Reports of Cases

OPINION OF ADVOCATE GENERAL
SAUGMANDSGAARD ØE
delivered on 19 December 2019[1]

Case C-311/18

Data Protection Commissioner
v
Facebook Ireland Limited,
Maximillian Schrems,
interveners:
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

(request for a preliminary ruling
from the High Court, Ireland)

(Reference for a preliminary ruling — Protection of natural persons with regard to the processing of personal data — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfer of personal data for commercial purposes to the United States of America — Processing by the United States of America's public authorities for national security purposes of the data transferred — Article 45 — Assessment of the adequacy of the level of protection ensured in a third country — Article 46 — Appropriate safeguards offered by the controller — Standard protection clauses — Article 58(2) — Powers of the national supervisory authorities — Decision 2010/87/EU — Validity — Decision (EU) 2016/1250 — 'EU-U.S. Privacy Shield — Validity — Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union)

Table of contents

I. Introduction 3

II. Legal framework 5

A. Directive 95/46/EC 5

B. The GDPR 6

C. Decision 2010/87 10

1 Original language: French.

D. The 'privacy shield' decision 15

III. The main proceedings, the questions for a preliminary ruling and the procedure before the Court .. 15

IV. Analysis 23

A. Preliminary considerations 23

B. The admissibility of the reference for a preliminary ruling 25

1. The applicability ratione temporis of Directive 95/46 25

2. The provisional nature of the doubts expressed by the DPC 26

3. The uncertainties relating to the definition of the factual background 27

C. The applicability of EU law to transfers for commercial purposes of personal data to a third State which may process the data for national security purposes (first question) 27

D. The level of protection required in the context of a transfer based on standard contractual clauses (first part of the sixth question) 29

E. The validity of Decision 2010/87 in the light of Article 7, 8 and 47 of the Charter (seventh, eighth and eleventh questions) 30

1. The obligations placed on the controllers 32

2. The obligations placed on the supervisory authorities 34

F. The lack of necessity to respond to the other questions or to examine the validity of the 'privacy shield' decision 37

1. There is no need for the Court to answer the other questions having regard to the subject matter of the dispute in the main proceedings 38

2. The reasons why the Court should not examine the other questions having regard to the object of the procedure pending before the DPC 39

G. Alternative observations relating to the effects and the validity of the 'privacy shield' decision ... 42

1. The impact of the 'privacy shield' decision on the way in which a supervisory authority deals with a complaint relating to the legality of a transfer based on contractual safeguards 42

2. The validity of the 'privacy shield' decision 43

(a) Explanations concerning the content of the examination of the validity of an adequacy decision 44

(1) The terms of the comparison permitting an assessment of the 'essential equivalence' of the level of protection 44

(2) The need to ensure an adequate level of protection while the data are in transit ... 49

(3) The taking into consideration of the findings of fact made by the Commission and the referring court concerning United States law 51

(4) The scope of the 'essential equivalence' standard 52

(b) The validity of the 'privacy shield' decision by reference to the rights to respect for private life and to the protection of personal data 53

(1) The existence of interferences 53

(2) The requirement that the interferences be 'provided for by law' 55

(3) No compromising of the essence of the fundamental rights 57

(4) The pursuit of a legitimate objective 60

(5) The necessity and the proportionality of the interferences 61

(c) The validity of the 'privacy shield' decision by reference to the exercise of the right to an effective remedy 64

(1) The effectiveness of the judicial remedies provided for by United States law 65

(2) The impact of the Ombudsperson Mechanism on the level of protection of the right to an effective remedy 68

V. Conclusion 70

I. Introduction

1. In the absence of common personal data protection safeguards at global level, cross-border flows of such data entail a risk of a breach in continuity of the level of protection guaranteed in the European Union. Desirous of facilitating those flows while limiting that risk, the EU legislature has established three mechanisms whereby personal data may be transferred from the European Union to a third State.

2. In the first place, such a transfer may take place on the basis of a decision whereby the European Commission finds that the third State in question ensures an 'adequate level of protection' of the data transferred to it.[2] In the second place, in the absence of such a decision, the transfer is authorised when it is accompanied by 'appropriate safeguards'.[3] Those safeguards may take the form of a contract between the exporter and the importer of the data containing standard protection clauses adopted by the Commission. The GDPR makes provision, in the third place, for certain derogations, based in particular on the consent of the data subject, that allow the data to be transferred to a third country even in the absence of an adequacy decision or appropriate safeguards.[4]

2 See Article 45 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1, 'the GDPR').

3 See Article 46 of the GDPR.

4 See Article 49 of the GDPR.

3. The request for a preliminary ruling submitted by the High Court, Ireland ('the High Court') relates to the second of those mechanisms. It concerns, more specifically, the validity of Decision 2010/87/EU,[5] whereby the Commission established standard contractual clauses for certain categories of transfers, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter').

4. The request was submitted in proceedings brought by the Data Protection Commissioner, Ireland ('the DPC') against Facebook Ireland Ltd and Mr Maximillian Schrems in respect of a complaint lodged by Mr Schrems before the DPC concerning the transfer of personal data relating to him by Facebook Ireland to Facebook, Inc., its parent company, established in the United States of America ('the United States'). The DPC takes the view that the assessment of that complaint is conditional on the validity of Decision 2010/87. In that regard, it requested that the referring court seek clarification from the Court of Justice on that point.

5. Let me state at the outset that examination of the questions for a preliminary ruling has in my view disclosed nothing to affect the validity of Decision 2010/87.

6. Furthermore, the referring court has highlighted certain doubts relating, in essence, to the adequacy of the level of protection guaranteed by the United States with regard to the interferences by the United States intelligence authorities with the exercise of the fundamental rights of the individuals whose data are transferred to the United States. Those doubts indirectly called into question the assessments made by the Commission in that respect in the Implementing Decision (EU) 2016/1250.[6] Although the resolution of the dispute in the main proceedings does not require the Court to settle that issue, and although I therefore suggest that it refrain from doing so, I shall set out, in the alternative, the reasons that lead me to question the validity of that decision.

7. My analysis as a whole will be guided by the desire to strike a balance between, on the one hand, the need to show a 'reasonable degree of pragmatism in order to allow interaction with other parts of the world',[7] and, on the other hand, the need to assert the fundamental values recognised in the legal orders of the Union and its Member States, and in particular in the Charter.

5 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100, 'Decision 2010/87').

6 Commission Implementing Decision of 12 July 2016 pursuant to [Directive 95/46] on the adequacy of the protection provided by the EU-U.S Privacy Shield (OJ 2016 L 207, p. 1 (the 'privacy shield decision').

7 See speech by the former Data Protection Supervisor, P. Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', p. 49, available at the following address: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

II. Legal framework

A. Directive 95/46/EC

8. Article 3(2) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [8] provided:

'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,

…'

9. Article 13(1) of that directive was worded as follows:

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the [Union], including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.'

10. Article 25 of that directive stated:

'1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer 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.

8 Directive of the European Parliament and of the Council of 24 October 1995 (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1, 'Directive 95/46').

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; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

…

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 necessary measures to comply with the Commission's decision.'

11. Article 26(2) and (4) of that 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 … 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.'

12. Article 28(3) of Directive 95/46 was worded as follows:

'Each authority shall in particular be endowed with:

…

– 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,

…'

B. The GDPR

13. Pursuant to Article 94(1), the GDPR repealed Directive 95/46 with effect from 25 May 2018, the date from which that regulation applies, in accordance with Article 99(2) thereof.

14. Article 2(2) of that regulation provides:

'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 [EU Treaty];

…

(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.'

15. 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, 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'.

16. Article 23 of the GDPR provides:

'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;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State …

…

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 of 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.'

17. Article 44 of that regulation, entitled 'General principle for transfers', states:

'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.'

18. In accordance with Article 45 of that regulation, entitled 'Transfers on the basis of an adequacy decision':

'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. …

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of [Directive 95/46].

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retroactive effect. …

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

…

9. Decisions adopted by the Commission on the basis of Article 25(6) of [Directive 95/46] shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.'

19. Article 46 of that regulation, entitled 'Transfers subject to appropriate safeguards', is worded as follows:

'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:

…

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

…

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of [Directive 95/46] shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of [Directive 95/46] shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.'

20. In the words of Article 58(2), (4) and (5) of the GDPR:

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

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

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

…

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(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.

5. Each Member State shall provide by law that its supervisory authority [is to] have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.'

C. Decision 2010/87

21. Article 26(4) of Directive 95/46 gave rise to the adoption by the Commission of three decisions in which it found that the standard contractual clauses set out therein afford sufficient safeguards in the light of the protection of the private life and freedoms and the fundamental rights of persons, and also with regard to the exercise of the corresponding rights ('the SCC decisions').[9]

9 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive [95/46] (OJ 2001 L 181, p. 19); Commission Decision 2004/915/EC of 27 December 2004 amending Decision [2001/497] as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (OJ 2004 L 385, p. 74); and Decision 2010/87.

22. Those decisions include Decision 2010/87, Article 1 of which provides that '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]'.

23. Pursuant to Article 3 of that decision:

'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;

…'

24. In its initial version Article 4 of that decision provided, in paragraph 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.'

25. In its current version, as resulting from the amendment of Decision 2010/87 by Implementing Decision (EU) 2016/2297,[10] Article 4 of Decision 2010/87 states that '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'.

26. The annex to Decision 2010/87 contains a number of standard contractual clauses. In particular, Clause 3 in that annex, entitled '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.

…'

27. Clause 4 in that annex, entitled 'Obligations of the data exporter', provides:

'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;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

10 Commission Decision of 16 December 2016 amending Decisions [2001/497] and [2010/87] on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive [95/46] (OJ 2016 L 344, p. 100).

(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;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).'

28. Clause 5 in the same annex, entitled 'Obligations of the data importer ([1])', states:

'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;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(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;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

…'

29. According to footnote 1, to which the title of Clause 5 in the annex to Decision 2010/87 refers:

'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. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.'

30. Clause 6 in that annex, entitled 'Liability', is worded as follows:

'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, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. …

…'

31. Clause 7 in that annex, entitled 'Mediation and jurisdiction', provides:

'1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer to dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.'

32. Clause 9 in that annex, entitled 'Governing law', provides that the standard contractual clauses are to be governed by the law of the Member State in which the data exporter is established.

D. The 'privacy shield' decision

33. Article 25(6) of Directive 95/46 served as the basis for the adoption by the Commission of two successive decisions whereby it found that the United States ensured an adequate level of protection of the personal data transferred to undertakings established in the United States which declared that they adhered, by means of a self-certification procedure, to the principles set out in those decisions.

34. Initially, the Commission adopted Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.[11] In the judgment of 6 October 2015, *Schrems*,[12] the Court declared that decision invalid.

35. Following that judgment, the Commission then adopted the 'privacy shield' decision.

36. Article 1 of that decision provides:

'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, 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.'

37. Annex III A to that decision, entitled 'EU-U.S. Privacy Shield Ombudsperson mechanism regarding signals intelligence', attached to a letter from Mr John Kerry, the then United States Secretary of State, dated 7 July 2016, contains a memorandum describing a new mediation procedure before a 'Senior Coordinator for International Information Technology Diplomacy' ('the Ombudsperson') designated by the Secretary of State.

38. In the words of that memorandum, that procedure was put in place in order 'to facilitate the processing of requests relating to national security access to data transmitted from the [Union] to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCSs), "Derogations" or "Possible Future Derogations", through established avenues under applicable United States laws and policy, and the response to those requests'.

III. The main proceedings, the questions for a preliminary ruling and the procedure before the Court

39. Mr Schrems, an Austrian national residing in Austria, is a user of the social network Facebook. All users of that social network residing in the territory of the European Union are required, when signing up, to enter into a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is established in the United States. Those users' personal data are transferred, in whole or in part, to servers belonging to Facebook Inc. situated in the territory of the United States, where they are processed.

11 Decision of 26 July 2000 pursuant to Directive [95/46] (OJ 2000 L 215, p. 7, 'the "safe harbour" decision').

12 C-362/14 (EU:C:2015:650, 'the judgment in *Schrems*').

40. On 25 June 2013, Mr Schrems filed a complaint with the DPC whereby he requested her, in essence, to prohibit Facebook Ireland from transferring the personal data relating to him to the United States. He claimed that the law and practices in force in the United States did not ensure adequate protection of the personal data retained in its territory against intrusions resulting from the surveillance activities practised by the public authorities. Mr Schrems referred in that regard to the revelations made by Mr Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency (NSA).

41. That complaint was rejected on the ground, in particular, that any question relating to the adequacy of the protection afforded in the United States had to be settled in accordance with the 'safe harbour' decision. In that decision, the Commission had found that the United States offered an adequate level of protection for personal data transferred to undertakings in its territory that adhered to the principles set out in that decision.

42. Mr Schrems brought an action against the decision rejecting his complaint before the High Court, which considered that, although Mr Schrems had not formally contested the validity of the 'safe harbour' decision, his complaint impugned, in reality, the legality of the regime established by that decision. In those circumstances, the High Court referred a number of questions to the Court, seeking, in essence, to ascertain whether the authorities of the Member States responsible for data protection (the 'supervisory authorities'), when dealing with a complaint concerning the protection of the rights and freedoms of a person in regard to the processing of personal data relating to him which have been transferred to a third State, are bound by the findings as to the adequacy of the level of protection afforded by that third State made by the Commission pursuant to Article 25(6) of Directive 95/46, when the complainant disputes those findings.

43. After holding, in paragraphs 51 and 52 of the judgment in *Schrems*, that an adequacy decision is binding on the supervisory authorities until such time as it is declared invalid, the Court stated the following in paragraphs 63 and 65 of that judgment:

'63. … where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim …, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

…

65. In the … situation … where the national supervisory authority considers that the objections advanced by [that person] are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.'

44. The Court also examined in that judgment the validity of the 'safe harbour' decision by reference to the requirements arising under Directive 95/46, read in the light of the Charter. After doing so, it declared that decision invalid. [13]

13 See judgment in *Schrems* (paragraph 106).

45. Following the judgment in *Schrems*, the referring court annulled the decision whereby the DPC had rejected Mr Schrems' complaint and referred that decision back to the DPC for assessment. The DPC opened an investigation and requested Mr Schrems to reformulate his complaint having regard to the declaration that the 'safe harbour' decision was invalid.

46. To that end, Mr Schrems asked Facebook Ireland to identify the legal bases for the transfer of personal data of users of the Facebook social network from the European Union to the United States. Facebook Ireland, without identifying all the legal bases on which it relies, referred to a data transfer processing agreement between it and Facebook Inc., which had been applicable since 20 November 2015, and relied on Decision 2010/87.

47. In his reformulated complaint, Mr Schrems claims, first, that the clauses in that agreement are not consistent with the standard contractual clauses in the annex to Decision 2010/87. Second, Mr Schrems asserts that those standard contractual clauses could not in any event justify the transfer of the personal data relating to him to the United States. That is so because under United States law Facebook Inc. is required make the personal data of its users available to United States authorities, such as the NSA and the Federal Bureau of Investigation (FBI), in the context of surveillance programmes that impede the exercise of the rights guaranteed in Articles 7, 8 and 47 of the Charter. Mr Schrems claims that there is no remedy that would allow the data subjects to rely on their rights to respect for private life and to protection of personal data. In those circumstances, Mr Schrems asks the DPC to suspend the transfer of such data in application of Article 4 of Decision 2010/87.

48. Facebook Ireland recognised, in the context of the DPC's investigation, that it continues to transfer the personal data of the users of the social network Facebook, who reside in the Union, to the United States and that in doing so it relies largely on the standard contractual clauses in the annex to Decision 2010/87.

49. The DPC's investigation sought to determine, first, whether the United States ensures adequate protection of the personal data of citizens of the Union and, second, whether the SCC decisions offer sufficient safeguards as regards the protection of those citizens' fundamental rights and freedoms.

50. In that regard, in a draft decision, the DPC considered provisionally that United States law does not offer effective remedies in accordance with Article 47 of the Charter to citizens of the Union whose data are transferred to the United States, where they are liable to be processed by the United States agencies for national security purposes in a way that is incompatible with Articles 7 and 8 of the Charter. The safeguards provided for in the clauses in the annex to the SCC decisions do not make up for that deficiency, since they are not binding on the United States authorities or agencies and they confer on the data subjects only contractual rights against the data exporter and/or importer.

51. In those circumstances, the DPC considered that it was impossible to adjudicate on Mr Schrems' complaint unless the Court examined the validity of the SCC decisions. In accordance with paragraph 65 of the judgment in *Schrems*, the DPC therefore brought proceedings before the referring court so that, if it shared the DPC's doubts, it would make a reference to the Court for a preliminary ruling on the validity of those decisions.

52. The United States Government, the Electronic Privacy Information Centre (EPIC), the Business Software Alliance (BSA) and Digitaleurope were granted leave to intervene before the referring court.

53. In order to determine whether it shares the doubts expressed by the DPC as to the validity of the SCC decisions, the High Court took evidence from the parties to the dispute and heard argument from them and from the interveners. In particular, evidence relating to the provisions of United States law was submitted by experts. In Irish law, foreign law is considered to be a point of fact to be established by evidence like any other fact. On the basis of that evidence, the referring court assessed the provisions of United States law that authorise surveillance by the Government authorities and

agencies, the operation of two publicly recognised surveillance programmes ('PRISM' and 'Upstream'), the various remedies available for individuals whose rights have been violated by surveillance measures and the systematic safeguards and supervisory mechanisms. The High Court set out the results of that assessment in a judgment of 3 October 2017 annexed to its order for reference ('the judgment of the High Court of 3 October 2017').

54. In that judgment, the referring court cited, among the legal bases authorising the interception of foreign communications by the United States intelligence services, section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 ('EO 12333').

55. According to the findings made in that judgment, section 702 of the FISA allows the United States Attorney General and the United States Director of National Intelligence (DNI) to authorise jointly, for a period of one year, in order to obtain foreign intelligence information, the surveillance of individuals who are not United States citizens and are not permanently resident in the United States (known as 'non-United States persons') who are reasonably believed to be located outside the United States.[14] In the words of the FISA, 'foreign intelligence information' means information that relates to the ability of the Government to protect against foreign attacks, terrorism, the proliferation of weapons of mass destruction and the conduct of the foreign affairs of the United States.[15]

56. Those annual authorisations, like the procedures governing the targeting of persons to be surveilled and the processing ('minimisation') of the information gathered,[16] must be approved by the United States Foreign Intelligence Surveillance Court (FISC). While the 'traditional' surveillance carried out on the basis of other provisions of the FISA requires that 'probable cause' giving rise to suspicion that the persons surveilled belong to or are the agents of a foreign power be shown, the surveillance activities carried out under section 702 of the FISA do not depend either on such 'probable cause' being shown or on the targeting of specific persons being approved by the FISC. In addition, still according to the findings of the referring court, the minimisation procedures do not apply to non-United States persons located outside the United States.

57. In practice, when authorisation has been granted by the FISC, the NSA sends to electronic communications services providers established in the United States orders containing search criteria, called 'selectors', associated with the targeted persons (such as telephone numbers or email addresses). Those providers are then required to supply the data corresponding to the selectors to the NSA and must keep secret the orders issued to them. They may make application to the FISC to modify or set aside a directive issued by the NSA. The decision of the FISC may be the subject of an appeal to the Foreign Intelligence Surveillance Court of Review (FISCR).

58. The High Court found that section 702 of the FISA serves as the legal basis for the PRISM and Upstream programmes.

59. In the context of the PRISM programme, the electronic communications services providers are required to submit to the NSA all communications 'from' or 'to' the selector communicated by the NSA. Some of those communications are sent to the FBI and the United States Central Intelligence Agency (CIA). In 2015, 94 386 persons were surveilled and in 2011 the United States Government obtained more than 250 million communications in the context of that programme.

14 50 U.S.C. 1881 (a).

15 50 U.S.C. 1881 (e).

16 The referring court found that the targeting procedures concern the way in which the executive determines that a particular person may reasonably be considered to be a non-United States person located outside the United States and that the targeting of that person may lead to the acquisition of foreign intelligence information. The minimisation procedures cover the acquisition, retention, use and dissemination of any non-public information relating to a U.S. person acquired under section 702 of the FISA.

60. The Upstream programme is based on the compelled assistance of undertakings operating the 'backbone' — namely the network of cables, switches and routers — over which telephonic communications and internet communications transit. Those undertakings are required to allow the NSA to copy and filter internet traffic flows in order to acquire communications 'from', to' or 'about' a selector mentioned in a directive from that agency. Communications 'about' a selector designate the communications which refer to that selector, without the non-United States person associated with that selector necessarily being a participant in that communication. Although it follows from an opinion of the FISC of 26 April 2017 that since that date the United States Government has no longer collected or acquired communications 'about' a selector, that opinion does not indicate that the NSA has stopped copying and searching communications flows as they pass through its surveillance equipment. The Upstream programme thus entails access by the NSA to both the metadata and the content of the communications. Since 2011 the NSA has received around 26.5 million communications per annum in the context of the Upstream programme, which, however, represents only a small portion of the communications subject to the filtering process carried out on the basis of that programme.

61. Furthermore, according to the findings of the High Court, EO 12333 authorises the surveillance of electronic communications outside the United States by permitting access, for foreign intelligence purposes, to data either 'in transit' to the United States or 'transiting' through the United States but not intended to be processed there, and also the collection and retention of those data. EO 12333 defines 'foreign intelligence' as including information relating to the capabilities, intentions and activities of foreign powers, organisations or persons. [17]

62. EO 12333 authorises the NSA to access the underwater cables on the floor of the Atlantic Ocean by means of which data are transferred from the EU to the United States before they arrive in the United States and are thus subject to the provisions of the FISA. However, there is no evidence of any programme having been implemented pursuant to that presidential order.

63. Although EO 12333 sets limits on the collection, retention and dissemination of information, those limits do not apply to non-United States persons. The latter benefit solely from the guarantees set out in Presidential Policy Directive 28 ('PPD 28'), which applies to all activities involving the collection and use of foreign intelligence signals information. PPD 28 provides that respect for privacy is an integral part of the considerations to be taken into account in the planning of those activities, that the collection must be aimed solely at the acquisition of foreign intelligence information and counter-intelligence and that the activities must be 'as tailored as feasible'.

64. According to the referring court, the NSA's activities based on EO 12333, which may be amended or revoked at any time by the President of the United States, are not governed by statute, are not subject to judicial oversight and are not justiciable.

65. On the basis of those findings, the referring court considers that the United States carries out mass and indiscriminate processing of personal data that might expose the data subjects to a risk of a violation of the rights which they derive from Articles 7 and 8 of the Charter.

