Court of Justice EU, 6 October 2015, Schrems v Data Protection Commissioner

PERSONAL DATA

Existence of a decision adopted by the Commission that a third country ensures an adequate level of protection does not prevent a supervisory authority of a Member State from examination.

- **Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

Decision of Commission that the USA ensures an adequate level of protection of transferred personal data (Safe Harbour) is invalid.

Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in **Digital Rights Ireland and Others, C‑293/12 and C‑594/12, EU:C:2014:238**, paragraph 33 and the case-law cited).

88. In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89. Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

Source: **curia.europa.eu**

Court of Justice EU, 6 October 2015

(V. Skouris, K. Lenaerts, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (rapporteur), S. Rodin, K. Jürimäe, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen, C. Lycourgos)

JUDGMENT OF THE COURT (Grand Chamber)

6 October 2015 (*)

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

In Case C‑362/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximillian Schrems

v

Data Protection Commissioner,

joined party:

Digital Rights Ireland Ltd,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,

Advocate General: Y. Bot,

Registrar: L. Hewlett, Principal Administrator,

having regard to the written procedure and further to the hearing on 24 March 2015,
after considering the observations submitted on behalf of:
– Mr Schrems, by N. Travers, Senior Counsel, P. O'Shea, Barrister-at-Law, G. Rudden, Solicitor, and H. Hofmann, Rechtsanwalt,
– the Data Protection Commissioner, by P. McDermott, Barrister-at-Law, S. More O'Ferrall and D. Young, Solicitors,
– Digital Rights Ireland Ltd, by F. Crehan, Barrister-at-Law, and S. McGarr and E. McGarr, Solicitors,
– Ireland, by A. Joyce, B. Counihan and E. Creedon, acting as Agents, and D. Fennelly, Barrister-at-Law,
– the Belgian Government, by J.-C. Halleux and C. Pochet, acting as Agents,
– the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,
– the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,
– the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,
– the Polish Government, by M. Kamejsza, M. Pawlicka and B. Majczyna, acting as Agents,
– the Slovenian Government, by A. Grum and V. Klemenc, acting as Agents,
– the United Kingdom Government, by L. Christie and J. Beeko, acting as Agents, and J. Holmes, Barrister,
– the European Parliament, by D. Moore, A. Caiola and M. Pencheva, acting as Agents,
– the European Commission, by B. Schima, B. Martenczuk, B. Smulders and J. Vondung, acting as Agents,
– the European Data Protection Supervisor (EDPS), by C. Docksey, A. Buchta and V. Pérez Asinari, acting as Agents,
after hearing the **Opinion of the Advocate General** at the sitting on 23 September 2015,
gives the following

Judgment

1. This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (*'the Charter'*), of Articles 25(6) and 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), 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'*), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

2. The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner (*'the Commissioner'*) concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd (*'Facebook Ireland'*) transfers the personal data of its users to the United States of America and keeps it on servers located in that country.

Legal context

Directive 95/46

3. Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:

'(2) ... data-processing systems are designed to serve man; ... they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to ... the well-being of individuals;

...

(10) ... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; ..., for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

...

(56) ... cross-border flows of personal data are necessary to the expansion of international trade; ... the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; ... the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) ... on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

...

(60) ... in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

...

(62) ... the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) ... such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...'

4. Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:

'Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
...
Article 2
Definitions
For the purposes of this Directive:
(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
...
(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
...
Article 25
Principles
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.
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.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
Member States shall take the measures necessary to comply with the Commission's decision.
Article 26
Derogations
1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that 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) may take place on condition that:
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
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.

3. The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).
Member States shall take the necessary measures to comply with the Commission's decision.
...
Article 28
Supervisory authority
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.
These authorities shall act with complete independence in exercising the functions entrusted to them.
2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.
3. Each authority shall in particular be endowed with:
– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
– the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.
Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.
...
6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
...
Article 31
...
2. Where reference is made to this Article, Articles 4 and 7 of [Council] Decision 1999/468/EC [of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23)] shall apply, having regard to the provisions of Article 8 thereof.
...'

Decision 2000/520

5. Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.
6. Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:
'(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.
...
(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.
...
(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.'
7. Articles 1 to 4 of Decision 2000/520 provide:
'Article 1
1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbour Privacy Principles" (hereinafter "the Principles"), as set out in Annex I to this Decision, implemented in accordance

with the guidance provided by the frequently asked questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:
(a) the safe harbour enforcement overview set out in Annex III;
(b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;
(c) a letter from the Federal Trade Commission set out in Annex V;
(d) a letter from the US Department of Transportation set out in Annex VI.
2. In relation to each transfer of data the following conditions shall be met:
(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and
(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.
3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).
Article 2
This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.
Article 3
1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:
(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or
(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.
The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.
2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.
3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.
4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.
Article 4
1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.
The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.
2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.'

