lack of any redress mechanism. In accordance with the case-law set out in paragraph 187 above, the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree makes it impossible to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

192 Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.

193 The Commission found, however, in recitals 115 and 116 of the Privacy Shield Decision, that, as a result of the Ombudsperson Mechanism introduced by the US authorities, as described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to that decision, and of the nature of that Ombudsperson's role, in the present instance, a 'Senior Coordinator for International Information Technology Diplomacy', the United States can be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

194 An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission's finding of limitations on the right to judicial protection must, in accordance with the requirements arising from Article 47 of the Charter and the case-law recalled in paragraph 187 above, start from the premiss that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.

195 In the letter referred to in paragraph 193 above, the Privacy Shield Ombudsperson, although described as 'independent from the Intelligence Community', was presented as '[reporting] directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided'. Furthermore, in addition to the fact that, as found by the Commission in recital 116 of that decision, the Ombudsperson is appointed by the Secretary of

State and is an integral part of the US State Department, there is, as the Advocate General stated in point 337 of his Opinion, nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman's independence from the executive (see, to that effect, judgment of 21 January 2020, *Banco de Santander*, C-274/14, EU:C:2020:17, paragraphs 60 and 63 and the case-law cited).

196 Similarly, as the Advocate General stated, in point 338 of his Opinion, although recital 120 of the Privacy Shield Decision refers to a commitment from the US Government that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Privacy Shield Ombudsperson, there is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.

197 Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

198 Therefore, in finding, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the Commission disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.

199 It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

200 Since Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.

201 In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.

202 As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016, *Borealis Polyolefine and Others*, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of

an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.

Costs

203 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 2(1) and (2) of 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), must be interpreted as meaning that that regulation 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, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.**

2. **Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor 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 personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.**

3. **Article 58(2)(f) and (j) of Regulation 2016/679 must be interpreted as meaning that, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data**

protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

4. **Examination of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.**

5. **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 is invalid.**

Lenaerts Silva de Lapuerta Arabadjiev

Prechal Vilaras Safjan

Rodin Xuereb Rossi

Jarukaitis Ilešič von Danwitz

Šváby

Delivered in open court in Luxembourg on 16 July 2020.

A. Calot Escobar K. Lenaerts

Registrar President