66. In addition, the referring court indicates that EU citizens do not have access to the same remedies against the unlawful processing of their personal data by the United States authorities as United States nationals. The Fourth Amendment to the Constitution of the United States, which constitutes the most important protection against unlawful surveillance, is inapplicable to EU citizens who do not have a significant voluntary connection with the United States. While they do have certain other remedies, those remedies encounter substantial obstacles.

17 EO 12333, paragraph 3.5(e).

67. In particular, under Article III of the United States Constitution any action before the Federal Courts is subject to the person concerned showing that he has 'standing'. Standing assumes, in particular, that that person concerned shows that he has suffered an injury in fact, which is (a) concrete and particularised and (b) actual or imminent. Referring, inter alia, to the judgment of the Supreme Court of the United States in *Clapper v. Amnesty International US*,[18] the referring court considers that that condition is in practice very difficult to satisfy, in view, in particular, of the absence of any obligation to inform the data subjects of the surveillance measures taken against them.[19] A part of the actions available to EU citizens is, moreover, subject to compliance with other restrictive conditions, such as the need to establish pecuniary loss. The sovereign immunity conferred on the intelligence agencies and the classification of the information concerned also constitute an obstacle to the exercise of certain remedies.[20]

68. The High Court also mentions various review and oversight mechanisms applicable to the activities of the intelligence agencies.

69. These include, first, the mechanism of annual certification by the FISC of the programmes based on section 702 of the FISA, although the FISC does not approve individual selectors. Nor is there any prior judicial oversight of the collection of foreign intelligence information under EO 12333.

70. Second, the referring court makes reference to numerous non-judicial oversight mechanisms applicable to intelligence activities. It mentions, in particular, the role of the United States Inspectors General, who, within each intelligence agency, are responsible for overseeing intelligence activities. In addition, the United States Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive, receives reports from designated persons within each agency acting as civil liberties or privacy officers. The PCLOB regularly reports to the congressional committees and the President. The agencies concerned must report incidents of non-compliance with the rules and procedures governing the collection of foreign intelligence information to, among others, the DNI. Those incidents are also reported to the FISC. The United States Congress, through the intelligence committees of the House of Representatives and the Senate, is also responsible for overseeing foreign intelligence activities.

71. However, the High Court emphasises the fundamental difference between, on the one hand, the rules designed to ensure that the data are obtained in accordance with the law and that, once obtained, they are not misused and, on the other hand, the remedies available when those rules are broken. The protection of the fundamental rights of the data subjects can be ensured only if effective remedies enable them to enforce their rights in the event of non-compliance with those rules.

72. In those circumstances, the referring court considers that the arguments put forward by the DPC, according to which the limitations imposed by United States law on the right to a remedy of the persons whose data are transferred from the EU do not respect the essence of the right guaranteed by Article 47 of the Charter and, in any event, constitute disproportionate interferences with the exercise of that right, are well founded.

18 133 S.Ct. 1138 (2013).

19 The referring court found, however, that there is an exception to the principle that the notification of the person subject to a surveillance measure is not required, where the United States Government seeks to use data collected pursuant to section 702 of the FISA against that person in criminal or administrative proceedings.

20 In particular, the referring court observed that, although the Judicial Redress Act (JRA) extended to citizens of the Union the provisions of the Privacy Act, which allows access by natural persons to information concerning them retained by certain agencies in connection with certain third countries, the NSA is not among the agencies designated under the JRA.

73. According to the High Court, the introduction by the United States Government of the Ombudsperson Mechanism described in the 'privacy shield' decision does not undermine that assessment. After emphasising that that mechanism is available to EU citizens who consider on a reasonable basis that their data have been transferred in accordance with the SCC decisions,[21] the High Court observed that the Ombudsperson is not a tribunal that satisfies the requirements of Article 47 of the Charter and, in particular, is not independent of the executive.[22] It also doubts that the intervention of the Ombudsperson, whose decisions are not amenable to appeal, represents an effective remedy. In fact, that intervention does not enable the persons whose data have been illegally seized, processed or shared to recover damages or obtain an injunction to prevent future wrongdoing, since the Ombudsperson neither confirms nor denies that a person has been subjected to an electronic surveillance measure.

74. Having thus set out its concerns as to the essential equivalence between the safeguards provided by United States law and the requirements arising under Articles 7, 8 and 47 of the Charter, the referring court questioned whether the standard contractual clauses provided for in the SCC decisions — which, by their nature, are not binding on the United States authorities — may nonetheless ensure the protection of the data subjects' fundamental rights. It concluded that it shared the DPC's doubts as to the validity of those decisions.

75. In that regard, the referring court considers, in particular, that Article 28(3) of Directive 95/46, to which Article 4 of Decision 2010/87 makes reference, in that it authorises the supervisory authorities to suspend or prohibit the transfer of data on the basis of the standard contractual clauses provided for in that decision, does not suffice to dispel those doubts. Apart from the fact that in its view that power is merely discretionary, the referring court wonders, in the light of recital 11 of Decision 2010/87, whether that power can be exercised when the deficiencies found do not relate to a particular and exceptional case, but are general and systemic.[23] It also considers that the risk that divergent decisions may be made in different Member States might preclude the finding of such shortcomings being entrusted to the supervisory authorities.

76. In those circumstances, the High Court decided, by decision of 4 May 2018,[24] received at the Court on 9 May 2018, to stay proceedings and to refer the following questions to the Court 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 [Decision 2010/87] 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) of 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?

21 The referring court refers, in that respect, to Annex IIIA to the 'privacy shield' decision (see points 37 and 38 of this Opinion).

22 The referring court refers to the judgment of 27 January 2005, *Denuit and Cordenier* (C-125/04, EU:C:2005:69, paragraph 12).

23 Recital 11 of Decision 2010/87 states: '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.'

24 Facebook Ireland appealed against the decision to refer before the Supreme Court of Ireland. That appeal was dismissed by judgment of 31 May 2019, *The Data Protection Commissioner* v. *Facebook Ireland Limited and Maximillian Schrems*, Appeal No 2018/68 ('the judgment of the Supreme Court of 31 May 2019').

(2) (a) In determining whether there is a violation of the rights of an individual through the transfer of data from the EU to a third country under [Decision 2010/87] where it may be further processed for national security purposes, is the relevant comparator for the purposes of Directive [95/46]:

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

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

(b) If the relevant comparator is (b), 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 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 EU to the US under [Decision 2010/87] 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 EU to the US under [Decision 2010/87]:

(a) does the level of protection afforded by the US 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 (a) is yes,

(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 [that Directive] 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 [Decision 2010/87] 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 [Decision 2010/87] 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 [supervisory 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 the Directive to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [Decision 2010/87], or can a [supervisory 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 [the supervisory authorities] and the courts of the Member States to the effect that the US ensures an adequate level of protection within the meaning of Article 25(2) of [Directive 95/46] by reason of its domestic law or 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 [Decision 2010/87]?

(10) Given the findings of the High Court in relation to US law, does the provision of the "privacy shield" Ombudsperson under Annex III A 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 US under [Decision 2010/87] that is compatible with Article 47 of the Charter?

(11) Does [Decision 2010/87] violate Articles 7, 8 and/or 47 of the Charter?'

77. The DPC, Facebook Ireland, Mr Schrems, the United States Government, the EPIC, the BSA, Digitaleurope, Ireland, the Belgian, Czech, German, Netherlands, Austrian, Polish, Portuguese and United Kingdom Governments, the European Parliament and the Commission lodged written observations before the Court. The DPC, Facebook Ireland, Mr Schrems, the United States Government, the EPIC, the BSA, Digitaleurope, Ireland, the German, French, Netherlands, Austrian and United Kingdom Governments, the Parliament, the Commission and the European Data Protection Board (EPDB) were represented at the hearing on 9 July 2019.

IV. Analysis

A. Preliminary considerations

78. Following the declaration by the Court in the judgment in *Schrems* that the 'safe harbour' decision was invalid, transfers of personal data to the United States have continued on the basis of other legal provisions. In particular, data-exporting companies have been able to make use of contracts with data importers, incorporating standard clauses drawn up by the Commission. Those clauses also serve as the legal basis for transfers to a multitude of other third countries in respect of which the

Commission has not adopted an adequacy decision.[25] The 'privacy shield' decision now allows undertakings which have self-certified their adherence to the principles set out in that decision to transfer personal data to the United States without further formalities.

79. As the order for reference expressly states, and as the BSA, Digitaleurope, Ireland, the Austrian and French Governments, the Parliament and the Commission have emphasised, the sole issue in the proceedings before the High Court is whether the decision whereby the Commission established the standard contractual clauses relied on in support of the transfers to which Mr Schrems' complaint relates, namely Decision 2010/87,[26] is valid.

80. The dispute has its origin in an application whereby the DPC requested the referring court to refer to the Court a question for a preliminary ruling on the validity of Decision 2010/87. According to the referring court, the dispute in the main proceedings therefore concerns the exercise of the remedy which the Court enjoined the Member States to provide for in paragraph 65 of the judgment in *Schrems*.

81. It will be recalled that the Court held, in paragraph 63 of that judgment, that a supervisory authority is required to deal with all due diligence with a complaint in which a person whose personal data have been or could be transferred to a third country which has been the subject of an adequacy decision disputes the compatibility of that decision with the fundamental rights enshrined in the Charter. In the words of paragraph 65 of that judgment, where the supervisory authority considers that the objections advanced in that complaint are well founded, it must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46 (to which Article 58(5) of the GDPR corresponds), read in the light of Article 8(3) of the Charter, be able to engage in legal proceedings. In that regard, it is incumbent upon the national legislature to provide for legal remedies enabling the person concerned to put forward those objections before the national courts in order for them, if they share the supervisory authority's doubts, to make a reference for a preliminary ruling on the validity of the decision at issue.

82. Like the referring court, I consider that those findings apply by analogy when a supervisory authority, when assessing a complaint brought before it, doubts the validity not of an adequacy decision but of a decision, such as Decision 2010/87, setting out standard contractual clauses for the transfer of personal data to third countries. Contrary to the view put forward by the German government, it is not determinative that those doubts are raised by the complainant in arguments before the supervisory authority or that that authority questions, of its own motion, the validity of the decision at issue. In fact, the requirements arising under Article 58(5) of the GDPR and Article 8(3) of the Charter, on which the Court's reasoning is based, apply irrespective of the legal basis of the transfer referred to in the complaint lodged with the supervisory authority and of the reasons leading that authority to question the validity of the decision at issue in the context of the adjudication of that compliant.

83. That being said, the reason why the DPC asked the referring court to question the Court about the validity of Decision 2010/87 was because she considers that clarification by the Court on that point seems to be necessary in order for her to adjudicate on the complaint whereby Mr Schrems requests her to exercise her power, under the second indent of Article 28(3) of Directive 95/46 — and now conferred by Article 58(2)(f) of the GDPR — to suspend the transfer of the personal data relating to him by Facebook Ireland to Facebook Inc.

25 The BSA confirms that 70% of the undertakings which are members of that alliance that responded to an investigation into the matter stated that they used standard contractual clauses as the principal basis of transfers of personal data to third countries. Digitaleurope also considers that the standard contractual clauses represent the main legal instrument relied on in support of those transfers.

26 Although the referring court states that its request for a preliminary ruling concerns the validity of the three SCC decisions, which are examined in the DPC's draft decision and in the judgment of 3 October 2017, the questions for a preliminary ruling relate exclusively to Decision 2010/87. The same applies since, before that court, Facebook Ireland identified that decision as the legal basis of the transfers of the data of European users of the Facebook social network to the United States. My analysis will therefore relate solely to that decision.

84. Thus, while the dispute in the main proceedings relates solely to the validity *in abstracto* of Decision 2010/87, the underlying procedure pending before the DPC relates to the exercise by her of her power to adopt corrective measures *in a specific case*. I shall propose that the Court confine itself to examining the questions before it to the extent necessary to adjudicate on the validity of Decision 2010/87, since such an examination will suffice to put the referring court in a position to settle the dispute pending before it. [27]

85. Before I assess the validity of that decision, it is appropriate to dismiss certain objections raised against the admissibility of the request for a preliminary ruling.

B. The admissibility of the reference for a preliminary ruling

86. The admissibility of the request for a preliminary ruling has been contested for various reasons relating, essentially, to the non-applicability *ratione temporis* of Directive 95/46 referred to in the questions (section 1), to the fact that the procedure before the DPC has not reached a sufficiently advanced stage to justify the utility of such a request (section 2) and to the existence of uncertainties with regard to the factual background described by the referring court (section 3).

87. I shall address those pleas of inadmissibility while bearing in mind the presumption of relevance enjoyed by questions referred to the Court under Article 267 TFEU. According to a consistent line of decisions, the Court may refuse to rule on a question referred for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, 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. [28]

1. The applicability ratione temporis of Directive 95/46

88. Facebook Ireland submits that the questions for a preliminary ruling are inadmissible on the ground that they refer to Directive 95/46, when that directive was repealed and replaced by the GDPR with effect from 25 May 2018. [29]

89. I share the view that the validity of Decision 2010/87 must be examined by reference to the provisions of the GDPR.

90. In accordance with Article 94(2) of that regulation, 'references to the repealed Directive shall be construed as references to [that regulation]'. It follows, in my view, that Decision 2010/87, in that it mentions as a legal basis Article 26(4) of Directive 95/46, must be understood as referring to Article 46(2)(c) of the GDPR, which essentially reproduces the content of the former provision. [30] Consequently, the implementing decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46, before the entry into force of the GDPR, must be interpreted in the light of that regulation. It is also by reference to that regulation that their validity must, where necessary, be evaluated.

27 See points 167 to 186 of this Opinion.

28 See, in particular, judgments of 10 December 2018, *Wightman and Others* (C-621/18, EU:C:2018:999, paragraph 27), and of 19 November 2019, *A.K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)* (C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 98).

29 See Article 94(1) and Article 99(1) of the GDPR.

30 I would emphasise that, in accordance with Article 46(5) of the GDPR, decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46 are to remain in force until amended, replaced or repealed.

91. That conclusion is not affected by the case-law according to which the legality of an EU measure must be assessed on the basis of the facts and the law as they stood at the time when the measure was adopted. That case-law relates to the examination of the validity of an EU measure in the light of the relevant factual circumstances at the time of its adoption [31] or the procedural rules governing its adoption. [32] Conversely, the Court has repeatedly examined the validity of acts of secondary law against higher-ranking substantive norms that have come into force after the adoption of those acts. [33]

92. However, while the designation, in the wording of the questions for a preliminary ruling, of a measure which is no longer applicable *ratione temporis* justifies the reformulation of those questions, it cannot render them inadmissible. [34] As the DPC and Mr Schrems have claimed, the references to Directive 95/46 in the wording of the questions for a preliminary ruling may, moreover, be explained by the procedural calendar of the present case, as the questions were referred to the Court before the GDPR entered into force.

93. In any event, the provisions of the GDPR that will be addressed for the purposes of the analysis of the questions for a preliminary ruling — namely, in particular, Articles 45, 46 and 58 — essentially reproduce, while developing it and introducing certain nuances, the content of Articles 25, 26 and 28 of Directive 95/46. As regards their relevance for the purposes of adjudicating on the validity of Decision 2010/87, I see no reason to attribute to those provisions of the GDPR a scope different from that of the corresponding provisions of Directive 95/46. [35]

2. The provisional nature of the doubts expressed by the DPC

94. In the German Government's submission, the request for a preliminary ruling is inadmissible on the ground that the remedy referred to in paragraph 65 of the judgment in *Schrems* assumes that the supervisory authority has formed a definitive opinion as to the merits of the complaints put forward by the applicant against the validity of the decision at issue. That, it submits, is not the case here, since the DPC expressed her doubts as to the validity of Decision 2010/87 which, moreover, Mr Schrems does not contest in a draft decision, delivered provisionally without prejudice to further observations being lodged by Facebook Ireland and Mr Schrems.

95. To my mind, the provisional nature of the doubts expressed by the DPC has no impact on the admissibility of the reference for a preliminary ruling. The criteria as to the admissibility of a question for a preliminary ruling must be assessed by reference to the subject matter of the dispute as defined by the referring court. [36] It is common ground that that dispute concerns the validity of Decision 2010/87. According to the order for reference and the judgment annexed thereto, the referring court considered that the doubts expressed by the DPC — irrespective of whether they were provisional or definitive — are well founded and therefore asked the Court to rule on the validity of that decision. In those circumstances, the light that the Court will shed on that subject is undoubtedly relevant for the purpose of enabling the referring court to resolve the dispute before it.

31 See, in particular, judgments of 7 February 1979, *France* v *Commission* (15/76 and 16/76, EU:C:1979:29, paragraph 7); of 17 May 2001, *IECC* v *Commission* (C-449/98 P, EU:C:2001:275, paragraph 87); and of 17 October 2013, *Schaible* (C-101/12, EU:C:2013:661, paragraph 50).

32 See, in particular, judgments of 16 April 2015, *Parliament* v *Council* (C-540/13, EU:C:2015:224, paragraph 35); of 16 April 2015, *Parliament* v *Council* (C-317/13 and C-679/13, EU:C:2015:223, paragraph 45); and of 22 September 2016, *Parliament* v *Council* (C-14/15 and C-116/15, EU:C:2016:715, paragraph 48).

33 In particular, in the judgment in *Schrems*, the Court assessed the validity of the 'safe harbour' decision in the light of the provisions of the Charter, the adoption of which postdates the adoption of that decision. See also judgments of 17 March 2011, *AJD Tuna* (C-221/09, EU:C:2011:153, paragraph 48), and of 11 June 2015, *Pfeifer & Langen* (C-51/14, EU:C:2015:380, paragraph 42).

34 See, in particular, judgments of 15 July 2010, *Pannon Gép Centrum* (C-368/09, EU:C:2010:441, paragraphs 30 to 35); of 10 February 2011, *Andersson* (C-30/10, EU:C:2011:66, paragraphs 20 and 21); and of 25 October 2018, *Roche Lietuva* (C-413/17, EU:C:2018:865, paragraphs 17 to 20).

35 See, in that regard, Opinion of Advocate General Bobek in *Fashion ID* (C-40/17, EU:C:2018:1039, point 87).

36 See point 87 of this Opinion.

3. The uncertainties relating to the definition of the factual background

96. The United Kingdom Government submits that the factual background described by the referring court reveals a number of deficiencies that compromise the admissibility of the questions referred for a preliminary ruling. It maintains that the referring court has not made clear whether the personal data relating to Mr Schrems were actually transferred to the United States or, if they were, whether they were collected by the United States authorities. Nor was the legal basis for those transfers identified with certainty, as the order for reference merely mentions that the data of European users of the social network Facebook are transferred 'in large part' on the basis of the standard contractual clauses provided for in Decision 2010/87. It has not in any event been established that the contract between Facebook Ireland and Facebook Inc., relied on in support of the transfer at issue, faithfully incorporates those clauses. The German Government also disputes the admissibility of the reference for a preliminary ruling on the ground that the referring court did not examine whether Mr Schrems undoubtedly consented to the transfers in question, in which case they were validly based on Article 26(1) of Directive 95/46 (the content of which is essentially reproduced in Article 49(1)(a) of the GDPR).

97. Those arguments do not call into question the relevance of the reference for a preliminary ruling in the light of the object of the dispute in the main proceedings. Since that dispute has its source in the exercise by the DPC of the remedy provided for in paragraph 65 of the judgment in *Schrems*, its very object consists in having the national court make a reference to the Court for a preliminary ruling on the validity of Decision 2010/87. The German and United Kingdom Governments are disputing, in reality, the need for the questions for a preliminary ruling not for the purpose of determining whether that decision is valid, but rather for the purpose of putting the DPC in a position to give an actual ruling on Mr Schrems' complaint.

98. In any event, even from the perspective of that procedure underlying the dispute in the main proceedings, the questions for a preliminary ruling on the validity of Decision 2010/87 do not seem irrelevant to me. In fact, the referring court has established that Facebook Ireland has continued to transfer its users' data to the United States after the 'safe harbour' decision was declared invalid and that those transfers are based, at least in part, on Decision 2010/87. Furthermore, while it may be advantageous for all the relevant facts to be established before it exercises its jurisdiction under Article 267 TFEU, it is for the referring court alone to determine at what stage of the proceedings it needs a preliminary ruling from the Court.[37]

99. In the light of all of the foregoing, I consider that the request for a preliminary ruling is admissible.

C. The applicability of EU law to transfers for commercial purposes of personal data to a third State which may process the data for national security purposes (first question)

100. By its first question, the referring court seeks to ascertain whether EU law applies to a transfer of personal data by a company in a Member State to a company established in a third country for commercial reasons when, after the transfer has been initiated, the data may be processed by the public authorities of that third country for purposes that include the protection of national security.

101. The significance of that question for the outcome of the dispute in the main proceedings lies in the fact that, if such a transfer fell outside the scope of EU law, all the objections raised against the validity of Decision 2010/87 in the present case would be rendered baseless.

37 See, to that effect, judgments of 1 April 1982, *Holdijk and Others* (141/81 to 143/81, EU:C:1982:122, paragraph 5) and of 9 December 2003, *Gasser* (C-116/02, EU:C:2003:657, paragraph 27).

102. As the referring court has observed, the processing of personal data for the purpose of public security was excluded from the scope of Directive 95/46 by Article 3(2) of that directive. Article 2(2) of the GDPR now makes clear that that regulation is not to apply to, inter alia, the processing of personal data in the course of an activity which falls outside the scope of EU law or by the competent authorities for the purposes of the protection of public security. Those provisions reflect the fact that Article 4(2) TEU recognises that competence in matters of the protection of national security is reserved to Member States.

103. The DPC, Mr Schrems, Ireland, the German, Austrian, Belgian, Czech, Netherlands, Polish and Portuguese Governments, and likewise the Parliament and the Commission, claim that transfers such as those referred to in Mr Schrems' complaint are not covered by those provisions and therefore come within the scope of EU law. Facebook Ireland defends the opposite argument. I support the viewpoint of the first-mentioned parties.

104. In that regard, it must be emphasised that the transfer of personal data from a Member State to a third country constitutes, as such, 'processing' within the meaning of Article 4(2) of the GDPR, carried out on the territory of a Member State.[38] The first question is specifically intended to determine whether EU law applies *to the processing consisting in the transfer itself*. That question does not concern the applicability of EU law to any subsequent processing by the United States authorities for national security purposes of the data transferred to the United States, which is excluded from the scope *ratione territoriae* of the GDPR.[39]

105. From that aspect, the only factor that must be taken into consideration, for the purposes of determining whether EU law applies to the data transfer at issue, is the activity of which that transfer forms part, while the purpose of any further processing that the transferred data will undergo by the public authorities in the third country of destination is irrelevant.[40]

106. It is apparent from the order for reference that the transfer referred to in Mr Schrems' complaint is part of a commercial activity. Nor does that transfer have the purpose of allowing the data in question to be processed subsequently by the United States intelligence services for national security purposes.