8 Annex I to Decision 2000/520 is worded as follows:

'Safe Harbour Privacy Principles

issued by the US Department of Commerce on 21 July 2000
... the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. ...
Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ...
Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible.
...'
9. Annex II to Decision 2000/520 reads as follows:
'Frequently Asked Questions (FAQs)
...
FAQ 6 — Self-Certification
Q: How does an organisation self-certify that it adheres to the Safe Harbour Principles?
A: Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.
To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:
1. name of organisation, mailing address, e-mail address, telephone and fax numbers;
2. description of the activities of the organisation with respect to personal information received from the [European Union]; and
3. description of the organisation's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) ..., and (g) the independent recourse mechanism that is available to investigate unresolved complaints.
Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles.
...
The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...
...
FAQ 11 — Dispute Resolution and Enforcement
Q: How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation's persistent failure to comply with the Principles be handled?
A: The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are

additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.
Recourse Mechanisms
Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...
...
FTC Action
The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ...
...'

10. Annex IV to Decision 2000/520 states:

'Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law
This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorisations" in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.
...
B. Explicit Legal Authorisations
The safe harbour principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation". Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side.
The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation". By way of illustration, where the law simply authorises a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorisation" to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients' medical records to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a "stand alone" authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information.
...'

Communication COM(2013) 846 final

11. On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled *'Rebuilding Trust in EU-US Data Flows'* (COM(2013) 846 final) (*'Communication COM(2013) 846 final'*). The communication was accompanied by the *'Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection'*, also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.

12. In point 1 of Communication COM(2013) 846 final, the Commission stated that *'[c]ommercial exchanges are addressed by Decision [2000/520]'*, adding that *'[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles'*. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed *'led to exponential growth in the quantity, quality, diversity and nature of data processing activities'*.

13. In point 2 of that communication, the Commission observed that *'concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown'* and that *'[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement'*.
14. It further stated in point 2 that *'[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]'* and that *'[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme'*.
15. In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 (*'the safe harbour principles'*) and that improvements had to be made to that decision regarding *'structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception'*. It observed, secondly, that *'Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes'*.
16. The Commission concluded in point 3.2 that whilst, *'[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]'*. Finally, the Commission added in that point that it would *'engage with the US authorities to discuss the shortcomings identified'*.

Communication COM(2013) 847 final

17. On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) (*'Communication COM(2013) 847 final'*). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.
18. Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 *'relies on commitments and self-certification of adhering companies'*, adding that *'[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up'*.
19. In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3 246 companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.
20. The Commission stated in point 2.2 that *'[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme'*.
21. It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.
22. In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that *'all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified'* and that *'[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'*. In that regard, the Commission noted in point 7.1 of that communication that *'a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]'* and that *'[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]'*.
23. In point 7.2 of Communication COM(2013) 847 final, headed *'Limitations and redress possibilities'*, the Commission noted that *'safeguards that are provided under US law are mostly available to US citizens or legal residents'* and that, *'[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes'*.
24. According to point 8 of Communication COM(2013) 847 final, the certified companies included *'[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo'*, which had *'hundreds of millions of clients in Europe'* and transferred personal data to the United States for processing.

25. The Commission concluded in point 8 that *'the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]'*.

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

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

27. Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

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

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

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

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

32. The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

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

34. However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in **Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238)**. The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

35. The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has

not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

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

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

Consideration of the questions referred

37. By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection. The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive

38. It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in **Österreichischer Rundfunk and Others, C‑465/00, C‑138/01 and C‑139/01, EU:C:2003:294, paragraph 68**; **Google Spain and Google, C‑131/12, EU:C:2014:317, paragraph 68**; and **Ryneš, C‑212/13, EU:C:2014:2428, paragraph 29**).

39. It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in **Rijkeboer, C‑553/07, EU:C:2009:293, paragraph 47**; **Digital Rights Ireland and Others, C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 53**; and **Google Spain and Google, C‑131/12, EU:C:2014:317**, paragraphs, 53, 66, 74 and the case-law cited).

40. As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in Commission v Austria, C‑614/10, EU:C:2012:631, paragraph 36, and Commission v Hungary, C‑288/12, EU:C:2014:237, paragraph 47).

41. The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in Commission v Germany, C‑518/07, EU:C:2010:125, paragraph 25, and Commission v Hungary, C‑288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

42. In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in Commission v Germany, C‑

518/07, EU:C:2010:125, paragraph 24, and Commission v Hungary, C‑288/12, EU:C:2014:237, paragraph 51).

43. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

44. It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.

45. However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in Parliament v Council and Commission, C‑317/04 and C‑318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines *'processing of personal data'* as *'any operation or set of operations which is performed upon personal data, whether or not by automatic means'* and mentions, by way of example, *'disclosure by transmission, dissemination or otherwise making available'*.

46. Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in **Lindqvist, C‑101/01, EU:C:2003:596, paragraph 63**).

47. As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

48. Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.

49. Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.

50. In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in **point 86 of his Opinion**, be made either by the Member States or by the Commission.

51. The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in Albako Margarinefabrik, 249/85, EU:C:1987:245, paragraph 17, and Mediaset, C‑69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

52. Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in Commission v Greece, C‑475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

53. However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in **points 61**, **93** and **116 of his Opinion**, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

54. Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.
55. In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear *'claims lodged by any person ... concerning the protection of his rights and freedoms in regard to the processing of personal data'*, does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.
56. Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.
57. On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.
58. If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in **Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68**).
59. A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.
60. In this connection, the Court's settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in Commission and Others v Kadi, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66; Inuit Tapiriit Kanatami and Others v Parliament and Council, C-583/11 P, EU:C:2013:625, paragraph 91; and Telefónica v Commission, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.
61. That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in Melki and Abdeli, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and CIVAD, C-533/10, EU:C:2012:347, paragraph 40).
62. Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in Foto-Frost, 314/85, EU:C:1987:452, paragraphs 15 to 20, and IATA and ELFAA, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.
63. Having regard to those considerations, 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, as in the main proceedings, 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.
64. In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to

the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in T & L Sugars and Sidul Açúcares v Commission, C‑456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

65. In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data 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.

66. Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The validity of Decision 2000/520

67. As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in **points 123 and 124 of his Opinion**, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

The requirements stemming from Article 25(6) of Directive 95/46

68. As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

69. However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission *'may find ... 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 ..., for the protection of the private lives and basic freedoms and rights of individuals'*.

70. It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that 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'* and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71. However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country *'ensures'* an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed *'for the protection of the private lives and basic freedoms and rights of individuals'*.

72. Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in **point 139 of his Opinion**, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

73. The word *'adequate'* in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in **point 141 of his Opinion**, the term *'adequate level of protection'* must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

74. It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must

ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

75. Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76. Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

77. Moreover, as the Advocate General has stated in **points 134 and 135 of his Opinion**, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

78. In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in **Digital Rights Ireland and Others, C‑293/12 and C‑594/12, EU:C:2014:238, paragraphs 47 and 48**).

Article 1 of Decision 2000/520

79. The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

80. An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

81. Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection *'by reason of its domestic law or ... international commitments'*, the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

82. In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are *'intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'*. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

83. Moreover, Decision 2000/520, pursuant to Article 2 thereof, *'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]'*, without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

84. In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, *'to the extent necessary to meet national security, public interest, or law enforcement requirements'* and *'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'*.

85. In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, *'[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'*.

86. Thus, Decision 2000/520 lays down that *'national security, public interest, or law enforcement requirements'* have primacy over the safe harbour

principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (**judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33** and the case-law cited).

88. In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89. Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in **points 204 to 206 of his Opinion**, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

90. Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91. As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in **Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55** and the case-law cited).

92. Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in **Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52** and the case-law cited).

93. Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council 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), judgment in **Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61**).

94. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment **in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39**).

95. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or

to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in Les Verts v Parliament, 294/83, EU:C:1986:166, paragraph 23; Johnston, 222/84, EU:C:1986:206, paragraphs 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, paragraph 14; and UGT-Rioja and Others, C‑428/06 to C‑434/06, EU:C:2008:488, paragraph 80).

96. As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

97. However, the Commission did not state, in Decision 2000/520, that the United States in fact *'ensures'* an adequate level of protection by reason of its domestic law or its international commitments.

98. Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

Article 3 of Decision 2000/520

99. It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.

100. However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

101. Under that provision, the national supervisory authorities may, *'[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]'*, under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

102. The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

103. The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

104. That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.

105. As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.

106. Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

Costs

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

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

1. Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC

of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.
2. Decision 2000/520 is invalid.
[Signatures]
* Language of the case: English.