107. Moreover, the approach proposed by Facebook Ireland would render the provisions of the GDPR relating to transfers to third countries devoid of purpose, since it can never be precluded that data transferred in the course of a commercial activity will be processed for national security purposes after being transferred.

108. The interpretation which I recommend finds confirmation in the wording of Article 45(2)(a) of the GDPR. That provision states that, when adopting an adequacy decision, the Commission is to take account of, inter alia, the legislation of the third country concerned *relating to national security*. It can thus be inferred that the possibility that the data will undergo processing by the authorities of the third country of destination for the purposes of the protection of national security does not render EU law inapplicable to the processing consisting in the transfer of data to that third country.

38 See, to that effect, judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346, 'the *PNR* judgment', paragraph 56), and judgment in *Schrems* (paragraph 45). Article 4(2) of the GDPR essentially reproduces the definition of 'processing' that appeared in Article 2(b) of Directive 95/46.

39 In accordance with Article 3(1) of the GDPR, that regulation is to apply to any processing carried out in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The question of the applicability of EU law to processing by the intelligence services of a third country outside the Union must be distinguished from the question of the relevance of the rules and practices applicable to such processing in the third country at issue for the purposes of determining whether an adequate level of protection is guaranteed in that country. The latter theme forms the subject matter of the second question and will be addressed in points 201 to 229 of this Opinion.

40 See my Opinion in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, point 47), where I emphasised the distinction between, on the one hand, the direct processing of data in the context of sovereign activities of the State and, on the other hand, commercial processing following which the data are used by the public authorities.

109. The reasoning and the conclusions adopted by the Court in the judgment in *Schrems* are also based on that premiss. In particular, in that judgment the Court evaluated the validity of the 'safe harbour' decision with regard to Article 25(6) of Directive 95/46 read in light of the Charter in so far as that decision concerned transfers of personal data to the United States where they might be collected and processed for national security protection purposes. [41]

110. Having regard to those considerations, I consider that EU law applies to a transfer of personal data from a Member State to a third country where that transfer forms part of a commercial activity, it being immaterial that the transferred data might undergo, on the part of the public authorities of that third country, processing intended to protect the national security of that country.

D. The level of protection required in the context of a transfer based on standard contractual clauses (first part of the sixth question)

111. By the first part of its sixth question, the referring court seeks to ascertain the level of protection of the fundamental rights of data subjects that must be ensured in order for personal data to be able to be transferred to a third country on the basis of the standard contractual clauses provided for in Decision 2010/87.

112. It observes that, in the judgment in *Schrems*, the Court interpreted Article 25(6) of Directive 95/46 (the content of which is essentially reproduced in Article 45(3) of the GDPR), in that it provided that the Commission can adopt an adequacy decision only after it has ensured that the third country concerned guarantees an *adequate* level of protection, as supposing that the Commission establish that that country ensures a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of that directive, read in the light of the Charter. [42]

113. In that context, the first part of the sixth question invites the Court to determine whether the application of standard contractual clauses adopted by the Commission on the basis of Article 26(4) of Directive 95/46 — and now corresponding to standard data protection clauses referred to in Article 46(2)(c) of the GDPR — must permit a level of protection corresponding to the same standard of 'essential equivalence' to be attained.

114. In that respect, Article 46(1) of the GDPR provides that the controller or processor may, in the absence of an adequacy decision, 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' (emphasis added). [43] In the words of Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission.

115. Like the DPC, Mr Schrems and Ireland, I consider that the 'appropriate safeguards' provided by the controller or processor to which Article 46(1) of the GDPR refers must ensure that the rights of the persons whose data are transferred benefit, as in the context of a transfer based on an adequacy decision, from a level of protection essentially equivalent to that which follows from the GDPR, read in the light of the Charter.

41 Likewise, in Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, 'Opinion 1.15'), the Court examined the compatibility with Articles 7, 8 and 47 of the Charter of a draft international agreement between Canada and the European Union concerning data which, after being transferred to Canada, were to be processed by the public authorities for national security protection purposes.

42 Judgment in *Schrems* (paragraph 73). The Court confirmed that finding in Opinion 1/15 (paragraph 134).

43 Article 26(2) of Directive 95/46 provided that a Member State might authorise such a transfer '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' (emphasis added). The concepts of 'adequate safeguards' and 'appropriate safeguards', referred to, respectively, in Article 26(2) of that directive and in Article 46(1) of the GDPR, have, in my view, the same content.

116. That conclusion follows from the objective of that provision and from the instrument of which it forms part.

117. Articles 45 and 46 of the GDPR are aimed at ensuring the continuity of the high level of protection of personal data ensured by that regulation when they are transferred outside the European Union. In fact, Article 44 of the GDPR, entitled 'General principle for transfers', opens Chapter V, on transfers to third countries, by announcing that all the provisions in that chapter are to be applied in order to ensure that the level of protection guaranteed by the GDPR is not undermined where data are transferred to a third State.[44] That rule is designed to ensure that the standards of protection resulting from EU law are not circumvented by transfers of personal data to a third country for the purpose of being processed there.[45] Having regard to that objective, it is immaterial that the transfer is based on an adequacy decision or on guarantees provided by the controller or processor, in particular by means of contractual clauses. The requirements of protection of fundamental rights guaranteed by the Charter do not differ according to the legal basis for a specific transfer.[46]

118. Conversely, the way in which the continuity of the high level of protection is maintained does differ according to the legal basis of the transfer.

119. On the one hand, the purpose of an adequacy decision is to find that the third country concerned itself ensures a level of protection essentially equivalent to that imposed by EU law. The adoption of an adequacy decision assumes that the Commission first evaluates, for a given third country, the level of protection guaranteed by the law and practices of that third country in the light of the factors set out in Article 45(3) of the GDPR. Personal data may then be transferred to that third country without the controller being required to obtain specific authorisation.

120. On the other hand, as explained in greater detail in the following section, the appropriate safeguards afforded by the controller or processor are intended to ensure a high level of protection where the safeguards available in the third country of destination are inadequate. Thus, although Article 46(1) of the GDPR allows personal data to be transferred to a third country which does not provide an adequate level of protection, it authorises such transfers only when appropriate safeguards are provided by other means. The standard contractual clauses adopted by the Commission represent, in that respect, a general mechanism applicable to transfers irrespective of the third country of destination and the level of protection guaranteed there.

E. The validity of Decision 2010/87 in the light of Article 7, 8 and 47 of the Charter (seventh, eighth and eleventh questions)

121. By its seventh question, the referring court asks essentially whether Decision 2010/87 is invalid because it is not binding on the authorities of the third States to which the data are transferred on the basis of the standard contractual clauses provided for in the annex to that decision and, in particular, it does not prevent the authorities requiring a data importer to make those data available to them. Thus, by that question the referring court calls into question the actual possibility of ensuring an adequate level of protection of such data by means of exclusively contractual mechanisms. The eleventh question relates, more generally, to the validity of Decision 2010/87 in the light of Articles 7, 8 and 47 of the Charter.

44 In that regard, recital 6 of the GDPR states that a 'high level' of the protection of personal data must be ensured both within the Union and in the event of transfer outside the Union. See also recital 101 of the GDPR.

45 See judgment in *Schrems* (paragraph 73) and Opinion 1/15 (paragraph 214).

46 That is so without prejudice to the possibility of transferring personal data, even in the absence of appropriate safeguards, on the basis of the grounds for derogations provided for in Article 49(1) of the GDPR.

122. The eighth question invites the Court to determine whether a supervisory authority is required to use the powers conferred on it by Article 58(2)(f) and (j) of the GDPR to suspend a transfer to a third country based on the standard contractual clauses provided for in Decision 2010/87 when it considers that the data importer is subject there to obligations that prevent it from honouring those clauses and have the effect that appropriate protection of the transferred data is not guaranteed. In so far as the answer to that question has in my view an impact on the validity of Decision 2010/87,[47] I shall deal with it together with the seventh and eleventh questions.

123. The wording of Article 46(1) of the GDPR, in that it provides that, '*in the absence of a decision pursuant to Article 45(3)*, a controller or processor may transfer personal data to a third country … only if the controller or processor *has provided* appropriate safeguards …' (emphasis added), underlines the logic behind the contractual mechanisms such as that provided for in Decision 2010/87. As emphasised in recitals 108 and 114 of the GDPR, the purpose of those mechanisms is to allow transfers to third countries in respect of which the Commission has not adopted an adequacy decision, as any inadequacies in the protection afforded in the legal order of that third country is then *compensated* by safeguards which the data exporter and importer contractually undertake to respect.

124. Since the *raison d'être* of the contractual safeguards consists specifically in compensating for any deficiencies in the protection afforded by the third country of destination, whatever they may be, the validity of a decision whereby the Commission finds that certain standard clauses adequately compensate for those deficiencies cannot depend on the level of protection guaranteed in each of the individual third countries to which data might be transferred. The validity of such a decision depends only on the soundness of the safeguards which those clauses provide in order to compensate for any inadequacy of the protection afforded in the third country of destination. The effectiveness of those safeguards must be evaluated by taking account also of the safeguards consisting in the powers of the supervisory authorities under Article 58(2) of the GDPR.

125. In that regard, as, in essence, the DPC, Mr Schrems, the BSA, Ireland, the Austrian, French, Polish and Portuguese Governments and the Commission have submitted, the safeguards in the standard contractual clauses may be reduced, or indeed eliminated, when the law of the third country of destination imposes obligations that are contrary to the requirements of those clauses on the importer. Thus, the prevailing legal context in the third country of destination may, depending on the actual circumstances of the transfer,[48] make the obligations set out in those clauses impossible to implement.

126. In those circumstances, as Mr Schrems and the Commission have observed, the contractual mechanism set out in Article 46(2)(c) of the GDPR is based on responsibility being placed on the exporter and, in the alternative, the supervisory authorities. It is on a *case-by-case basis*, for each specific transfer, that the controller or, failing that, the supervisory authority will examine whether the law of the third country of destination constitutes an obstacle to the implementation of the standard clauses and, therefore, to an adequate protection of the transferred data, so that the transfers must be prohibited or suspended.

127. In the light of those observations, I consider that the fact that Decision 2010/87 and the standard contractual clauses which it sets out are not binding on the authorities of the third country of destination does not in itself render that decision invalid. The compatibility of Decision 2010/87 with Articles 7, 8 and 47 of the Charter depends, in my view, on whether there are sufficiently sound mechanisms to ensure that transfers based on the standard contractual clauses are suspended or prohibited where those clauses are breached or impossible to honour.

47 See point 128 of this Opinion.

48 Let us imagine, for example, that a third country lays down an obligation for telecommunications services providers to grant the public authorities access to the data transferred without any restrictions or safeguards. While such providers would be unable to comply with the standard contractual clauses, companies which are not subject to that obligation would not be prevented from doing so.

128. In that regard, Article 46(1) of the GDPR provides that a transfer on the basis of appropriate safeguards can take place only 'on condition that enforceable data subject rights and effective legal remedies for data subjects are available'. It will be necessary to ascertain whether the safeguards provided for in the clauses in the annex to Decision 2010/87, supplemented by the powers of the supervisory authorities, make it possible to ensure that that condition is met. That, in my view, is the position only in so far as there is an *obligation* — placed on the controllers (section 1) and, where the latter fail to act, on the supervisory authorities (section 2) — to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with.

1. The obligations placed on the controllers

129. In the first place, the contractual clauses set out in the annex to Decision 2010/87 require that, in the event of conflict between the obligations which they lay down and the requirements of the law of the third country of destination, those clauses will not be relied on in support of a transfer to that third country or, if the transfer has already taken place on the basis of those clauses, the exporter will be informed and may suspend that transfer.

130. Thus, under Clause 5(a), the importer undertakes to process the personal data only on behalf of the data exporter and in compliance with its instructions and the standard contractual clauses. If the importer cannot comply with those clauses, it agrees to inform the exporter promptly, in which case the exporter is to be entitled to suspend the transfer and/or to terminate the contract.[49]

131. Footnote 5 relating to Clause 5 states that the standard clauses are not breached where the importer complies with mandatory requirements of the national legislation applicable to it in the third country, provided that those requirements do not go beyond what is necessary in a democratic society in order to protect one of the interests listed in Article 13(1) of Directive 95/46 (the content of which is reproduced, in essence, in Article 23(1) of the GDPR), which include public security and the safeguarding of the State. Conversely, breach of those clauses in order to comply with a contradictory obligation based on the law of the third country of destination which goes beyond what is proportionate to the safeguarding of a legitimate interest recognised by the Union is treated as a breach of those clauses.

132. To my mind, and as Mr Schrems and the Commission have maintained, Clause 5(a) cannot be interpreted as meaning that suspension of the transfer or termination of the contract is merely optional where the importer cannot comply with the standard clauses. Although that clause refers only to a right in that sense for the benefit of the exporter, that wording must be understood by reference to the contractual framework of which it forms part. The fact that the exporter is given a right, *in its bilateral relations with the importer*, to suspend the transfer or terminate the contract where the importer is unable to honour the standard clauses is without prejudice to the obligation placed on the exporter to do so *in the light of the requirements to protect the rights of the persons*

49 I note, moreover, that Clause 5(d)(i) exempts the importer from his obligation to inform the exporter of a legally binding request for disclosure by a law enforcement authority of the third country where the law of that third country prohibits such information being given. In such situations, the exporter will be unable to suspend the transfer if that disclosure, of which he will be unaware, infringes the standard clauses. However, under Clause 5(a) the importer is still required to inform the exporter, where appropriate, of the fact that he considers that the legislation of that third country prevents him from fulfilling his obligations under the contractual clauses agreed between them.

concerned arising under the GDPR. Any other interpretation would render Decision 2010/87 invalid in that the standard contractual clauses which it sets out would not permit the transfer to be accompanied by 'appropriate safeguards' as required by Article 46(1) of the GDPR, read in the light of the provisions of the Charter.[50]

133. In addition, according to Clause 5(b) the importer is to certify that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the exporter and its obligations under the contract. In the event of a change in that legislation that is likely to have a substantial adverse effect on the warranties and obligations provided by the standard clauses, the importer will promptly notify that change to the exporter, in which case the exporter is entitled to suspend the transfer of data and/or terminate the contract. In accordance with Clause 4(g), the exporter must forward the notification received from the importer to the competent supervisory authority if it decides to continue the transfer.

134. I believe it is necessary to make a few points here about the content of the examination which the parties to the contract should carry out in order to determine, in the light of the footnote referring to Clause 5, whether the obligations which the law of the third State imposes on the importer entail a breach of the standard clauses and thus prevent the transfer from being accompanied by appropriate safeguards. That issue has been raised, in essence, in the context of the second part of the sixth question.

135. Such an examination entails in my view a consideration of all of the circumstances characterising each transfer, which may include the nature of the data and whether they are sensitive, the mechanisms employed by the exporter and/or the importer to ensure its security,[51] the nature and the purpose of the processing by the public authorities of the third country which the data will undergo, the details of such processing and the limitations and safeguards ensured by that third country. The factors characterising the processing activities carried out by the public authorities and the safeguards applicable in the legal order of that third country may, in my view, overlap with those set out in Article 45(2) of the GDPR.

136. In the second place, the standard contractual clauses set out in the annex to Decision 2010/87 establish, in favour of data subjects, enforceable rights and remedies against the exporter and, in the alternative, against the importer.

137. Thus, Clause 3, entitled 'Third-party beneficiary', provides, in paragraph 1, for a remedy by the data subject against the exporter in the event of a breach of, in particular, Clause 5(a) or (b). In accordance with Clause 3(2) where the exporter has factually disappeared or has ceased to exist in law, the data subject may enforce that clause against the importer.

50 It follows from the case-law that the provisions of an implementing measure must be interpreted in accordance with the provisions of the basic act whereby the legislature authorised its adoption (see, to that effect, in particular, judgments of 26 July 2017, *Czech Republic* v *Commission* (C-696/15 P, EU:C:2017:595, paragraph 51); of 17 May 2018, *Evonik Degussa* (C-229/17, EU:C:2018:323, paragraph 29); and of 20 June 2019, *ExxonMobil Production Deutschland* (C-682/17, EU:C:2019:518, paragraph 112)). In addition, an EU measure must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter (see, in particular, judgment of 14 May 2019, *M and Others (Revocation of refugee status)* (C-391/16, C-77/17 and C-78/17, EU:C:2019:403, paragraph 77 and the case-law cited)).

51 In that regard, recital 109 of the GDPR encourages the exporter and the importer to provide additional safeguards to the standard clauses, in particular by contractual means.

138. Clause 6(1) grants, to any data subject who has suffered damage as a result of a breach of the obligations referred to in Clause 3, the right to receive compensation from the data exporter for the damage suffered. Under Clause 7(1), the importer agrees that if the data subject invokes third-party beneficiary rights against it and/or claims compensation for damages, it will accept the decision of the data subject either to refer the dispute to mediation by an independent person or, where applicable, by the supervisory authority, or to refer the dispute to the courts in the Member State in which the exporter is established.

139. In addition to the remedies available to them under the standard contractual clauses set out in the annex to Decision 2010/87, data subjects may, when they consider that there has been a breach of those clauses, request the supervisory authorities to exercise its corrective powers under Article 58(2) of the GDPR, to which Article 4 of Decision 2010/87 makes reference. [52]

2. The obligations placed on the supervisory authorities

140. The following reasons lead me to consider that, as Mr Schrems, Ireland, the German, Austrian, Belgian, Netherlands and Portuguese Governments and the EDPB submit, under Article 58(2) of the GDPR the supervisory authorities are required, when they consider following a diligent examination that data transferred to a third country do not benefit from appropriate protection because the contractual clauses agreed are not complied with, to take adequate measures to remedy that illegality, if necessary by ordering suspension of the transfer.

141. In the first place, I note that, contrary to the DPC's submission, no provision of Decision 2010/87 limits to exceptional cases the exercise of the powers to 'impose a temporary or definitive limitation including a ban on processing' or to 'order the suspension of data flows to a recipient in a third country' which the supervisory authorities enjoy under Article 58(2)(f) and (j) of the GDPR.

142. The initial version of Article 4 of Decision 2010/87 did admittedly, in paragraph 1, confine the exercise by the supervisory authorities of their powers to suspend or prohibit cross-border data flows to specific cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties intended to protect the data subject. However, Article 4 of that decision, as amended by the Commission in 2016 in order to comply with the judgment in *Schrems*, [53] now merely refers to those powers, without limiting them in any way. In any event, a Commission implementing decision, such as Decision 2010/87, cannot validly restrict the powers conferred on the supervisory authorities under the GDPR itself. [54]

143. That conclusion is not called into question by recital 11 of Decision 2010/87, which states that the powers to suspend and prohibit transfers may be exercised by the supervisory authorities only in 'exceptional cases'. That recital, which was already present in the initial version of that decision, referred to the former Article 4(1) of that decision, which limited the supervisory authorities' powers. When Decision 2010/87 was revised by Decision 2016/2297, the Commission failed to remove or amend that recital in order to adapt its content to the requirements of the new Article 4. However, recital 5 of Decision 2016/2297 reasserted the supervisory authorities' power to suspend or prohibit

52 Although Article 4(1) of Decision 2010/87 refers to Article 28(3) of Directive 95/46, I would again point out that, under Article 94(2) of the GDPR, references to that directive are to be construed as references to the corresponding provisions of the GDPR.

53 See recitals 6 and 7 of Decision 2016/2297. In paragraphs 101 to 104 of the judgment in *Schrems*, the Court had held that a provision of the 'safe harbour' decision that limited the powers conferred on the supervisory authorities by Article 28 of Directive 95/46 to 'exceptional cases' was invalid, on the ground that the Commission was not competent to restrict those powers.

54 See judgment in *Schrems* (paragraph 103).

any transfer which they consider to be contrary to EU law, in particular where the importer does not respect the standard contractual clauses. Recital 11 of Decision 2010/87, in that it now contradicts both the wording and the objective of a legally binding provision of that decision, must be deemed obsolete. [55]

144. In the second place, contrary to a further submission of the DPC, the exercise of the powers to suspend and prohibit transfers set out in Article 58(2)(f) and (j) of the GDPR is no longer merely an option left to the supervisory authorities' discretion. That conclusion follows, in my view, from an interpretation of Article 58(2) of the GDPR in the light of other provisions of that regulation and of the Charter, and also from the general scheme and the objectives of Decision 2010/87.

145. In particular, Article 58(2) of the GDPR must be read in the light of Article 8(3) of the Charter and Article 16(2) TFEU. In accordance with those provisions, compliance with the requirements entailed by the fundamental right to protection of personal data is subject to review by independent authorities. That task of monitoring compliance with the requirements relating to the protection of personal data, which is also referred to in Article 57(1)(a) of the GDPR, entails an obligation for the supervisory authorities to act in such a way as to ensure the proper application of that regulation.

146. Thus, a supervisory authority must examine with all due diligence the complaint lodged by a person whose data are alleged to be transferred to a third country in breach of the standard contractual clauses applicable to the transfer. [56] Article 58(1) of the GDPR confers on the supervisory authorities, for that purpose, significant investigative powers. [57]

147. The competent supervisory authority is also required to react appropriately to any infringements of the rights of the data subject which it has established following its investigation. In that regard, each supervisory authority has, under Article 58(2) of the GDPR, a wide range of means — the various powers to adopt corrective measures listed in that provision — of carrying out the task entrusted to it. [58]

148. Although the choice of the most effective means is a matter for the discretion of the competent supervisory authority having regard to all the circumstances of the transfer at issue, that authority is required to carry out in full the supervisory task entrusted to it. Where appropriate, it must suspend the transfer if it concludes that the standard contractual clauses are not being complied with and that appropriate protection of the data transferred cannot be ensured by other means, where the exporter has not itself put an end to the transfer.

149. That interpretation is supported by Article 58(4) of the GDPR, which provides that the exercise of the powers conferred on the supervisory authorities pursuant to that article is to be subject to appropriate safeguards, including an effective judicial remedy in accordance with Article 47 or the Charter. Article 78(1) and (2) of the GDPR, moreover, recognises the right of each person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them or where that authority fails to deal with his complaint. [59]

55 In any event, the preamble to an EU measure does not have binding legal force and cannot be relied upon as a ground for derogating from the actual provisions of that measure. See judgments of 19 November 1998, *Nilsson and Others* (C-162/97, EU:C:1998:554, paragraph 54); of 12 May 2005, *Meta Fackler* (C-444/03, EU:C:2005:288, paragraph 25); and of 10 January 2006, *IATA and ELFAA* (C-344/04, EU:C:2006:10, paragraph 76).

56 See, by analogy, judgment in *Schrems* (paragraph 63).

57 I would add that, pursuant to Clause 8(2) in the Annex to Decision 2010/87, the parties to the contract agree that the supervisory authority may conduct an audit of the importer subject to the same conditions as would apply to an audit of the exporter under the applicable law.