OPINION OF ADVOCATE GENERAL BOT
delivered on 23 September 2015 (1)
Case C‑362/14
Maximillian Schrems
v
Data Protection Commissioner
(Request for a preliminary ruling from the High Court (Ireland))
(Reference for a preliminary ruling — Personal data — Protection of individuals with respect to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Article 25 — Decision 2000/520/EC — Transfer of personal data to the United States — Assessment of whether or not the level of protection is adequate — Complaint by an individual whose data has been transferred to a third country — National supervisory authority — Powers)

I – Introduction

1. As the European Commission stated in its Communication of 27 November 2013, (2) *'[t]ransfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the [European Union] to the [United States]'*. (3)
2. Such commerce forms the subject-matter of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. (4) That decision provides a legal basis for the transfer of personal data from the European Union to undertakings established in the United States that adhere to the safe harbour principles.
3. Decision 2000/520 today faces the challenge of allowing data flows between the European Union and the United States while ensuring a high level of protection for that data, as required by EU law.
4. A number of revelations have recently brought to light the existence of large-scale information-gathering programmes in the United States. Those revelations have given rise to serious concerns as to whether the requirements of EU law are observed when personal data is transferred to undertakings established in the United States and about the weaknesses of the safe harbour scheme.
5. The present reference for a preliminary ruling invites the Court to make clear the approach that the national supervisory authorities and the Commission must take when they are faced with shortcomings in the application of Decision 2000/520.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (5) lays down in Chapter IV rules on the transfer of personal data to third countries.
7. In that chapter, the principle stated in Article 25(1) is that the transfer to a third country of personal data which is undergoing processing or is intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection of such data.
8. Conversely, as the EU legislature indicates in recital 57 of that directive, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.
9. As provided in Article 25(2) of Directive 95/46, *'[t]he 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'*.
10. Under Article 25(6) of that directive, the Commission may find that a third country ensures an adequate level of protection of personal data by reason of its domestic law or of the international commitments it has entered into. If the Commission adopts a decision to that effect, the transfer of personal data to the third country concerned may take place.
11. The Commission adopted Decision 2000/520 pursuant to that provision. It follows from Article 1(1) of Decision 2000/520 that the *'Safe Harbour Privacy Principles'*, implemented in accordance with the guidance provided by the frequently asked questions, (6) are considered to ensure an adequate level of protection for personal data transferred from the European Union to undertakings established in the United States.
12. Consequently, Decision 2000/520 authorises the transfer of personal data from the Member States to

undertakings established in the United States which have undertaken to comply with the safe harbour principles.

13. Decision 2000/520 sets out, in Annex I, a number of principles to which undertakings may subscribe voluntarily, together with limits and a specific monitoring system. The number of undertakings which have subscribed to what might be described as a *'code of conduct'* exceeded 3 200 in 2013.

14. The safe harbour scheme is based on a solution combining self-certification and self-assessment by private organisations and intervention by the public authorities.

15. The safe harbour principles were developed *'in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'*. (7)

16. The safe harbour principles, set out in Annex I to Decision 2000/520, establish, in particular:

– an obligation to provide information, under which *'[a]n organisation must inform individuals about the purposes for which it collects and uses information about them, how to contact the organisation with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organisation offers individuals for limiting its use and disclosure. This notice must be provided ... when individuals are first asked to provide personal information to the organisation or as soon thereafter as is practicable, but in any event before the organisation uses such information for a purpose other than that for which it was originally collected or processed by the transferring organisation or discloses it for the first time to a third party'*; (8)

– an obligation on the organisations to offer individuals the opportunity to choose whether their personal information is to be disclosed to a third party or to be used for a purpose that is incompatible with the purpose or purposes for which it was originally collected or subsequently authorised by the individual. As regards sensitive information, an individual *'must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorised by the individual through the exercise of opt in choice'*; (9)

– rules on the onward transfer of data. Thus, *'to disclose information to a third party, organisations must apply the Notice and Choice Principles'*; (10)

– as regards data security, an obligation on *'[o]rganisations creating, maintaining, using or disseminating personal information [to] take reasonable precautions to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction'*; (11)

– as regards data integrity, an obligation on organisations to *'take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current'*; (12)

– that a person whose personal information is held by an organisation must, in principle, *'have access to [that] information ... and be able to correct, amend, or delete [it] where it is inaccurate'*; (13)

– an obligation to make provision for *'mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organisation when the Principles are not followed'*. (14)

17. A United States organisation wishing to adhere to the safe harbour principles is required to state in its privacy policy that it discloses the fact that it adheres to those principles and in fact complies with them and to self-certify by declaring to the United States Department of Commerce that it complies with those principles. (15)

18. Organisations have a number of ways of complying with the safe harbour principles. Thus, they may, for example, *'[join] a self-regulatory privacy programme that adheres to the Principles [o]r qualify by developing their own self-regulatory privacy policies provided that they conform with the Principles. ... In addition, organisations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbour benefits'*. (16)