58 See, to that effect, judgment in *Schrems* (paragraph 43).

59 In the words of recital 141 of the GDPR, every person must have the right to an effective judicial remedy in accordance with Article 47 of the Charter if the supervisory authority 'does not act where such action is necessary to protect the rights of [that person]'. See also recitals 129 and 143 of the GDPR.

150. Those provisions imply, that, as Mr Schrems, the BSA, Ireland, the Polish and United Kingdom Governments and the Commission claim, in essence, a decision whereby a supervisory authority refrains from prohibiting or suspending a transfer to a third country, at the request of a person claiming that there is a risk that data relating to him will be processed in that third country in a manner that fails to respect his fundamental rights, may be the subject of a judicial action. The recognition of a right to a judicial remedy assumes the existence of a strict, and not purely discretionary, power on behalf of the supervisory authorities. In addition, Mr Schrems and the Commission have correctly emphasised that the exercise of an effective judicial remedy implies that the authority that adopts the contested act states to an adequate degree the reasons on which it is based.[60] To my mind, that obligation to state reasons extends to supervisory authorities' choice to use one or other of the powers conferred on them by Article 58(2) of the GDPR.

151. However, it is still necessary to respond to the arguments whereby the DPC claims that, even if the supervisory authorities were required to suspend or prohibit the transfer where the protection of the data subject's rights requires it, the validity of Decision 2010/87 would still not be ensured.

152. First, the DPC considers that such an obligation on the supervisory authorities would not redress the systemic problems relating to the absence of adequate safeguards in a third country such as the United States. The supervisory authorities' powers can be exercised only on a case-by-case basis, whereas the deficiencies characteristic of United States law are general and structural in nature. There is thus a risk that different supervisory authorities will adopt diverging decisions in respect of comparable transfers.

153. On that point, I cannot overlook the practical difficulties linked to the legislative choice to make the supervisory authorities responsible for ensuring that data subjects' fundamental rights are observed in the context of specific transfers or of data flows to a specific recipient. However, those difficulties do not seem to me to render Decision 2010/87 invalid.

154. In fact, in my view, EU law does not require that a general and preventive solution be applied for all transfers to a given third country that might entail the same risks of a violation of fundamental rights.

155. In addition, the risk that the approaches taken by the different supervisory authorities will be fragmented is inherent in the decentralised surveillance structure intended by the legislature.[61] Moreover, as the German Government has submitted, Chapter VII of the GDPR, entitled 'Cooperation and consistency', establishes measures designed to avoid that risk. Article 60 of that regulation sets out, in the event of cross-border processing of data, a procedure of cooperation between the supervisory authorities concerned and the supervisory authority of the establishment of the controller, known as 'lead supervisory authority'.[62] In the event of diverging opinions, the disagreement must be resolved by the EDPB,[63] which also has competence to deliver opinions, at the request of a supervisory authority, on any questions of interest to more than one Member State.[64]

60 See, in particular, judgments of 28 July 2011, *Samba Diouf* (C-69/10, EU:C:2011:524, paragraph 57) and of 17 November 2011, *Gaydarov* (C-430/10, EU:C:2011:749, paragraph 41).

61 See, in that respect, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, paragraphs 69 to 73).

62 See Article 56(1) of the GDPR. In accordance with Article 61 of that regulation, supervisory authorities are required to provide each other with mutual assistance. Article 62 of that regulation authorises those authorities to conduct joint operations.

63 See Article 65 of the GDPR.

64 See Article 64(2) of the GDPR.

156. Second, the DPC submits that Decision 2010/87 is invalid by reference to Article 47 of the Charter on the ground that the supervisory authorities can protect data subjects' rights only prospectively, and are unable to provide a solution to those whose rights have already been transferred. In particular, the DPC observes that Article 58(2) of the GDPR does not provide for a right of access, rectification and deletion of the data collected by the public authorities of the third country or allow for compensation for the damage sustained by the data subjects.

157. As regards the alleged absence of a right of access, rectification and deletion of the data collected, it must be stated that, where no effective remedy exists in the third country of destination, the remedies provided for within the European Union against the controller do not make it possible to obtain, from the public authorities of that third country, access to those data or to have them rectified or deleted.

158. To my mind, however, that objection cannot justify a finding that Decision 2010/87 is incompatible with Article 47 of the Charter. The validity of that decision does not depend on the level of protection that exists in each third country to which data might be transferred on the basis of the standard contractual clauses which it sets out. If the law of the third State of destination prevents the importer from complying with those clauses by requiring it to grant those authorities access to the data without any possibility of an appropriate remedy, it is for the supervisory authorities, where the exporter has not suspended the transfer pursuant to Clause 5(a) or (b) in the annex to Decision 2010/87, to adopt corrective measures.

159. Furthermore, as Mr Schrems submits, persons whose rights have been infringed now benefit, under Article 82 of the GDPR, from a right to compensation from the controller or processor for the material or non-material damage incurred as a result of the infringement of that regulation. [65]

160. As is clear from all of those considerations, my analysis has not revealed any element of such a kind as to affect the validity of Decision 2010/87 by reference to Articles 7, 8 and 47 of the Charter.

F. The lack of necessity to respond to the other questions or to examine the validity of the 'privacy shield' decision

161. In the present section, I shall set out the reasons, relating mainly to the fact that the subject matter of the main proceedings is limited to the validity of Decision 2010/87, why I consider that there is no need to respond to the second to the fifth questions and to the ninth and tenth questions or to rule on the validity of the 'privacy shield' decision.

162. The second question concerns the identification of the standards of protection which a third country must respect in order for data to be able to be lawfully transferred to that country on the basis of standard contractual clauses where, after being transferred, those data may be processed for purposes of national security by the authorities of that third country. The third question referred to the Court concerns the determination of the elements that characterise the scheme of protection applicable in the third State of destination that must be taken into account in order to determine whether that scheme meets those standards.

163. By its fourth, fifth and tenth questions, the referring court seeks essentially to ascertain whether, having regard to the facts which it has established with respect to United States law, appropriate safeguards are provided for in that country against interferences by the United States intelligence authorities with the exercise of the fundamental rights to respect for private life, to the protection of personal data and to effective judicial protection.

65 Article 83(5)(c) of the GDPR also provides that fines may be imposed on the controller in the event of infringement of Articles 44 to 49 of that regulation.

164. The ninth question relates to the impact — in the context of the examination whereby a supervisory authority verifies whether a transfer to the United States based on the standard contractual clauses set out in Decision 2010/87 is accompanied by appropriate safeguards — of the fact that the Commission established in the 'privacy shield' decision that the United States offers an adequate level of protection of the data subjects' fundamental rights against such interferences.

165. The question of the validity of the 'privacy shield' decision has not been explicitly raised by the referring court — although, as explained below,[66] the fourth, fifth and tenth questions indirectly call into question the validity of the finding of adequacy which the Commission made in that decision.

166. In my view, in the light of the elements that emerge from the foregoing analysis, any light that the Court might shed on those questions could not affect its finding as to the validity *in abstracto* of Decision 2010/87 or, accordingly, to influence the outcome of the dispute in the main proceedings (section 1). Furthermore, although the Court's answers to those questions might, at a later stage, prove helpful to the DPC for the purposes of determining, in the context of the procedure underlying the dispute, whether the transfers in question should, *in concreto*, be suspended because of the alleged absence of appropriate safeguards, it would, in my view, be premature to resolve them in the context of the present case (section 2).

1. There is no need for the Court to answer the other questions having regard to the subject matter of the dispute in the main proceedings

167. The dispute in the main proceedings arises, it will be recalled, from the exercise by the DPC of the remedy described in paragraph 65 of the judgment in *Schrems*, according to which each Member State must allow a supervisory authority, where it considers it necessary for the adjudication of a complaint before it, to request a national court to refer a question to the Court for a preliminary ruling on the validity of the adequacy decision or, by analogy, of a decision setting out standard contractual clauses.

168. In that regard, the High Court has made clear that its only options, in the proceedings brought by the DPC, were either to make the reference for a preliminary ruling on the validity of Decision 2010/87 requested by the DPC if it shared the latter's doubts as to the validity of that decision, or to refuse to grant that request if it did not. The High Court considers that, if it had taken the second option, it would have had to dismiss the proceedings since the DPC's complaint had no other object.[67]

169. Likewise, the Supreme Court, on appeal by Facebook Ireland against the order for reference, described the dispute in the main proceedings as a declaratory procedure whereby the DPC requested the referring court to refer a question to the Court for a preliminary ruling on the validity of Decision 2010/87. According to the Irish Supreme Court, the only substantive issue raised before the referring court and before this Court therefore relates to the validity of that decision.[68]

66 See point 175 of this Opinion.

67 Judgment of the High Court of 3 October 2017 (paragraph 337).

68 In the words of the judgment of the Supreme Court of 31 May 2019 (paragraph 2.7), 'the sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFEU]'. Paragraph 2.9 of that judgment continues: 'Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*' (emphasis added).

170. Having regard to the subject matter of the dispute in the main proceedings as thus defined, the referring court referred to the Court its first 10 questions, since it considered that examination of those questions would play a part in the overall evaluation necessary for the Court to rule, in answer to the eleventh question, on the validity of Decision 2010/87 by reference to Articles 7, 8 and 47 of the Charter. That question, according to the order for reference, is the logical consequence of the preceding questions.

171. From that aspect, the second to the fifth, and the ninth and tenth questions, seem to me to be underpinned by the premiss that the validity of Decision 2010/87 would depend on the level of protection of fundamental rights provided for in each of the third States to which data may be transferred on the basis of the standard contractual clauses set out in that decision. However, as is apparent from my analysis of the seventh question,[69] that premiss is in my view incorrect. Examination of the law of the third country of destination is relevant only when the Commission adopts an adequacy decision or when the controller — or, failing that, the competent supervisory authority — verifies whether, in the context of a transfer based on appropriate safeguards within the meaning of Article 46(1) of the GDPR, the obligations which the law of that third country imposes on the importer undermine the effectiveness of the protection afforded by those safeguards.

172. Consequently, the Court's answers to the abovementioned questions are not capable of influencing its conclusion concerning the eleventh question.[70] There is thus no need to answer those questions from the viewpoint of the subject matter of the dispute of the main proceedings.

173. I propose that the Court confine itself to dealing with the present case from the perspective of the subject matter of that dispute. To my mind, the Court should not go beyond what is required in order to resolve that dispute, by addressing the questions for a preliminary ruling from the viewpoint of the underlying procedure pending before the DPC. As explained below, that request to show restraint is based, on the one hand, on the desire not to short-circuit the normal progress of the procedure which will have to continue before the DPC after the Court has given a ruling on the validity of Decision 2010/87. On the other hand, in the light of the facts of the case, it would seem to me to be somewhat precipitous, even from the viewpoint of what is at issue in that procedure, for the Court to examine the problems raised by the second to the fifth and by the ninth and tenth questions.

2. The reasons why the Court should not examine the other questions having regard to the object of the procedure pending before the DPC

174. In the complaint which he lodged with the DPC, Mr Schrems asks the latter to exercise her powers under Article 58(2)(f) of the GDPR and order Facebook Ireland to suspend the transfer to the United States, carried out on the basis of the contractual clauses, of the personal data relating to him. In support of that request, Mr Schrems relies essentially on the inappropriateness of those contractual safeguards by reference to the interferences with the exercise of his fundamental rights resulting from the activities of the United States intelligence services.

69 See point 124 of this Opinion.

70 For that reason, the Supreme Court, in its judgment of 31 May 2019 (paragraphs 8.1 to 8.5), while acknowledging that it had no jurisdiction to call into question the referring court's decision to refer the questions for a preliminary ruling to the Court or to amend the terms of those questions, expressed doubts as to the need for some of those questions. In particular, paragraph 8.5 of that judgment states: 'The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures ….'

175. Mr Schrems' arguments call into question the finding, made by the Commission in the 'privacy shield' decision, that the United States affords an adequate level of protection of data transferred pursuant to that decision having regard to the restrictions placed on access to the data and their use by the United States intelligence authorities and to the legal protection offered to data subjects.[71] The concerns provisionally expressed by the DPC,[72] and also by the referring court in the context of its fourth, fifth and tenth questions also indirectly cast doubt on the validity of that finding.

176. Indeed, the 'privacy shield' decision merely finds that the level of protection of the personal data transferred, in accordance with the principles which it sets out, to an undertaking established in that third country which has self-certified its adherence to those principles is adequate.[73] However, the considerations stated in that decision go beyond the context of the transfers covered by that decision since they relate to the law and practices in force in the United States concerning the processing, for national security protection purposes, of the data transferred. As Facebook Ireland, Mr Schrems, the United States Government and the Commission essentially observe, the surveillance carried out by the United States intelligence authorities, like the safeguards against the risks of abuse which it entails and the mechanisms designed to ensure compliance with those safeguards, apply regardless, from the viewpoint of EU law, of the legal basis relied on in support of the transfer.

177. From that perspective, the question whether the findings made on that subject in the 'privacy shield' decision are binding on the supervisory authorities when they examine the legality of a transfer carried out on the basis of standard contractual clauses might prove to be relevant for the purposes of the DPC's treatment of Mr Schrems' complaint. If that question were to be answered in the affirmative, the question whether that decision is indeed valid would then arise.

178. Nevertheless, I advise the Court not to give a ruling on those questions with the sole aim of helping the DPC to deal with that complaint, when there is no need to answer them in order to allow the referring court to resolve the dispute in the main proceedings. As the procedure provided for in Article 267 TFEU establishes a dialogue between courts, the Court is not required to provide clarification for the sole purpose of helping an administrative authority in the context of a procedure underlying that dispute.

179. Reservation is called for, in my view, a fortiori because the validity of the 'privacy shield' decision has not been expressly referred to the Court — and, moreover, that decision is already the subject matter of an action for annulment pending before the General Court of the European Union.[74]

180. In addition, in ruling on the problems described above, the Court would to my mind disrupt the normal course of the procedure that will have to take place after it has delivered its judgment in the present case. In the context of that procedure, the DPC will be required to deal with Mr Schrems' complaint taking account of the answer that the Court will give to the eleventh question. If the Court deems, as I propose and contrary to what the DPC has maintained before it, that Decision 2010/87 is not invalid by reference to Articles 7, 8 and 47 of the Charter, the DPC should in my view be given the opportunity to re-examine the file in the procedure pending before her. If the DPC should consider

71 See recitals 64 to 141 of the 'privacy shield' decision. I observe that, as is apparent from Article 1(2) of that decision, the privacy shield is constituted not only by principles to which undertakings wishing to rely on that decision as the basis for data transfers must adhere, but also by official representations and commitments obtained from the United States Government contained in the documents annexed to that decision.

72 The DPC's draft decision predates the adoption of the 'privacy shield' decision. As the DPC stated in that draft, while it was provisionally concluded that the safeguards provided for by United States law did not make it possible, at least, to ensure that data transfers to that third country were consistent with Article 47 of the Charter, *she did not examine or take into account, at that stage, the new arrangements envisaged in the draft 'data shield' agreement, since it had not yet been adopted.* That being said, paragraph 307 of the judgment of the High Court of 3 October 2017 acknowledges: 'It is fair to conclude … that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court'.

73 See Article 1(1) and (3) and recitals 14 to 16 of the 'privacy shield' decision.

74 Pending Case T-738/16, *La Quadrature du Net and Others* v *Commission* (OJ 2017 C 6, p. 39).

that she is not in a position to adjudicate on Mr Schrems' complaint unless the Court first determines whether the 'privacy shield' decision constitutes an obstacle to her powers to suspend the transfer at issue, and confirm that she entertains doubts as to the validity of that decision, it would be open to her to bring the matter before the national courts again in order for them to make a reference to the Court on that point.[75]

181. That would initiate a procedure allowing any party referred to in the second paragraph of Article 23 of the Statute of the Court to submit observations to the Court relating specifically to the question of the validity of the 'privacy shield' decision, identifying, where appropriate, the particular assessments which he disputes and the reasons why in his view the Commission exceeded the reduced discretion at its disposal.[76] In the context of such a procedure, the Commission would have the opportunity to respond precisely and in detail to each of the criticisms that might be directed against that decision. Although the present case has already given the parties and interested persons who have submitted observations to the Court the opportunity to discuss certain relevant aspects for the purpose of evaluating the compatibility of the 'privacy shield' decision with Articles 7, 8 and 47 of the Charter, that question, in view of what is at stake, is deserving of a thorough and exhaustive exchange.

182. To my mind, prudence dictates that the Court should await the completion of those procedural steps before it examines the impact which the 'privacy shield' decision has on the way in which a supervisory authority deals with a request to suspend a transfer to the United States on the basis of Article 46(1) of the GDPR and adjudicates on the validity of that decision.

183. That applies a fortiori since the file submitted to the Court does not permit the conclusion that the way in which the DPC will deal with Mr Schrems' complaint will necessarily depend on whether the 'privacy shield' decision precludes the exercise by the supervisory authorities of their power to suspend a transfer that is based on standard contractual clauses.

184. In that regard, in the first place, it cannot be precluded that the DPC may find it necessary to suspend the transfer at issue for reasons other than those relating to the alleged inadequacy of the level of protection ensured in the United States against interferences with the fundamental rights of the data subjects as a result of the activities of the United States intelligence services. In particular, the referring court has explained that Mr Schrems maintains, in his complaint to the DPC, that the contractual clauses relied on by Facebook Ireland in support of that transfer do not faithfully reflect those set out in the annex to Decision 2010/87. Mr Schrems further claims that that transfer falls within the scope not of that decision but rather of the other SCC decisions.[77]

185. In the second place, the DPC and the referring court have submitted that Facebook Ireland did not rely, in support of the transfer referred to in Mr Schrems' complaint, on the 'privacy shield' decision,[78] which Facebook Ireland confirmed at the hearing. Although Facebook Inc. has self-certified its adherence to the privacy shield principles since 30 September 2016,[79] Facebook Ireland states that that adherence relates to only certain categories of data, namely those relating to Facebook Inc.'s business partners. It would therefore be inappropriate in my view for the Court to anticipate the questions that might arise in that respect by examining whether, on the assumption that Facebook Ireland could not rely on Decision 2010/87 in support of the transfer at issue, that transfer would nonetheless be covered by the 'privacy shield' decision, although Facebook Ireland did not raise that argument either before the referring court or before the DPC.

75 Moreover, I observe that, in her written observations, the DPC has not taken a position on the impact of the 'privacy shield' decision on the way in which she is dealing with the complaint lodged with her.

76 See, in that regard, judgment in *Schrems* (paragraph 78).

77 Mr Schrems claims, in support of that argument, that Facebook Inc. must be regarded not only as a processor, but also as a 'controller', within the meaning of Article 4(7) of the GDPR, so far as the processing of the personal data of users of the Facebook social network is concerned. See, in that regard, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, paragraph 30).

78 See judgment of the High Court of 3 October 2017 (paragraph 66).

79 See the 'privacy shield' website (https://www.privacyshield.gov/participant_search).

186. I conclude from the foregoing that there is no need to answer the second to the fifth or the ninth and tenth questions or to examine the validity of the 'privacy shield' decision.

G. Alternative observations relating to the effects and the validity of the 'privacy shield' decision

187. Although the preceding analysis leads me to propose that the Court should, primarily, refrain from ruling on the impact of the 'privacy shield' decision on the way in which a complaint such as that lodged by Mr Schrems before the DPC should be dealt with and on the validity of that decision, I consider it appropriate to develop, in the alternative and with certain reservations, some non-exhaustive observations on that subject.

1. The impact of the 'privacy shield' decision on the way in which a supervisory authority deals with a complaint relating to the legality of a transfer based on contractual safeguards

188. The ninth question raises the point whether the finding made in the 'privacy shield' decision in respect of the adequacy, in the light of the limitations placed on access to the transferred data and on their use by the United States authorities for national security purposes and also on the legal protection of the data subjects, of the level of protection guaranteed in the United States precludes a supervisory authority from suspending a transfer to that third country carried out pursuant to standard contractual clauses.

189. That problem must, it seems to me, be understood in the light of paragraphs 51 and 52 of the judgment in *Schrems*, from which it is clear that an adequacy decision is binding on the supervisory authorities until such time as it is declared invalid. A supervisory authority which has received a complaint from a person whose data are transferred to the third country to which an adequacy decision relates cannot therefore suspend the transfer on the ground that the level of protection in that country is inadequate, unless the Court has first declared that decision invalid.[80]

190. The referring court wishes to ascertain, essentially, whether, in the case of an adequacy decision — such as the 'privacy shield' decision or, before that, the 'safe harbour' decision — based on the voluntary adherence of the undertakings to the principles which it sets out, that conclusion applies solely in so far as the transfer to the third country concerned is covered by that decision, or whether it also applies when the transfer has a distinct legal basis.

191. According to Mr Schrems, the German, Netherlands, Polish and Portuguese Governments and the Commission, the finding of adequacy made in the 'privacy shield' decision does not deprive the supervisory authorities of their power to suspend or prohibit a transfer to the United States carried out pursuant to standard contractual clauses. When the transfer to the United States is not based on the 'privacy shield' decision, the supervisory authorities are not formally bound by that decision when exercising the powers conferred on them by Article 58(2) of the GDPR. Those authorities might, in other words, distance themselves from the findings made by the Commission as to the adequacy of the level of protection against interferences by the United States public authorities in the exercise of the data subjects' fundamental rights. The Netherlands Government and the Commission state that the supervisory authorities must nonetheless take those findings into account when using those powers. In the German Government's opinion, those authorities could reach the opposite conclusion only after a substantive examination, including the relevant investigations, of the findings made by the Commission.

80 See, to that effect, judgment in *Schrems* (paragraph 59).

192. Conversely, Facebook Ireland and the United States Government claim, in essence, that the binding effect of an adequacy decision means, in the light of the requirements of legal certainty and of the uniform application of EU law, that the supervisory authorities are not authorised to call into question, even when dealing with a complaint seeking suspension of transfers to the third country in question on a basis other than that decision, the findings made in that decision.

193. I subscribe to the first of those two approaches. As the scope of the 'privacy shield' decision is limited to transfers made to an undertaking which has self-certified on the basis of that decision, the decision cannot formally constrain the supervisory authorities in the case of transfers that do not fall within its scope. The 'privacy shield' decision likewise claims to ensure legal certainty only for the benefit of exporters who transfer data within the framework which it establishes. To my mind, the independence that Article 52 of the GDPR recognises to the supervisory authorities also tends to preclude their being bound by the findings made by the Commission in an adequacy decision falling outside its scope.

194. Clearly, the findings made in the 'privacy shield' decision relating to the adequacy of the level of protection ensured in the United States against the interferences connected with the activities of its intelligence services constitute the starting-point of the analysis whereby a supervisory authority assesses, on a case-by-case basis, whether a transfer based on standard contractual clauses must be suspended because of such interferences. However, if it considers, following a thorough investigation, that it is unable to support those findings as regards the transfer brought to its attention, the competent supervisory authority retains, in my view, the option to exercise the powers conferred on it by Article 58(2)(f) and (j) of the GDPR.