19. A number of mechanisms, combining private dispute resolution and oversight by the public authorities, exist to check compliance with the safe harbour principles. Scrutiny may thus be ensured through a system of out-of-court dispute resolution by an independent third party. Furthermore, undertakings may undertake to cooperate with the EU data protection panel. Last, the Federal Trade Commission (*'the FTC'*), on the basis of the powers conferred on it pursuant to section 5 of the Federal Trade Commission Act, and the Department of Transportation, on the basis of the powers conferred on it pursuant to section 41712 of the United States Code in Title 49 of that code, are empowered to deal with complaints.

20. According to the fourth paragraph of Annex I to Decision 2000/520, adherence to the safe harbour principles may be limited, in particular, *'to the extent necessary to meet national security, public interest, or law enforcement requirements'* and *'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'*. (17)

21. In addition, the possibility for the competent authorities of the Member States to suspend data flows is subject to a number of conditions laid down in Article 3(1) of Decision 2000/520.

22. The present request for a preliminary ruling raises the issue of the effect of Decision 2000/520 in the light

of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (*'the Charter'*) and of Article 25(6) of Directive 95/46. The request has been submitted in proceedings between Mr Schrems and the Data Protection Commissioner (*'the Commissioner'*) concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd (*'Facebook Ireland'*) keeps its subscribers' personal data on servers located in the United States.

23. Mr Schrems is an Austrian national residing in Austria. He has been a subscriber to the social network Facebook since 2008.

24. All Facebook subscribers residing in the European Union are asked to sign a contract with Facebook Ireland, a subsidiary of the parent company Facebook Inc. established in the United States (*'Facebook USA'*). Some or all of the data of subscribers to Facebook Ireland residing in the European Union is transferred to Facebook USA's servers in the United States, where it is kept.

25. Mr Schrems lodged a complaint with the Commissioner on 25 June 2013, claiming, in essence, that the law and practices of the United States offer no real protection of the data kept in the United States against State surveillance. That was said to follow from the revelations made by Edward Snowden from May 2013 concerning the activities of the United States intelligence services, in particular those of the National Security Agency (*'the NSA'*).

26. According to those revelations, the NSA established a programme called *'PRISM'* under which it obtained unrestricted access to mass data stored on servers in the United States owned or controlled by a range of companies active in the internet and technology field, such as Facebook USA.

27. The Commissioner considered that he was not required to investigate the complaint, since it was unsustainable in law. He considered that there was no evidence that the NSA accessed Mr Schrems' data. Furthermore, the complaint, in his view, had to be rejected by reason of Decision 2000/520, whereby the Commission found that under the safe harbour scheme the United States ensured an adequate level of protection of the personal data transferred. Any question relating to the adequacy of the protection of that data in the United States had to be settled in accordance with that decision which prevented him from examining the problem raised by the complaint.

28. The national legislation that led the Commissioner to reject the complaint is the following.

29. Section 10(1) of the Data Protection Act 1988, as amended by the Data Protection (Amendment) Act 2003 (*'the Data Protection Act'*), empowers the Commissioner to examine complaints, stating:

'(a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.

(b) Where a complaint is made to the Commissioner under paragraph (a) of this subsection, the Commissioner shall—

(i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and

(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.'

30. In this instance, the Commissioner concluded that Mr Schrems' complaint was *'frivolous or vexatious'*, in the sense that it was bound to fail because it was unsustainable in law. It was on that basis that the Commissioner refused to investigate the complaint.

31. Section 11 of the Data Protection Act governs the transfer of personal data outside national territory. Section 11(2)(a) provides:

'Where in any proceedings under this Act a question arises—

(i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area [(EEA)] to which personal data are to be transferred, and

(ii) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.'

32. Section 11(2)(b) of the Data Protection Act defines *'Community finding'* as follows:

'[I]n paragraph (a) of this subsection "Community finding" means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of [Directive 95/46] under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the [EEA].'

33. The Commissioner observed that Decision 2000/520 was a *'Community finding'* for the purposes of section 11(2)(a) of the Data Protection Act so that, under that Act, any question relating to the adequacy of data protection in the third country to which the data was transferred had to be settled in accordance with that finding. As this was the gist of Mr Schrems' complaint — namely that personal data was being transferred to a third country which did not in practice ensure an adequate level of protection — the Commissioner took the view that the nature and very existence of Decision 2000/520 prevented him from examining this question.

34. Mr Schrems brought proceedings before the High Court for judicial review of the Commissioner's decision rejecting his complaint. After examining the

evidence adduced in the main proceedings, the High Court found that the electronic surveillance and interception of personal data serve necessary and indispensable objectives in the public interest, namely the preservation of national security and the prevention of serious crime. The High Court states, in that regard, that the surveillance and interception of personal data transferred from the European Union to the United States serve legitimate counter-terrorism objectives.

35. Nevertheless, according to the High Court, the revelations made by Edward Snowden demonstrated a significant over-reach on the part of the NSA and other similar agencies. While the Foreign Intelligence Surveillance Court (*'the FISC'*), which operates under the Foreign Intelligence Surveillance Act of 1978, (18) exercises supervisory jurisdiction, proceedings before that court take place in secret and are ex parte. In addition, apart from the fact that decisions relating to access to personal data are taken on the basis of United States law, citizens of the Union have no effective right to be heard on the question of the surveillance and interception of their data.

36. According to the High Court, it is clear from the extensive exhibits accompanying the affidavits filed in the main proceedings that the accuracy of much of Edward Snowden's revelations is not in dispute. The High Court therefore concluded that, once personal data is transferred to the United States, the NSA and other United States security agencies such as the Federal Bureau of Investigation (FBI) are able to access it in the course of a mass and indiscriminate surveillance and interception of such data.

37. The High Court notes that in Irish law the importance of the constitutional rights to privacy and to inviolability of the dwelling requires that any interference with those rights be in accordance with the law and proportionate. The mass and undifferentiated accessing of personal data does not satisfy the requirement of proportionality and must therefore be considered contrary to the Constitution of Ireland. (19)

38. The High Court observes that, in order for interception of electronic communications to be regarded as constitutional, it must be shown that specific interceptions of communications and the surveillance of individuals or groups of individuals are objectively justified in the interests of national security and the suppression of crime and that there are appropriate and verifiable safeguards.

39. Accordingly, the High Court states that, if the present case were to be approached solely on the basis of Irish law, a significant issue would arise as to whether the United States *'ensures an adequate level of protection for the privacy and the fundamental rights and freedoms'* of data subjects, within the meaning of section 11(1)(a) of the Data Protection Act. It follows that, on the basis of Irish law, and in particular of its constitutional requirements, the Commissioner could not have rejected Mr Schrems' complaint, but would have been required to examine that issue.

40. However, the High Court finds that the case before it concerns the implementation of EU law as referred to in Article 51(1) of the Charter and that the legality of the Commissioner's decision should therefore be assessed in the light of EU law.

41. The problem facing the Commissioner is explained by the High Court as follows. Under section 11(2)(a) of the Data Protection Act, the Commissioner is required to determine the question of the adequacy of protection in the third country *'in accordance'* with a Community finding made by the Commission pursuant to Article 25(6) of Directive 95/46. It follows that the Commissioner cannot depart from such a finding. As the Commission found in Decision 2000/520 that the United States provides an adequate level of protection in respect of data processing by companies which adhere to the safe harbour principles, a complaint alleging the inadequacy of such protection must necessarily be rejected by the Commissioner.

42. While finding that the Commissioner thus demonstrated scrupulous steadfastness to the letter of Directive 95/46 and Decision 2000/520, the High Court observes that Mr Schrems' objection is in reality to the terms of the safe harbour scheme itself rather than to the manner in which the Commissioner applied it, while emphasising that Mr Schrems has not directly challenged the validity of Directive 95/46 or that of Decision 2000/520.

43. According to the High Court, the essential question is therefore whether, in the light of EU law and having regard, in particular, to the subsequent entry into force of Articles 7 and 8 of the Charter, the Commissioner is absolutely bound by the finding of the Commission made in Decision 2000/520 relating to the adequacy of the law and practice applicable to personal data protection in the United States.

44. The High Court further observes that in the proceedings before it no issue has been raised concerning the actions of Facebook Ireland and Facebook USA as such. Article 3(1)(b) of Decision 2000/520, which allows the competent national authorities to direct an undertaking to suspend data flows to a third country, applies, according to the High Court, only in circumstances where the complaint is directed against the conduct of the undertaking concerned, which is not the position in the present case.