195. That being so, if the Court should answer the question being examined here in a way contrary to that which I propose, it would then be necessary to examine whether those powers should nonetheless be restored because of the invalidity of the 'privacy shield' decision.

2. The validity of the 'privacy shield' decision

196. The observations that follow will raise certain questions as to the validity of the assessments set out in the 'privacy shield' decision as regards the adequacy, within the meaning of Article 45(1) of the GDPR, of the level of protection ensured by the United States with respect to the electronic communications surveillance activities carried out by the United States intelligence authorities. Those observations are not meant to set out a definitive or exhaustive position on the validity of that decision, but will merely provide certain reflections that might prove helpful to the Court should it wish, contrary to my recommendation, to give a ruling on that point.

197. In that regard, it follows from recital 64 and from paragraph I.5 of Annex II to the 'privacy shield' decision that the undertakings' adherence to the principles set out in that decision may be limited, in particular, by requirements relating to national security, public interest or law enforcement requirements or by conflicting obligations derived from United States law.

198. The Commission therefore assessed the safeguards available in United States law as regards access to the transferred data and their use by the United States public authorities for, in particular, national security purposes.[81] It obtained certain commitments from the United States Government concerning, first, the limitations on access and use by the United States authorities of the data transferred and also, second, the legal protection offered to data subjects.[82]

81 See recital 65 of the 'privacy shield' decision.

82 See Annexes III to VII to the 'privacy shield' decision.

199. Before the Court, Mr Schrems claims that the 'privacy shield' decision is invalid on the ground that the safeguards thus described are not sufficient to ensure an adequate level of protection of the fundamental rights of persons whose data are transferred to the United States. The DPC, the EPIC and the Austrian, Polish and Portuguese Governments, without directly calling into question the validity of that decision, dispute the assessments made by the Commission in that decision concerning the adequacy of the level of protection against the interferences resulting from the activities of the United States intelligence services. Those doubts convey the concerns expressed by the Parliament,[83] the EDPB[84] and the European Data Protection Supervisor.[85]

200. Before I examine the validity of the finding of adequacy made in the 'privacy shield' decision, it is necessary to describe the methodology that should guide that examination.

(a) Explanations concerning the content of the examination of the validity of an adequacy decision

(1) The terms of the comparison permitting an assessment of the 'essential equivalence' of the level of protection

201. In accordance with Article 45(3) of the GDPR and the Court's case-law,[86] the Commission may find that a third country ensures an adequate level of protection only in so far as it has concluded, duly stating reasons, that the level of protection of the fundamental rights of the data subjects is 'essentially equivalent' to that required within the European Union pursuant to that regulation read in the light of the Charter.

202. Thus, the verification of the adequacy of the level of protection ensured in a third country necessarily entails a comparison between the rules and practices prevailing in that third country, on the one hand, and the standards of protection in force in the Union, on the other hand. By its second question, the referring court asks the Court to clarify the terms of that comparison.[87]

203. More specifically, the referring court seeks to ascertain whether the reservation of competence which Article 4(2) TEU and Article 2(2) of the GDPR recognise to the Member States in relation to the protection of national security implies that the legal order of the European Union does not include standards of protection with which the safeguards in place in a third country as regards the processing by the public authorities, for national security protection purposes, of data transferred there should be compared in order to evaluate the adequacy of those safeguards. If that is the case, the referring court wishes to know how the relevance reference framework must be determined.

83 Resolutions of the Parliament of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2017)0131, and of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2018)0315.

84 See Article 29 Working Party on data protection ('WP29'), Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13 April 2016, WP 238; WP29, EU-US Privacy Shield — First Annual Joint Review, 28 November 2017, WP 255, and EDPB, EU-US Privacy Shield — Second Annual Joint Review, 22 January 2019. WP29 had been set up pursuant to Article 29(1) of Directive 95/46, which provided that it was to have advisory status and to act independently. In accordance with paragraph 2 of that article, that working party was composed of a representative of each national supervisory authority, a representative of each authority established for the Community institutions and bodies and a representative of the Commission. Since the entry into force of the GDPR, the Article 29 Working Party has been replaced by the EDPB (see Article 94(2) of that regulation).

85 See European Data Protection Supervisor, Opinion 4/2016 of 30 May 2016 on the 'EU-US Privacy Shield draft adequacy decision'. The European Data Protection Supervisor was established by Article 1(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1). He monitors the application of the provisions of that regulation.

86 See point 112 of this Opinion.

87 I recall that the essential equivalence of the level of protection guaranteed by a third State by comparison with that which is required in the Union must also be evaluated when, in the context of a specific transfer based on the standard contractual clauses provided for in Decision 2010/87, the controller or, failing that, the competent supervisory authority is to ascertain whether the public authorities of the third country of destination subject the importer to requirements that exceed the limits of what is necessary in a democratic society (see Clause 5 in the Annex to Decision 2010/87 and footnote relating to that clause). See points 115, 134 and 135 of this Opinion.

204. In that regard, it should be borne in mind that the *raison d'être* of the restrictions that EU law places on international transfers of personal data, by requiring that the continuity of the level of protection of the fundamental rights of the data subjects be guaranteed, is designed to avoid the risk that the standards applicable within the Union will be circumvented.[88] As Facebook Ireland maintains in essence, it would be wholly unjustified, having regard to that objective, if a third country were expected to comply with requirements that did not correspond to obligations borne by the Member States.

205. In accordance with Article 51(1), the Charter applies to the Member States only when they are implementing Union law. Consequently, the validity of an adequacy decision having regard to the restrictions on the exercise of the data subjects' fundamental rights originating in the rules of the third country of destination depends on a comparison between those restrictions and the restrictions which the provisions of the Charter allow the Member States to impose *solely in so far as similar rules of a Member State fall within the scope of EU law*.

206. However, the assessment of the adequacy of the level of protection ensured in the third State of destination cannot ignore any interference with the exercise of the fundamental rights of the persons concerned that would result from State measures, notably in the field of national security, which, if they were adopted by a Member State, would fall outside the scope of EU law. For the purposes of that assessment, Article 45(2)(a) of the GDPR requires that the rules on national security in force in that Member State, without any restriction whatsoever, be taken into account.

207. The assessment of the adequacy of the level of protection with regard to such State measures entails, in my view, a comparison of the safeguards attached to them with the level of protection required within the Union under the law of the Member States, including their commitments under the ECHR. Since the Member States' adherence to the ECHR requires that they ensure that their internal law is consistent with the provisions of that Convention and thus, as Facebook Ireland, the German and Czech Governments and likewise the Commission have submitted in essence, constitutes a common denominator in the Member States, I shall regard those provisions as the relevant comparator for the purposes of that assessment.

208. In this instance, as stated above,[89] the requirements relating to the national security of the United States take priority over the obligations of the undertakings which have self-certified on the basis of the 'privacy shield' decision. Also, the validity of that decision depends on whether those requirements are accompanied by safeguards that offer a level of protection essentially equivalent to that which must be ensured in the European Union.

209. The answer to that question requires that the standards — namely those derived from the Charter, or indeed from the ECHR — to which rules applicable to the surveillance of electronic communications comparable to those which the Commission examined in the 'privacy shield' decision must correspond, within the Union, be identified in advance. The determination of the applicable standards depends on whether rules such as section 702 of the FISA and EO 12333 would, if they emanated from a Member State, fall within the limitation placed on the scope of the GDPR pursuant to Article 2(2) of that regulation, read in the light of Article 4(2) TEU.

88 See point 117 of this Opinion.

89 See point 197 of this Opinion.

210. On that point, it follows from the wording of Article 4(2) TEU and from settled case-law that EU law and, in particular, the instruments of secondary legislation concerning the protection of personal data do not apply to activities connected with the protection of national security in so far as they constitute activities of the State or of State authorities that are unrelated to fields in which individuals are active. [90]

211. That principle means, *on the one hand*, that rules in the field of the protection of national security do not come within the scope of EU law where they govern only State activities and do not apply to any activity carried out by individuals. Consequently, EU law does not in my view apply to national measures relating to the collection and use of personal data that are directly implemented by the State for the purposes of the protection of national security, without imposing specific obligations on private operators. In particular, as the Commission claimed at the hearing, a measure adopted by a Member State which, like EO 12333, authorised direct access by its security services to data in transit, would be excluded from the scope of EU law. [91]

212. Far more complex is the question whether, *on the other hand*, national provisions which, in the same way as section 702 of the FISA, require electronic communications services providers to lend their support to the authorities competent in national security matters in order to allow them to access certain personal data also fall outside the scope of EU law.

213. Whereas the *PNR* judgment argues in favour of a positive answer to that question, the reasoning adopted in the judgments in *Tele2 Sverige* and *Ministerio Fiscal* might justify its being answered in the negative.

214. In the *PNR* judgment, the Court annulled the decision whereby the Commission had found that the level of protection of personal data contained in the air passengers' files (Passenger Name Records, PNR) transferred to the United States authority competent for customs and border protection was adequate. [92] The Court held that the processing to which that decision related — namely the transfer of PNR data by the airlines to the authority in question — fell, *having regard to its object*, within the exclusion from the scope of Directive 95/46 provided for in Article 3(2) of that directive. According to the Court, that processing was necessary not for the supply of services but for the safeguarding of public security and for law-enforcement purposes. Since the transfer at issue came

90 See, in particular, judgment of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596, paragraphs 43 and 44); *PNR* judgment (paragraph 58); judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia* (C-73/07, EU:C:2008:727, paragraph 41); judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, 'the judgment in *Tele2 Sverige*', paragraph 69); and judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, 'the judgment in *Ministerio Fiscal*', paragraph 32).

91 In order to avoid any confusion on this point, I would emphasise that, in the 'privacy shield' decision, the Commission was not in a position to determine whether the United States does actually intercept communications sent via the transatlantic cables, since the United States authorities did not confirm or deny that proposition (see recital 75 of that decision and letter of 22 February 2016 from Mr Robert Litt, in Annex VI, paragraph I(a), thereto). However, since the United States Government has not denied collecting data in transit on the basis of EO 12333, the Commission was in my view required, before making a finding of adequacy, to obtain assurances from the United States Government that such data-gathering, on the assumption that it did take place, would be accompanied by sufficient safeguards against the risks of misuse. It is from that aspect that the Commission, in recitals 68 to 77 of that decision, examined the limitations and safeguards that were to apply in such a situation pursuant to PPD 28.

92 Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Control (OJ 2004 L 235, p. 11).

within a framework established by the public authorities that related to public security, it was excluded from the scope of that directive in spite of the fact that the PNR data were initially collected by private operators in the context of a commercial activity coming within the scope of that directive that the transfer was organised by those operators.[93]

215. In the subsequent judgment in *Tele2 Sverige*,[94] the Court held that national provisions, based on Article 15(1) of Directive 2002/58/EC,[95] governing both the retention by telecommunications services providers of traffic and location data, as well as the access by the public authorities to the data retained for the purposes referred to in that provision — which include law enforcement and the protection of national security — come within the scope of that directive and, accordingly, of the Charter. According to the Court, neither the provisions relating to data retention nor those relating to access to the retained data are covered by the exclusion from the scope of that directive provided for in Article 1(3), which refers, in particular, to activities of the State in relation to criminal law and the protection of national security.[96] The Court confirmed that decision in the judgment in *Ministerio Fiscal*.[97]

216. Section 702 of the FISA differs from such legislation, however, in that that provision does not impose on electronic communications services providers any obligation to retain the data or to carry out any other processing in the absence of a request from the intelligence authorities for access to the data.

217. The question therefore arises whether national measures which impose on those providers an obligation to make data available to public authorities for national security purposes, *independently of any obligation to retain the data*, fall within the scope of the GDPR and therefore of the Charter.[98]

218. A *first approach* might consist in reconciling, as much as possible, the two lines of case-law mentioned above by interpreting the conclusion drawn by the Court in the judgments in *Tele2 Sverige* and *Ministerio Fiscal*, concerning the applicability of EU law to measures governing access to the data by national authorities for the purpose of, inter alia, national security,[99] as being limited to situations in

93 Judgment in *PNR* (paragraphs 56 to 58). Furthermore, in the judgment of 10 February 2009, *Ireland* v *Parliament and Council* (C-301/06, EU:C:2009:68, paragraphs 90 and 91), the Court held that the considerations developed in the *PNR* judgment could not be transposed to the processing referred to by Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54). The Court justified that conclusion by the fact that Directive 2006/24, unlike the decision at issue in the *PNR* judgment, governed only the activities of services providers in the internal market and did not regulate the activities of public authorities for law-enforcement purposes. By that reasoning, the Court seems to have confirmed that, conversely, the conclusion drawn in the *PNR* judgment would have been capable of being transposed to provisions relating to access to the retained data or to their use by those authorities.

94 Judgment in *Tele2 Sverige* (paragraphs 67 to 81).

95 Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

96 Since Directive 2002/58 gives concrete form to the requirements of Directive 95/46, now repealed by the GDPR, which largely replicates its content, the case-law on the interpretation of Article 1(3) of Directive 2002/58 is, it seems to me, applicable by analogy to the interpretation of Article 2(2) of the GDPR. See, to that effect, judgments in *Tele2 Sverige* (paragraph 69) and *Ministerio Fiscal* (paragraph 32).

97 Judgment in *Ministerio Fiscal* (paragraphs 34, 35 and 37).

98 The same question has been raised in the context of three other references for a preliminary ruling pending before the Court. See Case C-623/17, *Privacy International* (OJ 2018 C 22, p. 29); Joined Cases C-511/18 and C-512/18, *La Quadrature du Net and Others* and *French Data Network and Others* (OJ 2018 C 392, p. 7).

99 In the judgment in *Tele2 Sverige*, although the Court concentrated on examining the justification for the interferences resulting from the retention and access measures at issue by reference to the objective of combating criminal offences, the conclusion which it reached also applies, *mutatis mutandis*, where such measures are aimed at protecting national security. Article 15(1) of Directive 2002/58 mentions, among the objectives capable of justifying such measures, both the fight against criminal offences and the protection of national security. Furthermore, Article 1(3) of Directive 2002/58 and Article 2(2) of the GDPR preclude from the scope of those measures State activities in both national security matters and areas of criminal law. Moreover, the measures at issue in the case that gave rise to the judgment in *Tele2 Sverige* also pursued an aim linked with national security. In paragraph 119 of that judgment, the Court expressly addressed the issue of justification for measures relating to the retention of and access to traffic and location data in the light of the objective of protecting national security in that it encompasses the fight against terrorism.

which the data are retained *by virtue of a legal obligation* imposed on the basis of Article 15(1) of Directive 2002/58. That conclusion would not apply, on the other hand, to the distinct factual context of the *PNR* judgment, which concerned the transfer to a United States authority competent for internal security of data retained by the airlines, for commercial purposes, on their own initiative.

219. According to a *second approach*, which the Commission recommends and which I consider more convincing, the reasoning adopted in the judgments in *Tele2 Sverige* and *Ministerio Fiscal* would justify the applicability of EU law to national rules that require electronic communications services providers to lend their assistance to the authorities responsible for national security so that they may access certain data, *it being immaterial whether or not those rules accompany a prior obligation to retain the data*.

220. The core of that reasoning is based not on the objective of the provisions at issue, as in the *PNR* judgment, but on the fact that those provisions governed the providers' activities and required them to carry out data processing. Those activities did not constitute State activities in the fields referred to in Article 1(3) of Directive 2002/58 and Article 3(2) of Directive 95/46, the content of which is essentially replicated in Article 2(2) of the GDPR.

221. Thus, in the judgment in *Tele2 Sverige*, the Court observed that 'access to the data retained by [the] providers … concerns the processing of personal data *by those providers*, and that processing falls within the scope of that directive.[100] Likewise, it held in the judgment in *Ministerio Fiscal* that legislative measures requiring providers to grant competent authorities access to the retained data 'necessarily involve the processing, *by those providers*, of those data'.[101]

222. The 'making available' of data by the controller for the benefit of a public authority satisfies the definition of 'processing' in Article 4(2) of the GDPR.[102] The same applies to the prior filtering of the data by means of search criteria for the purposes of isolating the data to which the public authorities have requested access.[103]

223. I conclude that, following the reasoning adopted by the Court in the judgments in *Tele2 Sverige* and *Ministerio Fiscal*, the GDPR and therefore the Charter apply to national rules that require a provider of electronic communications services to lend its assistance to the authorities responsible for national security by making data available to them, where appropriate after having filtered them, even independently of any legal obligation to retain the data.

224. In addition, that interpretation seems to follow, at least implicitly, from the judgment in *Schrems*. As the DPC, the Austrian and Polish Governments and the Commission have emphasised, the Court, when examining the validity of the 'safe harbour' decision, held in that judgment that the law of the third country to which an adequacy decision relates must provide, against the interferences by its public authorities with data subjects' fundamental rights for national security purposes, safeguards essentially equivalent to those arising under, in particular, Articles 7, 8 and 47 of the Charter.[104]

100 Judgment in *Tele2 Sverige* (paragraph 78, emphasis added). As shown by the use of the word 'further', it was only in order to confirm that conclusion concerning the applicability of Directive 2002/58 that the Court emphasised, in paragraph 79 of that judgment, the intrinsic connection between the obligation to retain the data at issue in the case that gave rise to that judgment and the provisions relating to access by the national authorities to the retained data.

101 Judgment in *Ministerio Fiscal* (paragraph 37, emphasis added).

102 See, to that effect, judgment in *Ministerio Fiscal* (paragraph 38).

103 See, to that effect, judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 28).

104 Judgment in *Schrems* (paragraphs 91 to 96). In recitals 90, 124 and 141 of the 'privacy shield' decision, moreover, the Commission refers to the provisions of the Charter, thus accepting the principle that limitations of fundamental rights that meet an objective of protecting national security must be consistent with the Charter.

225. It follows, more specifically, that a national measure requiring electronic communications services providers to respond to a request from the authorities with competence for national security for access to certain data retained by those providers in the context of their commercial activities, independently of any legal obligation, by identifying in advance the data requested by the application of selectors (as in the context of the PRISM programme), would not fall within Article 2(2) of the GDPR. The same would apply to a national measure requiring undertakings operating the telecommunications 'backbone' to grant the authorities responsible for national security access to data transiting via the infrastructures which they operate (as in the context of the Upstream programme).

226. Conversely, once those data have come into the possession of the State authorities, the retention and subsequent use of those data by those authorities for national security purposes are in my view, for the same reasons as those set out in point 211 of this Opinion, covered by the derogation provided for in Article 2(2) of the GDPR and therefore do not come within the scope of that regulation or, accordingly, of the Charter.

227. In view of all of the foregoing, I consider that the review of the validity of the 'privacy shield' decision by reference to the restrictions on the principles set out in that decision that are likely to result from the activities of the United States intelligence authorities requires a double verification.

228. It will be necessary, *in the first place*, to examine whether the United States ensures a level of protection essentially equivalent to that which follows from the provisions of the GDPR and the Charter against the restrictions resulting from the application of section 702 of the FISA, in that that provision allows the NSA to require providers to make personal data available to it.

229. *In the second place*, the provisions of the ECHR will constitute the relevant reference framework for the purpose of evaluating whether the limitations that the implementation of EO 12333 might entail — in that it authorises the intelligence authorities to collect personal data themselves, without the assistance of private operators — call into question the adequacy of the level of protection afforded in the United States. Those provisions will also provide the standards of comparison that will make it possible to assess the adequacy of that level of protection with respect to the retention and use by those authorities for national security purposes of the data acquired.

230. It will still be necessary, however, to determine whether a finding of adequacy entails that the collection of data pursuant to EO 12333 is accompanied by a level of protection essentially equivalent to that which must be ensured within the Union, *even to the extent that the collection of the data took place outside the territory of the United States*, during the stage in which the data are in transit from the Union to that third country.

(2) The need to ensure an adequate level of protection while the data are in transit

231. Three distinct positions were defended before the Court as regards the need or otherwise for the Commission to take account, for the purpose of evaluating the adequacy of the level of protection ensured in a third country, of national measures relating to access to the data by the authorities of that third country, outside its territory, during the stage in which the data are in transit from the Union to its territory.

232. First, Facebook Ireland and the United States and United Kingdom Governments maintain, in essence, that the existence of such measures has no impact in the context of a finding of adequacy. They rely, in support of that approach, on the fact that it is impossible for that third State to monitor all the means of communication outside its territory by which the data travel from the Union, so that by definition it could never be guaranteed that another third State will not secretly collect the data while they are in transit.

233. Second, the DPC, Mr Schrems, the EPIC, the Austrian and Netherlands Governments, the Parliament and the EDPB claim that the requirement of continuity of the level of protection, set out in Article 44 of the GDPR, means that that level must be adequate throughout the transfer, including when the data travel via submarine cables before reaching the territory of the third country of destination.

234. While recognising that principle, the Commission maintains, third, that the purpose of a finding of adequacy is confined to the protection ensured by the third country in question *within its borders*, so that the fact that an adequate level of protection is not guaranteed *during transit* to that third country does not call into question the validity of an adequacy decision. It is nonetheless for the controller, in accordance with Article 32 of the GDPR, to ensure the security of the transfer by protecting the personal data as much as possible during the stage of transit to that third country.

235. In that regard, I note that pursuant to Article 44 of the GDPR a transfer is subject to compliance with the conditions set out in the provisions of Chapter V of that regulation in so far as the data may be processed 'after transfer'. Those words might be understood as meaning either, as the United States Government maintained in its written answer to the questions put by the Court, that those conditions must be complied with *once the data have arrived at their destination*, or that they are binding *after the transfer has been initiated* (including during the transit stage).

236. As the wording of Article 44 of the GDPR is not conclusive, a teleological interpretation leads me to adopt the second of those interpretations and therefore to support the second of the approaches referred to above. If the requirement of continuity of the level of protection laid down in that provision were considered to cover only the surveillance measures implemented within the territory of the third country of destination, it could be circumvented when that third country applied such measures outside its territory during the stage in which the data are in transit. In order to avoid that risk, the evaluation of the adequacy of the level of protection ensured by a third country must cover all the provisions, in particular in national security matters, of the legal order of that third country, [105] which also include both those relating to the surveillance implemented on its territory and those that allow surveillance of the data in transit to that territory. [106]

237. That being the case, no one disputes that, as the EDPB has emphasised, the evaluation of the adequacy of the level of protection concerns only, as is apparent from Article 45(1) of the GDPR, the provisions of the legal order *of the third country of destination of the data*. The fact that it is impossible, as Facebook Ireland and the United States and United Kingdom Governments submit, to ensure that another third State will not secretly collect those data while they are in transit, does not affect that evaluation. Moreover, such a risk cannot be precluded even after the data have arrived on the territory of the third State of destination.

238. It is also true, moreover, that when the Commission assesses the adequacy of the level of protection guaranteed by a third country it might find that that third country fails to disclose to it the existence of certain secret surveillance programmes. It does not follow, however, that, *when such programmes are brought to its knowledge*, the Commission may refrain from taking them into account in its examination of adequacy. Likewise, if, after the adoption of an adequacy decision, the existence of certain secret surveillance programmes, implemented by the third country in question on its territory or while the data are in transit to that territory, is disclosed to it, the Commission is required to reconsider its finding as to the adequacy of the level of protection ensured by that third country if such disclosure gives rise to doubt in that respect. [107]

105 See, to that effect, judgment in *Schrems* (paragraphs 74 and 75).

106 See, to that effect, EDPB, EU-US Privacy Shield — Second Annual Joint Review, 22 January 2019 (p. 17, paragraph 86).

107 See Article 45(5) of the GDPR. See also judgment in *Schrems* (paragraph 76).

(3) The taking into consideration of the findings of fact made by the Commission and the referring court concerning United States law

239. While it is common ground that the Court does not have jurisdiction to carry out an interpretation of the law of a third country which would be binding in that country's legal order, the validity of the 'privacy shield' decision depends on the validity of the assessments made by the Commission concerning the level of protection, guaranteed by the law and practices of the United States, of the fundamental rights of the persons whose data are transferred to that third country. The Commission was required to state reasons for its finding of adequacy with regard to those matters, relating in particular to the content of the law of that third country, referred to in Article 45(2) of the GDPR. [108]

240. The High Court set out, in its judgment of 3 October 2017, a number of detailed findings describing the relevant aspects of United States law after evaluating the evidence adduced by the parties to the dispute. [109] That account largely coincides with the findings made by the Commission, in the 'privacy shield' decision, in relation to the content of the rules applicable to the collection of and access to the transferred data by the United States intelligence authorities and to the remedies and oversight mechanisms associated with those activities.

241. The referring court, like a number of the parties and interested persons who have submitted observations to the Court, call into question the legal consequences which the Commission based on those findings — namely the conclusion that the United States ensures an adequate level of protection of the fundamental rights of the persons whose data are transferred on the basis of that decision — rather than the description which it gave of the content of United States law.

242. In those circumstances, I shall essentially evaluate the validity of the 'privacy shield' decision in the light of the findings made by the Commission itself as regards the content of United States law, by examining whether those findings warranted the adoption of that adequacy decision.

243. In that respect, I do not subscribe to the viewpoint, defended by the DPC and Mr Schrems, that the findings made by the High Court concerning United States law are binding on the Court when it examines the validity of the 'privacy shield' decision. They claim that, since foreign law is a question of fact under Irish procedural law, the referring court alone has jurisdiction to establish its content.

244. Consistent case-law does admittedly recognise that the national court has exclusive jurisdiction to establish the relevant elements of fact and to interpret the law of a Member State and apply it to the dispute pending before it. [110] That case-law reflects the allocation of functions between the Court and the referring court in the procedure established by Article 267 TFEU. Although the Court has sole jurisdiction to interpret EU law and to rule on the validity of secondary law, it is for the national court, which is required to settle the actual dispute pending before it, to establish the factual and regulatory context of that dispute so that the Court can provide it with a useful answer.

108 Thus, the 'safe harbour' decision was declared to be invalid on the ground that the Commission had not stated in that decision that the United States in fact ensured an adequate level of protection by reason of its domestic law or its international commitments (see judgment in *Schrems*, paragraph 97). In particular, the Commission had not established the existence of State rules intended to limit any interferences with data subjects' fundamental rights (judgment in *Schrems*, paragraph 88) or of effective legal protection against such interferences (judgment in *Schrems*, paragraph 89).

109 Points 54 to 73 of this Opinion summarise these findings.

110 See, in particular, judgments of 4 May 1999, *Sürül* (C-262/96, EU:C:1999:228, paragraph 95); of 11 September 2008, *Eckelkamp and Others* (C-11/07, EU:C:2008:489, paragraph 32); and of 26 October 2016, *Senior Home* (C-195/15, EU:C:2016:804, paragraph 20).

245. The *raison d'être* of that exclusive jurisdiction of the national court does not seem to me to be capable of being transposed to the establishment of the law of a third country as an element liable to influence the Court's conclusion as to the validity of an act of secondary law.[111] Since a declaration that such an act is invalid is binding *erga omnes* in the legal order of the Union,[112] the Court's conclusion cannot depend on the origin of the reference for a preliminary ruling. As Facebook Ireland and the United States Government have emphasised, that conclusion would be dependent on the origin of the reference if the Court were bound by the findings made by the referring court in respect of the law of a third State, which are likely to vary according to the national court that made those findings.

246. In the light of those considerations, I consider that, where the answer to a question for a preliminary ruling on the validity of an EU measure implies that the content of the law of a third State be evaluated, although the Court may take the findings made by the referring court in respect of the law of that third State into account, it is not bound by them. The Court may, where appropriate, disregard them or supplement them, taking into consideration, while observing the *inter partes* principle, other sources in order to establish the elements necessary for the evaluation of the validity of the act in question.[113]

(4) The scope of the 'essential equivalence' standard

247. The validity of the 'privacy shield' decision depends, it will be recalled, on whether the legal order of the United States ensures, for persons whose data are transferred from the Union to the United States, a level of protection that is 'essentially equivalent' to that guaranteed within the Member States under the GDPR and the Charter and also, in the fields excluded from the application of EU law, their commitments pursuant to the ECHR.

248. As the Court made clear in the judgment in *Schrems*,[114] that standard does not mean that the level of protection must be 'identical' to that required in the Union. Although the means which a third country employs in order to protect the data subjects' rights may differ from those prescribed by the GDPR read in the light of the Charter, 'those means must … prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union'.

249. It also follows from that judgment, in my view, that the law of the third State of destination may reflect its own scale of values according to which the respective weight of the various interests involved may diverge from that attributed to them in the EU legal order. Moreover, the protection of personal data that prevails within the European Union meets a particularly high standard by comparison with the level of protection in force in the rest of the world. The 'essential equivalence' test should therefore in my view be applied in such a way as to preserve a certain flexibility in order to take the various legal and cultural traditions into account. That test implies, however, if it is not to be deprived of its substance, that certain minimum safeguards and general requirements for the protection of fundamental rights that follow from the Charter and the ECHR have an equivalent in the legal order of the third country of destination.[115]

111 See, in that regard, judgment of the Supreme Court of 31 May 2019 (paragraph 6.18).

112 See judgment of 13 May 1981, *International Chemical Corporation* (66/80, EU:C:1981:102, paragraphs 12 and 13).

113 See, in that regard, judgment of 22 March 2012, *GLS* (C-338/10, EU:C:2012:158, paragraphs 15, 33 and 34), where the Court, in order to assess the validity of a regulation imposing an anti-dumping duty, took account of Eurostat statistics produced by the Commission at the Court's request. See also judgment of 22 October 1991, *Nölle* (C-16/90, EU:C:1991:402, paragraphs 17, 23 and 24). Likewise, in the judgment in *Schrems* (paragraph 90), the Court, when examining the validity of the 'safe harbour' decision, took certain Commission communications into consideration.

114 Judgment in *Schrems* (paragraphs 73 and 74).

115 See, to that effect, WP29, 'Adequacy Referential (updated)', 28 November 2017, WP 254 (pp. 3, 4 and 9).

250. In that regard, in accordance with 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 and, subject to the principle of proportionality, be necessary and actually correspond to an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others. Those requirements correspond essentially to those set out in Article 8(2) of the ECHR. [116]

251. In accordance with Article 52(3) of the Charter, in so far as the rights guaranteed in Articles 7, 8 and 47 correspond to those enshrined in Articles 8 and 13 of the ECHR, they share their meaning and scope, it being understood that EU law may nonetheless afford them wider protection. From that aspect, and as my narrative will reveal, the standards resulting from Articles 7, 8 and 47 of the Charter, as interpreted by this Court, are in certain respects stricter than those arising under Article 8 of the ECHR according to the interpretation of those provisions by the European Court of Human Rights ('the ECtHR').

252. I also observe that certain cases pending before each of those courts invite them to reconsider certain aspects of their respective case-law. Thus, first, two recent judgments of the ECtHR on the surveillance of electronic communications — namely the judgments in *Centrüm för Rättvisa v. Sweden* [117] and in *Big Brother Watch v. United Kingdom* [118] — have been referred for reconsideration in the Grand Chamber. Second, three national courts have made references to this Court for preliminary rulings that open the discussion as to whether its case-law resulting from the judgment in *Tele2 Sverige* needs to be varied. [119]

253. Having made that clear, I shall now examine the validity of the 'privacy shield' decision by reference to Article 45(1) of the GDPR, read in the light of the Charter and the ECHR in that they guarantee the rights to respect for private life and to the protection of personal data (section (b)) and to effective judicial protection (section (c)).

(b) The validity of the 'privacy shield' decision by reference to the rights to respect for private life and to the protection of personal data

254. In the context of its fourth question, the referring court, in essence, calls into question the essential equivalence between the level of protection guaranteed by the United States and that which data subjects derive, within the Union, from their fundamental rights to respect for private life and the protection of personal data.

(1) The existence of interferences

255. In recitals 67 to 124 of the 'privacy shield' decision, the Commission refers, in particular, to the possibility that the United States public authorities will have access to the data transferred from the Union and will use them for national security purposes in the context of the programmes based, in particular, on section 702 of the FISA or EO 12333.

116 Article 8(2) of the ECHR does not, however, refer to the concept of the 'essence' of the right to respect for private life. See, on that subject, footnote 161 of this Opinion.

117 ECtHR, 19 June 2018 (CE:ECHR:2018:0619JUD003525208, 'the judgment in *Centrüm för Rättvisa*').

118 ECtHR, 13 September 2018 (CE:ECHR:2018:0913JUD005817013, 'the judgment in *Big Brother Watch*').

119 See the cases cited in footnote 98 of this Opinion and Case C-520/18, *Ordre des barreaux francophones et germanophones and Others* (OJ 2018 C 408, p. 39).

256. The implementation of those programmes entails intrusions on the part of the United States intelligence services which, if they were attributable to the authorities of a Member State, would be regarded as interferences with the exercise of the right to respect for private life guaranteed in Article 7 of the Charter and Article 8 of the ECHR. They also expose the data subjects to a risk that their personal data will undergo processing that does not satisfy the requirements set out in Article 8 of the Charter. [120]

257. I would make clear at the outset that the rights to respect for private life and to the protection of personal data encompass the protection not only of the content of the communications but also the traffic data [121] and location data (designated together by the word 'metadata'). Both this Court and the ECtHR have recognised that the metadata, like the content data, are capable of revealing very specific data relating to the private life of an individual. [122]

258. According to the Court's case-law, for the purposes of establishing the existence of an interference with the exercise of the right guaranteed in Article 7 of the Charter, it does not matter whether the data concerned are sensitive or whether the persons concerned have been inconvenienced in any way as a result of the surveillance measure at issue. [123]

259. That having been stated, the surveillance programmes based on section 702 of the FISA entail, primarily, interferences with the exercise of the fundamental rights of individuals whose communications correspond to selectors chosen by the NSA and are therefore sent to the NSA by the electronic communications services providers. [124] More specifically, the obligation imposed on providers to *make the data available* to the NSA, in so far as it derogates from the principle of confidentiality of communications, [125] entails in itself an interference even if those data are not subsequently consulted and used by the intelligence authorities. [126] The *retention* and actual *access* by those authorities to the metadata and content of the communications made available to them, just like the *use* of those data, constitute additional interferences. [127]

260. What is more, according to the findings of the referring court [128] and other sources such as the PCLOB report on programmes implemented pursuant to section 702 of the FISA brought to the Court's attention by the United States Government, [129] the NSA already had *access for filtering purposes*, in the context of the Upstream programme, to huge 'packets' of data forming part of the communication flows passing through the telecommunications 'backbone' and encompassing communications that do not contain the selectors identified by the NSA. The NSA could examine

120 Although processing may infringe both Articles 7 and 8 of the Charter, the relevant framework of analysis for the purposes of applying Article 8 is structurally different from that applicable to Article 7. The right to protection of personal data means, in the words of Article 8(2) of the Charter, that 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law' and that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. Infringement of that right assumes that personal data have been processed in breach of those requirements. That is the case, in particular, where the processing is not based on either the consent of the person concerned *or on some other legitimate basis laid down by law*. In such a situation, although the question of the existence of an interference and that of its justification are conceptually distinct in the context of Article 7 of the Charter, they overlap in the case of Article 8 of the Charter.

121 Article 2(b) of Directive 2002/58 defines 'traffic data' as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.

122 See judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238, 'the judgment in *Digital Rights Ireland*', paragraph 27) and judgment in *Tele2 Sverige* (paragraph 99). See also ECtHR, 2 August 1984, *Malone v. United Kingdom* (CE:ECHR:1984:0802JUD000869179, § 84) and 8 February 2018, *Ben Faiza v. France* (CE:ECHR:2018:0208JUD003144612, § 66).

123 See judgment in *Digital Rights Ireland* (paragraph 33); Opinion 1/15 (paragraph 124); and judgment in *Ministerio Fiscal* (paragraph 51).

124 See recitals 78 to 81 and Annex VI, point II, to the 'privacy shield' decision.

125 See, in that regard, judgment in *Digital Rights Ireland* (paragraph 32).

126 See, in that regard, Opinion 1/15 (paragraphs 124 and 125), from which it is clear that the communication of data to a third party constitutes an interference with the exercise of the fundamental rights of the person concerned irrespective of their subsequent use.

127 See, to that effect, judgment in *Digital Rights Ireland* (paragraph 35); judgment in *Schrems* (paragraph 87); and Opinion 1/15 (paragraphs 123 to 126).

128 See point 60 of this Opinion.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], of 2 July 2014 ('the PCLOB report', pp. 84 and 111). See also WP29, EU-U.S. Privacy Shield — First Annual Joint Review, of 28 November 2017, WP 255 (in B.1.1, p. 15).

those packets of data only in order to determine quickly, in an automated fashion, whether they contain those selectors. Only communications thus filtered are then saved in the NSA's databases. That access to the data for filtering purposes also constitutes in my view an interference with the exercise of the right to respect for the private life of the data subjects, whatever the subsequent use of the data retained.[130]

261. Furthermore, the making available and the filtering of the data in question,[131] access to the data by the intelligence authorities, and likewise any retention, analysis and use of the data come within the concept of 'processing' within the meaning of Article 4(2) of the GDPR and Article 8(2) of the Charter. Such processing must therefore meet the requirements laid down in the latter provision.[132]

262. Surveillance on the basis of EO 12333 might entail direct access by the intelligence authorities to the data in transit, causing an interference with the exercise of the right guaranteed by Article 8 of the ECHR. In addition to that interference would be the interference consisting in the possible subsequent use of those data.

(2) The requirement that the interferences be 'provided for by law'

263. In accordance with the settled case-law of this Court[133] and of the ECtHR,[134] the requirement that any interference with the exercise of fundamental rights must be 'provided for by law', within the meaning of Article 52(1) of the Charter and Article 8(2) of the ECHR, implies not only that the measure providing for the interference must have a legal basis in domestic law but also that that legal basis must have certain qualities of accessibility and foreseeability in such a way as to avoid the risk of arbitrariness.

264. In that regard, the parties and interested persons who have submitted observations to the Court disagree, essentially, as to whether section 702 of the FISA and EO 12333 satisfy the condition relating to the foreseeability of the law.

265. That condition, as interpreted by this Court[135] and by the ECtHR,[136] requires that regulations which entail an interference with the exercise of the right to respect for private life lay down clear and precise rules governing the scope and application of the measure at issue and imposing a minimum of requirements, in such a way as to provide the persons concerned with sufficient guarantees to protect their data against the risks of abuse and also against any unlawful access to or use of the data. Such

130 See footnote 126 of this Opinion.

131 See, in that respect, point 222 of this Opinion.

132 See Opinion 1/15 (paragraph 123 and the case-law cited).

133 See in particular Opinion 1/15 (paragraph 146).

134 See in particular ECtHR, 2 August 1984, *Malone v. United Kingdom* (CE:ECHR:1984:0802JUD000869179, §66); decision of 29 June 2006, *Weber and Saravia v. Germany* (CE:ECHR:2006:0629DEC005493400, §84 and the case-law cited); and judgment of 4 December 2015, *Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, 'judgment in *Zakharov*', § 228).

135 See, in particular, judgment in *Digital Rights Ireland* (paragraphs 54 and 65); judgment in *Schrems* (paragraph 91); judgment in *Tele2 Sverige* (paragraph 109); and Opinion 1/15 (paragraph 141).

136 See, in particular, decision in *Weber and Saravia* (§§ 94 and 95); judgment in *Zakharov* (§ 236); and ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary* (CE:ECHR:2016:0112JUD003713814, 'judgment in *Szabó and Vissy*', § 59).

rules must, in particular, indicate in which circumstances and on what conditions the public authorities may retain, have access to and use personal data.[137] Furthermore, the legal basis that allows the interference must itself define the scope of the limitation on the exercise of the right to respect for private life.[138]

266. I doubt, as do Mr Schrems and the EPIC, that EO 12333, like PPD 28, which sets out guarantees applicable to all signals intelligence activities,[139] are sufficiently foreseeable to have the 'quality of law'.

267. Those instruments expressly state that they do not confer legally enforceable rights on the persons concerned.[140] The latter cannot therefore rely on the guarantees set out in PPD 28 before the courts.[141] The Commission considered, moreover, in the 'privacy shield' decision, that although the guarantees set out in PPD 28 have binding force for the intelligence services,[142] they are 'not phrased in … legal terms'.[143] EO 12333 and PPD 28 bear more resemblance to internal administrative instruction that can be revoked or amended by the President of the United States. The ECtHR has already held that internal administrative directives do not constitute 'law'.[144]

268. As regards section 702 of the FISA, the foreseeability of that provision is called into question by Mr Schrems on the ground that it does not frame the choice of selection criteria used to filter the data with sufficient guarantees against the risks of misuse. Since that problem also concerns the strict necessity of the interferences provided for in section 702 of the FISA, I shall examine it below.[145]

269. The third question overlaps with the theme of compliance with the conditions relating to the 'quality of law'. By that question, the referring court seeks, in essence, to ascertain whether the adequacy of the level of protection ensured in a third country must be examined by reference solely to the legally binding rules in force in that third country and to the practices designed to ensure compliance with those rules, or also to the various non-binding instruments and extra-judicial control mechanisms applied there.

137 See judgment in *Tele2 Sverige* (paragraph 117) and Opinion 1/15 (paragraph 190). See also, inter alia, ECtHR, 2 August 1984, *Malone v. United Kingdom* (CE:ECHR:1984:0802JUD000869179, § 67); judgment in *Zakharov* (§ 229); and judgment in *Szabó and Vissy* (§ 62). The ECtHR stated in those cases that the requirement of foreseeability does not have the same scope with regard to the interception of communications as in other fields. In the context of secret measures of surveillance, 'foreseeability … cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly'.

138 Opinion 1/15 (paragraph 139). See also, to that effect, ECtHR, 25 March 1983, *Silver and Others v. United Kingdom* (CE:ECHR:1983:0325JUD000594772, §§ 88 and 89).

139 Recitals 69 to 77 of and Annex VI to the 'privacy shield' decision contain an overview of PPD 28. It is stated in that overview that that presidential directive applies to intelligence activities based on section 702 of the FISA as well as to activities carried out outside the United States.

140 Paragraph 3.7(c) of EO 12333 states: 'This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person'. Article 6(d) of PPD 28 also provides: 'This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person'.

141 See, to that effect, EDPB, EU-U.S. Privacy Shield — Second Annual Joint Review, 22 January 2019 (paragraph 99).

142 See recitals 69 and 77 of the 'privacy shield' decision.

143 Recital 76 of the 'privacy shield' decision.

144 See ECtHR, 25 March 1983, *Silver and Others v. United Kingdom* (CE:ECHR:1983:0325JUD000594772, §§ 26 and 86).

145 See points 295 to 301 of this Opinion. In the judgment in *Tele2 Sverige* (paragraphs 116 and 117) and Opinion 1/15 (paragraphs 140 and 141), the condition that the law must be foreseeable was presented as being intrinsically linked with the condition that the interference must be necessary and proportionate. Likewise, according to the case-law of the ECtHR, the existence of effective safeguards against the risks of abuse forms part of both the condition that the interference be 'foreseeable' and the condition that it be 'necessary in a democratic society', compliance with those conditions being examined together. See ECtHR, 18 May 2010, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, § 155); judgment in *Zakharov* (§ 236); judgment in *Centrüm för Rättvisa* (§ 107); and judgment in *Big Brother Watch* (§ 322).

270. In that respect, Article 45(2)(a) of the GDPR sets out a non-exhaustive list of circumstances which the Commission is to take into account when assessing the adequacy of the level of protection afforded by a third country. Those circumstances include the applicable legislation and the way in which it is implemented. Article 45(2)(a) also mentions the impact of other types of rules, such as professional rules and security measures. It also requires that 'effective and enforceable … rights' and 'effective administrative and judicial redress for the data subjects whose personal data are being transferred' be taken into consideration. [146]

271. Read in its entirety and having regard to the non-exhaustive nature of the list contained therein, that provision means, in my view, that practices or instruments that do not have an accessible and foreseeable legal basis may be taken into account in the global assessment of the level of protection guaranteed in the third country in question in such a way as to support guarantees which themselves have a legal basis which is accessible and foreseeable. However, as the DPC, Mr Schrems, the Austrian Government and the EDPB essentially claim, such instruments or practices cannot take the place of such guarantees or, accordingly, themselves ensure the requisite level of protection.

(3) No compromising of the essence of the fundamental rights

272. The requirement, set out in Article 52(1) of the Charter, that any limitation of the rights and freedoms guaranteed by the Charter must respect the essence of those rights and freedoms means that, when an interference compromises those rights and freedoms, no legitimate objective can justify it. The interference is then deemed to be contrary to the Charter without it being necessary to examine whether it is appropriate and necessary for the purpose of achieving the objective pursued.

273. In that respect, the Court has held that national legislation authorising generalised access to the *content* of electronic communications by the public authorities compromises the very essence of the right to respect for private life guaranteed in Article 7 of the Charter. [147] Conversely, while emphasising the risks associated with access to and the analysis of *traffic and location data*, [148] the Court considered that the essence of that right is not affected when national legislation permits generalised access by the State authorities to such data. [149]

274. Section 702 of the FISA cannot in my view be considered to authorise the United States intelligence authorities to have generalised access to the content of electronic communications.