45. The High Court emphasises, accordingly, that the real objection is not to the conduct of Facebook USA as such, but rather to the fact that the Commission has determined that the law and practice on data protection in the United States ensure adequate protection when it is clear from Edward Snowden's disclosures that the United States authorities can have access on a mass and undifferentiated basis to personal data of the population living in the territory of the European Union. (20)

46. In that regard, the High Court considers that it is difficult to see how Decision 2000/520 could in practice satisfy the requirements of Articles 7 and 8 of the Charter, especially if regard is had to the principles articulated by the Court in its judgment in Digital Rights Ireland and Others. (21) In particular, the guarantee enshrined in Article 7 of the Charter and by the core values common to the traditions of the

Member States would be compromised if the public authorities were allowed access to electronic communications on a casual and generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individuals concerned and attended by appropriate and verifiable safeguards. According to the High Court, since Mr Schrems' action suggests that Decision 2000/520 could be incompatible in abstracto with Articles 7 and 8 of the Charter, the Court of Justice may consider that Directive 95/46, in particular Article 25(6) thereof, and Decision 2000/520 could be interpreted as allowing the national authorities to conduct their own investigations in order to ascertain whether the transfer of personal data to a third country satisfies the requirements of Articles 7 and 8 of the Charter.

47. It was in those circumstances that the High Court decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'Whether in the course of determining a complaint which has been made to [the Commissioner] that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, [the Commissioner] is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

Or, alternatively, may and/or must the [Commissioner] conduct his or her own investigation of the matter in the light of factual developments in the meantime since [Decision 2000/520] was first published?'

II – My analysis

48. The two questions formulated by the High Court invite the Court to clarify the powers available to the national supervisory authorities when they receive a complaint concerning a transfer of personal data to an undertaking established in a third country and it is claimed, in support of the complaint, that that third country does not guarantee an adequate level of protection of the data transferred, although the Commission, acting on the basis of Article 25(6) of Directive 95/46, has adopted a decision recognising the adequacy of the level of protection ensured by that third country.

49. I would observe that there are two aspects to the complaint that Mr Schrems filed with the Commissioner. It seeks to challenge the transfer of personal data from Facebook Ireland to Facebook USA. Mr Schrems asks that that transfer be brought to an end since, in his submission, the United States does not ensure an adequate level of protection of the personal data transferred under the safe harbour scheme. More specifically, he takes issue with the United States for having set up the PRISM programme, which allows the NSA unrestricted access to the mass data stored on servers located in the United States. Thus, the complaint relates specifically to transfers of personal data from Facebook Ireland to Facebook USA, while challenging more generally the level of protection ensured for such data under the safe harbour scheme.

50. The Commissioner considered that the very existence of a Commission decision recognising that the United States ensures an adequate level of protection under the safe harbour scheme prevented him from investigating the complaint.

51. It is therefore appropriate to examine together the two questions, which seek, in essence, to ascertain whether Article 28 of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the existence of a decision adopted by the Commission on the basis of Article 25(6) of that directive has the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data.

52. Article 7 of the Charter guarantees the right to respect for private life, while Article 8 expressly proclaims the right to the protection of personal data. Article 8(2) and (3) states that such data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified, and that compliance with those rules is to be subject to control by an independent authority.

A – The powers of the national supervisory authorities where the Commission has adopted an adequacy decision

53. As Mr Schrems states in his observations, for the purposes of the complaint at issue in the main proceedings the key issue is that of the transfer of personal data from Facebook Ireland to Facebook USA in the light of the generalised access which the NSA and other United States security agencies have under the powers conferred on them by United States legislation to the data stored at Facebook USA.

54. When the national supervisory authority receives a complaint challenging the finding that a third country ensures an adequate level of protection for the transferred data, it is empowered, according to Mr Schrems, if it has evidence that the allegations made in the complaint are well founded, to direct that the transfer of data by the undertaking designated in the complaint be suspended.

55. In the light of the Commissioner's obligations to protect Mr Schrems' fundamental rights, Mr Schrems maintains that the Commissioner is under an obligation not only to investigate, but also, if the complaint is upheld, to use his powers to suspend the data flows between Facebook Ireland and Facebook USA.

56. However, the Commissioner rejected the complaint on the basis of the provisions of the Data Protection Act which set out his powers. That conclusion was based on the Commissioner's view that he was bound by Decision 2000/520.