275. First, access to the data by the intelligence authorities, on the basis of section 702 of the FISA, *for the purpose of their possible analysis and use*, is limited to data that satisfy the selection criteria associated with individual targets.

146 See also recital 104 of the GDPR.

147 See judgment in *Schrems* (paragraph 94). See also judgments in *Digital Rights Ireland* (paragraph 39) and *Tele2 Sverige* (paragraph 101). Given the close link between the rights to respect for private life and to protection of personal data, a national measure that granted the public authorities general access to the content of communications would also to my mind infringe the essential content of the right enshrined in Article 8 of the Charter.

148 See point 257 of this Opinion. In the judgment in *Tele2 Sverige* (paragraph 99), the Court emphasised that metadata provide, in particular, the means of establishing the profile of data subjects. In Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014 (p. 5), the WP29 observes that, because of their structured nature, metadata are easier to aggregate and analyse than content data.

149 See judgment in *Tele2 Sverige* (paragraph 99). Some commentators have questioned the validity of the distinction between generalised access to the content of communications and generalised access to metadata given the developments in technologies and modes of communication. See Falot, N. and Hijmans, H., 'Tele2: de afweging tussen privacy en veiligheid nader omlijnd', *Nederlands Tijdschrift voor Europees Recht*, No 3, 2017 (p. 48) and Ojanen, T., 'Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter' (commentary on the judgment in *Schrems*), *European Constitutional Law Review*, 2016 (p. 5).

276. Second, the Upstream programme might, admittedly, entail generalised access to the content of electronic communications *for automated filtering purposes* in the event that selectors were applied not only to the 'from' and 'to' fields, but also to the entire content of the communications flows (search 'concerning' the selector).[150] However, as the Commission maintains and contrary to the contentions of Mr Schrems and the EPIC, temporary access by the intelligence authorities to all the content of the electronic communications *for the sole purpose of filtering* by the application of selection criteria cannot be treated as equivalent to generalised access to that content.[151] To my mind, the gravity of the interference resulting from that temporary access for automatic filtering purposes does not attain the gravity of the interference resulting from generalised access to that content by the public authorities with a view to its analysis and possible use.[152] Temporary access for filtering purposes does not allow those authorities to retain the metadata or the content of the communications that do not meet the selection criteria or, in particular, as the United States Government has observed, to establish profiles relating to the persons not targeted by those criteria.

277. That being so, the question whether targeting by means of selectors in the context of the programmes based on section 702 of the FISA effectively limits the powers of the intelligence authorities depends on the framework of the choice of selectors.[153] Mr Schrems claims, on that point, that in the absence of sufficient control to that effect, United States law does not provide any safeguard against generalised access to the content of the communications already at the filtering stage, and therefore compromises the very essence of the data subjects' right to respect for private life.

278. As I shall explain in greater detail below,[154] I tend to share those doubts as to the sufficiency of the framework of the choice of selectors for the purposes of meeting the criteria of foreseeability and proportionality of the interferences. However, the existence of that framework, imperfect though it may be, precludes the conclusion that section 702 of the FISA permits generalised access by the public authorities to the content of the electronic communications and thus amounts to a breach of the very essence of the right enshrined in Article 7 of the Charter.

279. I would also emphasise that, in Opinion 1/15, the Court considered that the essence of the right to protection of personal data, guaranteed in Article 8 of the Charter, is preserved when the purposes of the processing are limited and the processing is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing.[155]

150 See footnote 87 of the 'privacy shield' decision. However, according to the EPIC's observations and to the United States Government's written answer to the questions put by the Court, the FISC required, in 2017, suspension of searches 'concerning' a selector because of irregularities that had affected searches of that type. Congress had however provided, in the act reapproving the FISA adopted in 2018, the possibility of introducing that type of searches with the consent of the FISC and Congress. See also EDPB, EU-U.S. Privacy Shield — Second Annual Joint Review, 22 January 2019 (p. 27, paragraph 55).

151 From that aspect, the referring court, in paragraphs 188 and 189 of its judgment of 3 October 2017, distinguishes 'bulk searching' and 'bulk acquisition, collection or retention'. It considers, essentially, that, if the Upstream programme involves 'bulk' searching in all the data flows passing through the telecommunications 'backbone', the acquisition, collection and retention are targeted in the sense that they are aimed only at the data containing the selectors in question.

152 See, to that effect, judgment of the Supreme Court of 31 May 2019 (paragraphs 11.2 and 11.3). The Supreme Court observes: 'it is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term "processing" covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis.'

153 See Opinion 1/15 (paragraph 122). See also Report of the European Commission for Democracy through Law (Venice Commission) of 15 December 2015 on the democratic oversight of signals intelligence agencies (CDL-AD(2015)011, p. 11): 'In practice, whether this process adequately limits unnecessary intrusion into innocent personal communications depends on both the relevance and specificity of the selector used and the quality of the computer algorithm employed to sort for relevant data within the parameters chosen …'.

154 See points 297 to 301 of this Opinion.

155 Opinion 1/15 (paragraph 150).

280. In the 'privacy shield' decision, the Commission found that both section 702 of the FISA and PPD 28 delimit the purposes for which data may be collected in the context of the programmes implemented on the basis of section 702 of the FISA.[156] The Commission also stated in that decision that PPD 28 lays down rules limiting access to the data and their storage and distribution, in order to ensure their security and to protect them against unauthorised access.[157] As will be shown below,[158] I entertain doubts, in particular, about whether the purposes of the processing at issue are defined with sufficient clarity and precision to ensure a level of protection essentially equivalent to that prevailing in the legal order of the Union. However, those possible weaknesses would not suffice, in my view, to substantiate a finding that such programmes would, if they were employed within the Union, violate the essence of the right to protection of personal data.

281. Furthermore, the adequacy of the level of protection guaranteed in the context of surveillance activities on the basis of EO 12333 must, it will be recalled, be evaluated by reference to the provisions of the ECHR. In that respect, it is apparent from the 'privacy shield' decision that the only restrictions placed on the implementation of measures based on EO 12333 for the purpose of collecting data relating to non-United States persons are those set out in PPD 28,[159] which provides that the use of external intelligence must be 'as tailored as feasible'. However, it expressly refers to the possibility of collecting data 'in bulk' outside the territory of the United States for the purposes of pursuing certain specific national security objectives.[160] In Mr Schrems' view, the provisions of PPD 28, which, incidentally, does not create rights for individuals, do not protect data subjects against the risk of generalised access to the content of their electronic communications.

282. I shall merely observe, on that subject, that the ECtHR has not had recourse, in its case-law relating to Article 8 of the ECHR, to the concept of violation of the essential content, or the very essence, of the right to respect for private life.[161] It has not thus far considered that regimes that allow the interception of electronic communications, even on a mass scale, *exceeded as such the margin of appreciation of the Member States*. The ECtHR considers that such regimes are compatible with Article 8(2) of the ECHR provided that they are accompanied by a number of minimum guarantees.[162] In those circumstances, it does not seem appropriate to me to conclude that a surveillance regime such as that provided for by EO 12333 would exceed the margin of appreciation of the Member States without undertaking any examination whatsoever of any guarantees that accompany it.

156 See recitals 70, 103 and 109 of the 'privacy shield' decision.

157 See recitals 83 to 87 of and Annex VI, point I(c) to the 'privacy shield' decision. I note that, according to the PCLOB report (pp. 51 to 66), the NSA's 'minimisation' procedures on the basis of section 702 of the FISA are aimed, so far as most of their aspects are concerned, only at United States persons. PPD 28 was intended to extend the applicable safeguards to non-United States persons. See PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, available at https://www.pclob.gov/reports/report-PPD28/ (p. 2). That being so, the storage and use of data for national security purposes after they have been acquired by the public authorities does not in my view fall within the scope of EU law (see point 226 of this Opinion). The adequacy of the level of protection ensured in the context of those activities must therefore be evaluated only by reference to Article 8 of the ECHR.

158 See points 283 to 289 of this Opinion.

159 In particular, the Commission stated, in recital 127 of the 'privacy shield' decision, that the Fourth Amendment to the United States Constitution does not extend to non-U.S. persons.

160 See recitals 73 and 74 of, and Annex VI, point I(b) to, the 'privacy shield' decision. Those objectives consist in combating espionage and other threats and activities on the part of foreign powers directed against the United States and its interests; against terrorist threats; against threats resulting from the development, possession, proliferation or use of weapons of mass destruction; against cybersecurity threats; against threats to the United States or allied armed forces; and against transnational criminal threats. According to footnote 5 of the PPD 28, the limitations on the objectives justifying the use of data collected in 'bulk' do not apply to signals intelligence data that are temporarily acquired to facilitate targeted collection.

161 Although the provisions of the ECHR do not mention the 'essential content' of fundamental rights, the equivalent concept of 'very essence' of a fundamental right may be found in the case-law of the ECtHR relating to certain of those provisions. See, as regards the very essence of the right to a fair trial guaranteed in Article 6 of the ECHR, in particular, ECtHR, 25 May 1985, *Ashingdane v. United Kingdom* (CE:ECHR:1985:0528JUD000822578, §§ 57 and 59); 21 December 2000, *Heaney and McGuinness v. Ireland* (CE:ECHR:2000:1221JUD003472097, §§ 55 and 58); and 23 June 2016, *Baka v. Hungary* (CE:ECHR:2016:0623JUD002026112, § 121). As regards the very essence of the right to marriage enshrined in Article 12 of the ECHR, see ECtHR, 11 July 2002, *Christine Goodwin v. United Kingdom* (CE:ECHR:2002:0711JUD002895795, §§ 99 and 101). As concerns the very essence of the right to education guaranteed in Article 2 of Protocol No. 1 to the ECHR, see ECtHR, 23 July 1968, case 'Relating to certain aspects of the laws on the use of language in education in Belgium' (CE:ECHR:1968:0723JUD000147462, § 5).

162 See, in particular, judgments in *Centrüm för Rättvisa* (§§ 112 to 114 and the case-law cited) and in *Big Brother Watch* (§ 337).

(4) The pursuit of a legitimate objective

283. In the words of Article 52(1) of the Charter, any limitation on the exercise of the rights recognised by the Charter must genuinely meet an objective of general interest recognised by the Union. Article 8(2) of the Charter also provides that any processing of personal data that is not based on the consent of the person concerned must have a 'legitimate basis laid down by law'. Article 8(2) of the ECHR lists the aims capable of justifying interference with the exercise of the right to respect for private life.

284. Under the 'privacy shield' decision, adherence to the principles which it sets out may be limited in order to meet obligations relating to national security, the public interest and law enforcement.[163] Recitals 67 to 124 of that decision examine more specifically the limitations that follow from access to and use of the data by the United States public authorities for national security purposes.

285. It is common ground that the protection of national security is a legitimate objective that may justify derogations from the requirements derived from the GDPR,[164] and also from the fundamental rights enshrined in Articles 7 and 8 of the Charter and Article 8 of the ECHR.[165] However, Mr Schrems, the Austrian Government and the EPIC have observed that the objectives pursued in the context of the surveillance programmes based on section 702 of the FISA and EO 12333 go beyond national security alone. The purpose of those instruments is to obtain 'foreign intelligence information', a concept which covers various types of information including — but not necessarily limited to — information relating to national security.[166] The concept of 'foreign intelligence information', within the meaning of section 702 of the FISA, thus covers data concerning the conduct of foreign affairs.[167] EO 12333 defines that concept as including information relating to the capabilities, intentions and activities of foreign powers, organisations or persons.[168] Mr Schrems calls into question the legitimate nature of the objective thus referred to in that it goes further than national security.

286. To my mind, the perimeter of national security may include, to a certain extent, the protection of interests relating to the conduct of foreign affairs.[169] Furthermore, it is not inconceivable that some of the purposes other than protection of national security which are covered by the concept of 'foreign intelligence information', as defined in section 702 of the FISA and in EO 12333, correspond to important objectives of general public interest capable of justifying an interference with the fundamental rights to respect for private life and the protection of personal data. Those objectives would, in any event, weigh less heavily than the protection of national security when the fundamental rights of those concerned are weighed against the objective sought by the interference.[170]

163 See point 197 of this Opinion.

164 See Article 23(1)(a) of the GDPR.

165 See judgment in *Schrems* (paragraph 88). The Court has regarded the related concept of 'public security' within the meaning of the provisions of the TFEU that permit derogations from the fundamental freedoms which it guarantees, as an autonomous concept of EU law covering both the internal and external security of the Member States (see, in particular, judgments of 26 October 1999, *Sirdar* (C-273/97, EU:C:1999:523, paragraph 17) and of 13 September 2016, *CS* (C-304/14, EU:C:2016:674, paragraph 39 and the case-law cited)). While internal security may be affected by, inter alia, a direct threat to the peace of mind and physical security of the population of the Member State concerned, external security may be jeopardised by, inter alia, the risk of a serious disturbance to the foreign relations or the peaceful coexistence of nations. Without being able to determine unilaterally the content of those concepts, each Member State has a certain discretion to define its essential interests in terms of security. See, in particular, judgment of 2 May 2018, *K. and H. F. (Right of residence and allegations of war crimes)* (C-331/16 and C-366/16, EU:C:2018:296, paragraphs 40 to 42 and the case-law cited). Those considerations can in my view be transposed to the interpretation of the concept of 'national security' as an interest protection of which may justify restrictions of the provisions of the GDPR and of the rights guaranteed in Articles 7 and 8 of the Charter.

166 See, in that regard, recital 89 and footnote 97 of the 'privacy shield' decision.

167 See point 55 of this Opinion.

168 See point 61 of this Opinion.

169 In the judgment in *Centrüm för Rättvisa* (§ 111), the ECtHR held that surveillance activities aimed at supporting Sweden's foreign, defence and security policy and identifying external threats organised in Sweden pursued legitimate aims in the interest of national security.

170 See, on that subject, judgment in *Tele2 Sverige* (paragraph 115) and judgment in *Ministerio Fiscal* (paragraph 55), where the Court emphasised the link between the degree of seriousness of the interference and the degree of the interest relied on in order to justify it.

287. However, it is still necessary, in accordance with Article 52(1) of the Charter, that national security or another legitimate objective is genuinely pursued by the measures providing for the interferences at issue.[171] Furthermore, the purposes of the interferences must be defined in a fashion that meets the requirements of clarity and precision.[172]

288. However, according to Mr Schrems, the purpose of the surveillance measures provided for in section 702 of the FISA and EO 12333 is not set out with sufficient precision to comply with the guarantees of foreseeability and proportionality. That is so, in particular, in so far as those instruments define the concept of 'foreign intelligence information' in particularly broad terms. In addition, the Commission stated in recital 109 of the 'privacy shield' decision that section 702 of the FISA requires that the collection of foreign intelligence information be a 'significant purpose' of the collection of information, a form of words that does not, prima facie and as the EPIC observes, preclude the pursuit of other undefined objectives.

289. For those reasons, without its being precluded that the surveillance measures based on section 702 of the FISA or EO 12333 meet legitimate objectives, it may be asked whether those measures are defined sufficiently clearly and precisely to prevent the risk of abuse and to permit a review of the proportionality of the ensuing measures.[173]

(5) The necessity and the proportionality of the interferences

290. The Court has repeatedly emphasised that 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 and weighed up against other fundamental rights, in accordance with the principle of proportionality.[174] As Facebook Ireland has submitted, those other rights include the right to security guaranteed in Article 6 of the Charter.

291. In that regard, according to an equally consistent body of case-law, any interference with the exercise of the rights guaranteed in Articles 7 and 8 of the Charter must be subject to a strict review of proportionality.[175]

292. In particular, it follows from the judgment in *Schrems* that 'legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the … data … without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail'.[176]

171 The WP29, in its Working Document on surveillance of electronic communications for intelligence and national security purposes of 5 December 2014 (p. 27), underlined the importance of critically assessing whether surveillance is actually conducted for the purpose of national security.

172 See Opinion 1/15 (paragraph 181), where the Court held that the wording of the legislative provisions envisaging the interferences did not meet the requirements as to clarity and precision and that the interferences were therefore not limited to what was strictly necessary. In the same vein, Advocate General Bot considered, in his Opinion in *Schrems* (C-362/14, EU:C:2015:627, points 181 to 184), that the aims of the surveillance measures were formulated in too general terms to be regarded as objectives of general interest, except with respect to national security.

173 Similar doubts were expressed by the European Data Protection Supervisor in Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision of 30 May 2016 (p. 8).

174 See judgment of 9 November 2010, *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 48); Opinion 1/15 (paragraph 136); and judgment of 24 September 2019, *Google (Territorial scope of dereferencing)* (C-507/17, EU:C:2019:772, paragraph 60).

175 See, in particular, judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia* (C-73/07, EU:C:2008:727, paragraph 56); judgment in *Digital Rights Ireland* (paragraphs 48 and 52); judgment in *Schrems* (paragraphs 78 and 92); and Opinion 1/15 (paragraphs 139 and 140). See also recital 140 of the 'privacy shield' decision.

176 Judgment in *Schrems* (paragraph 93). See also, to that effect, judgment in *Digital Rights Ireland* (paragraph 60).

293. The Court has also held that, except in cases of validly established urgency, access must be subject to a prior review carried out either by a court or by an independent administrative body whose decision is designed to limit access to and use of data to what is strictly necessary in order to attain the objective pursued.[177]

294. Article 23(2) of the GDPR now establishes a series of safeguards that a Member State must offer when it derogates from the provisions of that regulation. The legislation permitting such a derogation must contain provisions relating, in particular, to the purposes of the processing, the scope of the derogation from the safeguards designed to prevent abuse, the storage periods and the right of data subjects to be informed about the derogation, unless that may be prejudicial to the purpose of the derogation.

295. In the present case, Mr Schrems maintains that section 702 of the FISA is not accompanied by sufficient safeguards against the risks of abuse and of unlawful access to the data. In particular, the choice of selection criteria is not sufficiently circumscribed, so that that provision does not offer safeguards against generalised access to the content of the communications.

296. The United States Government and the Commission claim, on the other hand, that section 702 of the FISA limits by objective criteria the choice of selectors since it permits only the collection of the electronic communications data of non-United States persons located outside the United States for the purpose of obtaining foreign intelligence information.

297. To my mind, it is permissible to doubt the sufficiently clear and precise nature of those criteria and the existence of sufficient guarantees to prevent the risks of abuse.

298. First of all, recital 109 of the 'privacy shield' decision states that the selectors are not individually approved by the FISC or by any other judicial or independent administrative body before being applied. The Commission states in that recital that 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs … on the basis of annual certifications', which the United States Government confirmed before the Court. Recital 109 states that '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' that can be collected. The Commission also states in that recital that 'the FISC does not assess — under a probable cause or any other standard — that individuals are properly targeted to acquire foreign intelligence information', although it controls the condition that 'a significant purpose of the acquisition is to obtain foreign intelligence information'.

299. Next, in the words of that recital, section 702 of the FISA allows the NSA to collect communications 'only if it can be reasonably believed that a given means of communication is being used to communicate foreign intelligence information'. Recital 70 of the 'privacy shield' decision adds that the choice of selectors takes place within the National Intelligence Priorities Framework (NIPF). That decision does not mention more precise requirements to state reasons or to provide justification for the choice of selectors in the light of those administrative priorities imposed on the NSA.[178]

177 See judgment in *Tele2 Sverige* (paragraph 120) and Opinion 1/15 (paragraph 202).

178 The PCLOB report (p. 45) states in that respect: 'With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to "identify" the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorised by the Section 702 certification'.

300. Last, recital 71 of the 'privacy shield' decision refers to the requirement, laid down in PPD 28, that foreign intelligence collection must always be 'as tailored as feasible'. Apart from the fact that PPD 28 does not create any rights for individuals, the essential equivalence between the criteria of an activity 'as tailored as feasible' and the criterion of 'strict necessity' which Article 52(1) of the Charter prescribes for the purpose of justifying an interference with the exercise of the rights guaranteed in Articles 7 and 8 of the Charter seems to me to be far from obvious. [179]

301. In the light of those considerations, it is not certain that, on the basis of the elements set out in the 'privacy shield' decision, the surveillance measures based on section 702 of the FISA are accompanied by safeguards, relating to the limitation of persons who might be subject to a surveillance measure and of the objectives for the purpose of which data may be collected, that are essentially equivalent to those required under the GDPR, read in the light of Articles 7 and 8 of the Charter. [180]

302. Furthermore, as regards the evaluation of the adequacy of the level of protection applicable to surveillance on the basis of EO 12333, the ECtHR recognises that the Member States have a broad margin of appreciation when choosing the means to protect their national security, although that margin is limited by the requirement to provide adequate and sufficient safeguards against abuse. [181] In its case-law relating to secret measures of surveillance, the ECtHR ascertains whether the domestic law on which those measures are based contains guarantees and sufficient and effective safeguards capable of meeting the requirements of 'foreseeability' and 'necessity in a democratic society'. [182]

303. The ECtHR sets out, in that respect, a number of minimum safeguards. Those safeguards relate to a clear indication of the nature of the offences which may give rise to an interception order; a definition of the categories of people whose communications are likely to be intercepted; a limit on the duration of the implementation of the measure; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed. [183]

304. The adequacy and effectiveness of the safeguards applicable to the interference depend on all the circumstances of the case, including the nature, scope and duration of the measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. [184]

179 See, to that effect, WP29, Opinion 1/2016 of 13 April 2016 on the EU-U.S. Privacy Shield draft adequacy decision WP 238 (point 3.3.1, p. 38); Resolution of the Parliament of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2017)0131 (paragraph 17); Report of the Parliament of 20 February 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement A8-0044/2017 (paragraph 17).

180 See, to that effect, WP29, EU-U.S. Privacy Shield — First Annual Joint Review, 28 November 2017, WP 255 (p. 3); European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2018)0315 (paragraph 22); and EDPB, EU-U.S. Privacy Shield — Second Annual Joint Review, 22 January 2019 (paragraphs 81 to 83 and paragraph 87).

181 See in particular judgment in *Zakharov* (§ 232) and judgment in *Szabó and Vissy* (§ 57).

182 See in particular judgments in *Zakharov* (§ 237), *Centrüm för Rättvisa* (§ 111) and *Big Brother Watch* (§ 322).

183 See, in particular, decision in *Weber and Saravia* (§ 95); ECtHR, 28 June 2007, *Association for European integration and human rights and Ekimdzhiev* (CE:ECHR:2007:0628JUD006254000, § 76), and judgment in *Zakharov* (§ 231).

184 See, in particular, decision in *Weber and Saravia* (§ 106); judgment in *Zakharov* (§ 232); and judgment in *Centrüm för Rättvisa* (§ 104).

305. In particular, for the purposes of evaluating the justification for a secret measure of surveillance, the ECtHR takes account of the controls carried out 'when the surveillance is ordered', 'while it is being carried out' and 'after it has been terminated'.[185] As regards the first of these three stages, the ECtHR requires that such a measure be authorised by an independent body. Although in its view the judiciary represents the best guarantees of independence, impartiality and a properly conducted procedure, the body in question need not necessarily belong to the judiciary.[186] Extensive *post factum* judicial oversight may counterbalance the shortcomings in the authorisation procedure.[187]

306. In the present case, it follows from the 'privacy shield' decision that the only safeguards that limit the collection and use of data outside the territory of the United States are set out in PPD 28, as section 702 of the FISA does not apply outside the United States. I am not convinced that those safeguards can suffice to meet the conditions of 'foreseeability' and 'necessity in a democratic society'.

307. First of all, I have already pointed out that PPD 28 does not create rights for individuals. Next, I doubt that the requirement to guarantee surveillance 'as tailored as feasible' is formulated in sufficiently clear and precise terms to forewarn the data subjects adequately against the risks of abuse.[188] Last, the 'privacy shield' decision does not establish that the surveillance based on EO 12333 would be subject to prior review by an independent body or might be the subject of *post factum* judicial review.[189]

308. In those circumstances, I have doubts about the validity of the finding that the United States guarantees, in the context of the activities of their intelligence services on the basis of section 702 of the FISA and EO 12333, an adequate level of protection within the meaning of Article 45(1) of the GDPR, read in the light of Articles 7 and 8 of the Charter and of Article 8 of the ECHR.

(c) The validity of the 'privacy shield' decision by reference to the exercise of the right to an effective remedy

309. The fifth question invites the Court to determine whether persons whose data are transferred to the United States enjoy judicial protection there that is essentially equivalent to the protection that must be guaranteed in the Union under Article 47 of the Charter. By its tenth question, the referring court asks the Court, in essence, whether the fifth question must be answered in the affirmative as a result of the introduction by the 'privacy shield' decision of the Ombudsperson Mechanism.

310. I note at the outset that, in recital 115 of that decision, the Commission recognises that the United States legal system contains a number of deficiencies in the judicial protection of individuals.

311. In the words of that recital, first, 'at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered' by the possibilities of judicial redress. EO 12333 and PPD 28 do not confer rights on those concerned and cannot be relied upon by them before the courts. Effective judicial protection assumes, at least, that individuals have rights that may be relied on in judicial proceedings.

185 See, in particular, judgment of 6 September 1978, ECtHR, *Klass and others v. Germany* (CE:ECHR:1978:0906JUD000502971, § 55); judgment in *Zakharov* (§ 233); and judgment in *Centrüm för Rättvisa* (§ 105).

186 See, in particular, judgment in *Klass* (§ 56); ECtHR, 18 May 2010, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, § 167); and judgment in *Zakharov* (§§ 233 and 258).

187 See judgments in *Szabó and Vissy* (§ 77) and in *Centrüm för Rättvisa* (§ 133).

188 That is a fortiori the case in the light of the considerations set out in point 281 of this Opinion.

189 See points 330 and 331 of this Opinion.

312. Second, 'even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under the FISA, the available causes of action are limited and claims brought by individuals … will be declared inadmissible where they cannot show "standing", which restricts access to ordinary courts.'

313. It can be seen from recitals 116 to 124 of the 'privacy shield' decision that the establishment of the Ombudsperson is intended to compensate for those limitations. The Commission concludes, in recital 139 of that decision, that '*taken as a whole*, the *oversight and recourse* mechanisms provided for by the Privacy Shield … offer legal remedies to the data subject to gain access to personal data relating to him and, eventually, to obtain the rectification or erasure of such data' (emphasis added).

314. While recalling the general principles established in the case-law of this Court and of the ECtHR concerning the right to a remedy against communications surveillance measures, I shall examine whether the judicial remedies provided for in United States law, as described in the 'privacy shield' decision, can ensure adequate judicial protection of the persons concerned (section 1). I shall then determine whether the establishment of the extrajudicial mediation mechanism makes it possible, where appropriate, to compensate for any deficiencies in the judicial protection of those persons (section 2).

(1) The effectiveness of the judicial remedies provided for by United States law

315. *In the first place*, the first paragraph of Article 47 of the Charter establishes the right of everyone whose rights and freedoms guaranteed by the law of the Union are violated to an effective remedy before a tribunal.[190] According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.[191] The Court has held that access to an independent tribunal is of the essence of the right guaranteed by Article 47 of the Charter.[192]

316. That right to individual judicial protection is in addition to the obligation placed on Member States by Articles 7 and 8 of the Charter, to make any surveillance measure, except in the case of duly justified urgency, subject to prior review by a tribunal or an independent administrative authority.[193]

317. Admittedly, as the German and French Governments have asserted, the right to an effective judicial remedy is not an absolute guarantee,[194] as that right may be limited on national security grounds. However, derogations are permitted only in so far as they do not compromise the essence of the right and are strictly necessary in order to attain a legitimate objective.

190 The explanations relating to the Charter state, in that regard, that 'in Union law the protection [afforded by Article 47 of the Charter] is more extensive [than that afforded by Article 13 of the ECHR] since it guarantees the right to an effective remedy before a court'. See also Opinion of Advocate General Wathelet in *Berlioz Investment Fund* (C-682/15, EU:C:2017:2, point 37).

191 In order to assess whether a body is a 'court' for the purposes of the application of Article 47 of the Charter, it is necessary to consider whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is inter partes, whether it applies rules of law and whether it is independent. See judgment of 27 February 2018, *Associação Sindical dos Juízes Portugueses* (C-64/16, EU:C:2018:117, paragraph 38 and the case-law cited).

192 See, inter alia, judgments of 25 July 2018, *Minister for Justice and Equality (Deficiencies in the judicial system)* (C-216/18 PPU, EU:C:2018:586, paragraphs 59 and 63); of 5 November 2019, *Commission* v *Poland (Independence of the ordinary courts)* (C-192/18, EU:C:2019:924, paragraph 106), and of 19 November 2019, *A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)* (C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 120).

193 See point 293 of this Opinion. Article 45(3)(a) of the GDPR provides that, when assessing the adequacy of the level of protection afforded by a third State, it is necessary to take account of effective 'administrative *and judicial*' redress for the data subjects (emphasis added). Likewise, in the words of recital 104 of the GDPR, the adoption of an adequacy decision should be subject to the condition that the data subjects are provided, in the third country concerned, with 'effective administrative *and judicial* redress' (emphasis added). See also WP29, EU-U.S. Privacy Shield — First Annual Joint Review, 28 November 2017, WP 255 (paragraph B.3); European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, P8_TA(2018)0315 (paragraphs 25 and 30); and EDPB, EU-U.S. Privacy Shield — Second Annual Joint Review, 22 January 2019 (paragraphs 94 to 97).

194 See, to that effect, judgment of 28 February 2013, *Review Arango Jaramillo and Others* v *EIB* (C-334/12 RX-II, EU:C:2013:134, paragraph 43).

318. In that regard, the Court has held, in the judgment in *Schrems*, that legislation that *does not provide for any possibility* for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right enshrined in Article 47 of the Charter.[195]

319. It must be emphasised that that right of access entails the possibility for a person to obtain from the public authorities, subject to the derogations that are strictly necessary in order to pursue a legitimate interest, *confirmation of whether they are or are not processing data of a personal nature relating to him*.[196] That, in my view is the practical scope of the right of access when the person concerned is unaware whether the public authorities have retained personal data relating to him following, inter alia, an automated filtering process of electronic communications flows.

320. Furthermore, it follows from the case-law that the authorities of a Member State are required, in principle, to notify access to the data *as soon as that notification is no longer liable to jeopardise the investigations undertaken*.[197] Such notification constitutes a prerequisite to the exercise of the right to a remedy under Article 47 of the Charter.[198] That obligation is now set out in Article 23(2)(h) of the GDPR.

321. Recitals 111 to 135 of the 'privacy shield' decision provide a succinct account of all of the remedies available to persons whose data are transferred when they fear that those data have been processed by the United States intelligence services after being transferred. Those remedies were also described in the judgment of the High Court of 3 October 2017 and in the observations of, among others, the United States Government.

322. There is no need to recount in detail the content of those accounts. The referring court calls into question the adequacy of the safeguards relating to the legal protection of the persons concerned on the ground, essentially, that the particularly strict requirements with respect to 'standing',[199] in conjunction with the absence of any obligation to notify the persons who have been subject to a surveillance measure *even when notification would no longer jeopardise the objectives*, would in practice make the exercise of the remedies provided for in United States law excessively difficult. Those doubts are shared by the DPC, Mr Schrems, the Austrian, Polish and Portuguese Governments and the EDPB.[200]

195 Judgment in *Schrems* (paragraph 95).

196 Article 15 of the GDPR, entitled 'Right of access by the data subject', provides in paragraph 1 that the latter 'shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the … data'. The principle relating to access provided for in Annex II, paragraph II 8(a), to the 'privacy shield' decision has the same meaning.

197 Judgment in *Tele2 Sverige* (paragraph 121), and Opinion 1/15 (paragraph 220). As Facebook Ireland has observed, notification of access by the public authorities to the data cannot be systematically required. In that respect, the ECtHR considers that 'it may not be feasible in practice to require subsequent notification', since the threat against which the surveillance measures is directed 'may continue for years, even decades', after suspension of those measures, so that notification may 'jeopardise the long-term purpose that originally prompted the surveillance' and 'might serve to reveal the working methods and fields of operation of the intelligence services and … to identify their agents' (judgment in *Zakharov* (§ 287 and the case-law cited)). In the absence of notification, although individual remedies may therefore be impracticable in the event of breach of the legal requirements, other safeguards may suffice to protect the right to respect for private life (see also judgment in *Centrüm för Rättvisa*, §§ 164 to 167 and 171 to 178). See point 330 of this Opinion.

198 See, in that regard, footnote 210 of this Opinion

199 See point 67 of this Opinion.

200 See EDPB, EU-U.S. Privacy Shield — Second Annual Joint Review, 22 January 2019 (p. 18, paragraph 97).

323. I shall confine myself, on that subject, to pointing out that the rules on standing cannot undermine effective judicial protection,[201] and to stating that the 'privacy shield' decision does not mention any requirement to inform the data subjects that they were the subject of a surveillance measure.[202] Since it would be likely to prevent the exercise of judicial remedies, the absence of any obligation to notify such a measure, even when informing the data subject of the measure in question would no longer jeopardise its effectiveness, seems to be problematic in the light of the case-law referred to in point 320 of this Opinion.

324. Footnote 169 of the 'privacy shield' decision recognises, moreover, that the available causes of action 'either require the existence of damage … or a showing that the government intends to use or disclose information obtained … from electronic surveillance'. As the referring court, the DPC and Mr Schrems have maintained, that requirement contrasts with the Court's case-law in which it has held that, for the purpose of establishing the existence of an interference with the right to respect for private life of the person concerned, it is not necessary for that person to have been inconvenienced in any way as a result of the alleged interference.[203]

325. Furthermore, the viewpoint expressed by Facebook Ireland and the United States Government, according to which the weaknesses characterising the judicial protection of the persons whose data are transferred to the United States would be made good by the prior and subsequent reviews carried out by the FISC and also by the multiple surveillance mechanisms established within the executive and the legislature,[204] fails to convince me.

326. In that regard, first, I have already observed that, in accordance with the findings made in the 'privacy shield' decision, the FISC does not review individual surveillance measures before they are implemented.[205] As stated in recital 109 of that decision, and as the United States Government has confirmed in its written answer to the questions put by the Court, the purpose of the *ex post* review of the application of the selectors is, second, to verify, when an incident relating to the possible failure to comply with the targeting and minimisation procedures is brought to the attention of the FISC by an intelligence agency,[206] compliance with the conditions governing the choice of selectors laid down in the annual certification. The procedure before the FISC therefore does not appear to offer an effective individual remedy to persons whose data are transferred to the United States.

327. While the extrajudicial control mechanisms referred to in recitals 95 to 110 of the 'privacy shield' decision might, in appropriate circumstances, reinforce any judicial remedies, they cannot in my view suffice to ensure an adequate level of protection as regards the right to a remedy of the persons concerned. In particular, the inspector-generals, belonging to the internal structure of each agency, are not, in my view, independent control mechanisms. The surveillance carried out by the PCLOB and by the intelligence committees of the United States Congress is not equivalent to a mechanism of individual remedy against surveillance measures.

201 See, in particular, judgments of 11 July 1991, *Verholen and Others* (C-87/90 to C-89/90, EU:C:1991:314, paragraph 24 and the case-law cited), and of 28 February 2013, *Review Arango Jaramillo and Others* v *BEI* (C-334/12 RX-II, EU:C:2013:134, paragraph 43).

202 The United States Government has made clear, however, as has the referring court, that a surveillance measure based on section 702 of the FISA must be notified to the targeted person if the data collected are used against him in judicial proceedings.

203 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 75); judgment in *Digital Rights Ireland* (paragraph 33); judgment in *Schrems* (paragraph 87); and Opinion 1/15 (paragraph 124).

204 These mechanisms are described in recitals 95 to 110 of the 'privacy shield' decision, where the Commission distinguishes, within the category of rules relating to 'effective legal protection', oversight mechanisms (see recitals 92 to 110) from individual redress (see recitals 111 to 124).

205 See point 298 of this Opinion.

206 In the words of recital 109 of the 'privacy shield' decision, 'the Attorney General and the Director of [the NSA] verify compliance and the agencies have the obligation to report [all] incidents of non-compliance to the FISC …, which on this basis can modify the authorisation'.

328. It will therefore be necessary to examine whether the establishment of the Ombudsperson compensates for those deficiencies by providing the persons concerned with an effective remedy before an independent and impartial body. [207]

329. *In the second place*, for the purposes of evaluating the merits of the finding of adequacy made in the 'privacy shield' decision by reference to the remedies available to persons who think that they have been the subject of surveillance based on EO 12333, the relevant reference framework is to be found, it will be recalled, in the provisions of the ECHR.

330. As explained above, [208] in order to examine whether a surveillance measure meets the conditions of 'foreseeability' and 'necessity in a democratic society' within the meaning of Article 8(2) of the ECHR, [209] the ECtHR undertakes a global examination of the control and oversight mechanisms implemented 'before, during or after' its implementation. Where the exercise of an individual measure is prevented because notification of the surveillance is not possible without compromising its effectiveness, [210] that deficiency may be counterbalanced by the implementation of an independent control carried out before the measure at issue is applied. [211] Thus, although the ECtHR considers that such notification is 'desirable' when it may be given without altering the effectiveness of the surveillance measure, it has not made it a requirement. [212]

331. In that regard, the 'privacy shield' decision does not reveal that the surveillance measures based on EO 12333 would be notified to the individuals concerned or accompanied by judicial or independent administrative control mechanisms at any stage of their adoption or implementation.

332. In those circumstances, it is appropriate to examine whether recourse to the Ombudsperson nonetheless makes it possible to ensure independent control of the surveillance measures, including when they are based on EO 12333.

(2) The impact of the Ombudsperson Mechanism on the level of protection of the right to an effective remedy

333. In the words of recital 116 of the 'privacy shield' decision, the Ombudsperson Mechanism described in Annex III A to that decision is intended to provide an additional redress avenue accessible for all persons whose data are transferred from the Union to the United States.

334. As the United States Government has emphasised, the admissibility of a complaint lodged with the Ombudsperson is not subject to compliance with rules on standing comparable to those governing access to the United States courts. Recital 119 to that decision states, in that regard, that recourse to the Ombudsperson does not assume that the person concerned demonstrates that the United States Government has consulted personal data relating to him.

207 See points 333 to 340 of this Opinion.

208 See point 305 of this Opinion.

209 In its case-law on telecommunications surveillance measures, the ECtHR has addressed the question of remedies in the context of the examination of the 'quality of law' and the need for an interference with the exercise of the right guaranteed in Article 8 of the ECHR (see in particular judgments in *Zakharov* (§ 236) and in *Centrüm för Rättvisa* (§ 107)). In the judgment of 1 July 2008, *Liberty and others v. United Kingdom* (CE:ECHR:2008:0701JUD005824300, § 73), and the judgment in *Zakharov* (§ 307), the ECtHR, after finding that there had been a violation of Article 8 of the ECHR, did not consider it necessary to examine separately the complaint based on Article 13 of that Convention.

210 According to the ECtHR, although the failure to notify at any stage does not necessarily prevent a surveillance measure from meeting the condition that it be 'necessary in a democratic society', it undermines access to the courts and thus the effectiveness of the remedies (see, in particular, judgment of 6 September 1978, *Klass and others v. Germany* (CE:ECHR:1978:0906JUD000502971, §§ 57 and 58); decision in *Weber and Saravia* (§ 135); and judgment in *Zakharov* (§ 302)].

211 See, to that effect, judgment in *Centrum för Rättvisa* (§ 105).

212 In the judgment in *Big Brother Watch* (§ 317), the ECtHR refused to add, among the minimum guarantees applicable to a surveillance regime characterised by the bulk interception of electronic communications, a requirement that the surveillance be notified to the persons concerned. See, also, judgment in *Centrüm för Rättvisa* (§ 164). The referral of those judgments to the Grand Chamber of the ECtHR relates, inter alia, to the reconsideration of that conclusion.

335. Like the DPC, Mr Schrems, the Polish and Portuguese Governments and the EPIC, I doubt the ability of that mechanism to compensate for the insufficiencies of the judicial protection afforded to persons whose data are transferred from the Union to the United States.

336. First of all, although an extrajudicial remedy mechanism may constitute an effective remedy for the purposes of Article 47 TFEU, that is so only in so far as, in particular, the body in question was established by law and satisfies the condition of independence. [213]

337. However, it is apparent from the 'privacy shield' decision that the Ombudsperson Mechanism, which has its source in PPD 28, [214] is not established by law. The Ombudsperson is designated by the Secretary of State and is an integral part of the United States State Department. [215] There is nothing in that decision to indicate that the revocation of the Ombudsperson or the cancellation of his appointment would be accompanied by any particular guarantees. [216] Although the Ombudsperson is presented as being independent of the 'intelligence community', he reports to the Secretary of State and is therefore not independent of the executive. [217]

338. Next, the effectiveness of an extrajudicial remedy also depends, in my view, on the ability of the body in question to adopt binding reasoned decisions. On that subject, the 'privacy shield' decision gives no indication that the Ombudsperson would take such decisions. It does not show that the establishment of the Ombudsperson would allow applicants to have access to the data relating to them and to have such data rectified or erased, or that the Ombudsperson would award compensation to persons harmed by a surveillance measure. In particular, as is clear from Annex III A, point 4(e) to that decision, 'the … Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance, nor will [he] confirm the specific remedy that was applied'. [218] Although the United States Government has given a commitment that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Ombudsperson, [219] the 'privacy shield' decision does not mention any legal safeguards that would accompany that political commitment and on which the individuals concerned could rely.

213 The concept of independence has a first aspect, which is external and presumes that the body concerned is protected against external intervention or pressure liable to jeopardise the independent judgment of its members as regards proceedings before them. The second aspect of that concept, which is internal, is linked to impartiality and seeks to ensure a level playing field for the parties to the proceedings and their respective interests with regard to the subject matter of those proceedings. See, in particular, judgments of 19 September 2006, *Wilson* (C-506/04, EU:C:2006:587, paragraphs 50 to 52); of 25 July 2018, *Minister for Justice and Equality (Deficiencies in the judicial system)* (C-216/18 PPU, EU:C:2018:586, paragraphs 63 and 65), and of 19 November 2019, *A. K. and Others* (*Independence of the Disciplinary Chamber of the Supreme Court*) (C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraphs 121 and 122). In accordance with the principle of separation of powers, the independence of the courts must be guaranteed in relation to, inter alia, the executive. See judgment of 19 November 2019, *A. K. and Others* (*Independence of the Disciplinary Chamber of the Supreme Court*) (C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraph 127 and the case-law cited).

214 Annex III A to the 'privacy shield' decision refers, in that regard, to section 4(d) of PPD 28.

215 See recital 116 of the 'privacy shield' decision.

216 In the judgment of 31 May 2005, *Syfait and Others* (C-53/03, EU:C:2005:333, paragraph 31), the Court emphasised the importance of such safeguards in order to satisfy the condition of independence. See, also, in that respect, judgments of 24 June 2019, *Commission* v *Poland* (Independence of the Supreme Court) (C-619/18, EU:C:2019:531, paragraph 76) and of 5 November 2019, *Commission* v *Poland (Independence of the ordinary courts)* (C-192/18, EU:C:2019:924, paragraph 113).

217 See recitals 65 and 121 and Annex III A, paragraph 1, to the 'privacy shield' decision.

218 In addition, recital 121 of the 'privacy shield' decision states that 'the Ombudsperson will have to "confirm" that (i) the complaint has been properly investigated and that (ii) relevant U.S. law — including in particular the limitations and safeguards set out in Annex VI — has been complied with or, in the event of non-compliance, such violation has been remedied'.

219 The Commission stated, in the context of the third annual review of the privacy shield, that, according to the U.S. Government, in a situation in which the Ombudsperson's investigation revealed a violation of the targeting and minimisation procedures approved by the FISC, that violation would be reported to the FISC, which would then carry out an independent review and, if necessary, order the intelligence agency concerned to take remedial action. See Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23 October 2019, SWD(2019) 390 final, p. 28. The Commission refers in that document to the document entitled 'Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure', available at https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (pp. 4 and 5).

339. Consequently, the establishment of the Ombudsperson does not to my mind provide a remedy before an independent body offering the persons whose data are transferred a possibility of relying on their right of access to the data or of contesting any infringements of the applicable rules by the intelligence services.

340. Last, in accordance with the case-law, respect for the right guaranteed by Article 47 of the Charter thus assumes that a decision of an administrative authority that does not itself satisfy the condition of independence must be subject to subsequent control by a judicial body with jurisdiction to consider all the relevant issues.[220] However, according to the indications provided in the 'privacy shield' decision, the decisions of the Ombudsperson are not the subject of independent judicial review.

341. In those circumstances, as the DPC, Mr Schrems, the EPIC and the Polish and Portuguese Governments have maintained, the essential equivalence between the judicial protection afforded in the United States legal order to persons whose data are transferred to the United States from the Union and that which follows from the GDPR read in the light of Article 47 of the Charter and of Article 8 of the ECHR seems to me to be open to question.

342. In the light of all of the foregoing considerations, I entertain certain doubts as to the conformity of the 'privacy shield' decision to Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter and of Article 8 of the ECHR.

V. Conclusion

343. I propose that the Court answer the questions for a preliminary ruling referred by the High Court, Ireland, as follows:

Analysis of the questions for a preliminary ruling has disclosed nothing to affect the 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/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016.

220 See judgments of 16 May 2017, *Berlioz Investment Fund* (C-682/15, EU:C:2017:373, paragraph 55) and of 13 December 2017, *El Hassani* (C-403/16, EU:C:2017:960, paragraph 39).