57. It follows that the central issue in the present case is whether the Commission's assessment as to the adequacy of the level of protection, contained in Decision 2000/520, is absolutely binding on the national data protection authority and prevents it from investigating allegations challenging that finding. The questions referred to the Court therefore relate to the extent of the investigative powers of the national data protection authorities where the Commission has adopted an adequacy decision.
58. According to the Commission, it is necessary to take account of the allocation of powers between it and the national data protection authorities. The powers of the national data protection authorities are focused on the application of the relevant legislation in individual cases, while the general review of the application of Decision 2000/520, including any decision involving its suspension or repeal, comes within the powers of the Commission.
59. The Commission maintains that Mr Schrems has not put forward any specific arguments that would indicate that he was at imminent risk of grave harm owing to the transfer of data between Facebook Ireland and Facebook USA. On the contrary, owing to their general and abstract nature, the concerns which he expresses about the surveillance programmes implemented by the United States security agencies are exactly the same as those that led the Commission to embark on the review of Decision 2000/520.
60. In the Commission's submission, the national supervisory authorities would encroach upon its power to renegotiate the terms of that decision with the United States or, if necessary, to suspend that decision if they were to take action on the basis of complaints raising only structural and abstract concerns.
61. I do not share the Commission's opinion. To my mind, the existence of a decision adopted by the Commission on the basis of Article 25(6) of Directive 95/46 cannot eliminate or even reduce the national supervisory authorities' powers under Article 28 of that directive. Contrary to the Commission's contention, if the national supervisory authorities receive individual complaints, that does not in my view prevent them, by virtue of their investigative powers and their independence, from forming their own opinion on the general level of protection ensured by a third country and from drawing the appropriate conclusion when they determine individual cases.
62. The Court has consistently held that, in interpreting provisions of EU law, it is necessary to consider not only their wording but also the context in which they occur and the objectives pursued by the rules of which they are part. (22)
63. It is apparent from recital 62 of Directive 95/46 that *'the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data'*.
64. As set out in the first subparagraph of Article 28(1) of Directive 95/46, *'[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive'*. The second subparagraph of Article 28(1) provides that *'[t]hese authorities shall act with complete independence in exercising the functions entrusted to them'*.
65. Article 28(3) of Directive 95/46 lists the powers of each supervisory authority, namely: investigative powers; effective powers of intervention, enabling that authority, in particular, to impose a temporary or definitive ban on processing; and the power to engage in legal proceedings where the national provisions adopted pursuant to that directive have been violated or to bring those violations to the attention of the judicial authorities.
66. Furthermore, under the first subparagraph of Article 28(4) of Directive 95/46, *'[e]ach supervisory authority shall hear claims lodged by any person ... concerning the protection of his rights and freedoms in regard to the processing of personal data'*. The second subparagraph of Article 28(4) states that *'[e]ach supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply'*. Article 13 enables Member States to adopt legislative measures to restrict the scope of a number of obligations and rights provided for in Directive 95/46 when such a restriction constitutes a necessary measure to safeguard, in particular, national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.
67. As the Court has already held, the requirement that compliance with EU rules on the protection of individuals with regard to the processing of personal data is subject to control by an independent authority derives also from the primary law of the European Union, in particular from Article 8(3) of the Charter and Article 16(2) TFEU. (23) It has also observed that *'[t]he establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data'*. (24)
68. The Court has also held that *'the second subparagraph of Article 28(1) of Directive 95/46 must be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes inter alia any directions or any other external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data'*. (25)
69. The Court has stated too that *'[t]he guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of*

the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data'. (26) That guarantee of independence was established *'in order to strengthen the protection of individuals and bodies affected by [the] decisions [of those national supervisory authorities]'*. (27)

70. As is apparent, in particular, from recital 10 and Article 1 of Directive 95/46, that directive seeks to ensure, in the European Union, *'a high level of protection of fundamental rights and freedoms with respect to the processing of personal data'*. (28) According to the Court, *'[t]he supervisory authorities provided for in Article 28 of Directive 95/46 are therefore the guardians of those fundamental rights and freedoms'*. (29)

71. In the light of the importance of the role played by the national supervisory authorities in the protection of individuals with regard to the processing of personal data, their powers of intervention must remain intact even when the Commission has adopted a decision on the basis of Article 25(6) of Directive 95/46.

72. I note, in this connection, that there is nothing to suggest that arrangements for the transfer of personal data to third countries are excluded from the substantive scope of Article 8(3) of the Charter, which enshrines at the highest level of the hierarchy of rules in EU law the importance of control by an independent authority of compliance with the rules on the protection of personal data.

73. If the national supervisory authorities were absolutely bound by decisions adopted by the Commission, that would inevitably limit their total independence. In accordance with their role as guardians of fundamental rights, the national supervisory authorities must be able to investigate, with complete independence, the complaints submitted to them, in the higher interest of the protection of individuals with regard to the processing of personal data.

74. In addition, as the Belgian Government and the European Parliament rightly observed at the hearing, there is no hierarchical connection between Chapter IV of Directive 95/46 on the transfer of personal data to third countries and Chapter VI of that directive which is devoted, in particular, to the role of the national supervisory authorities. There is nothing in Chapter VI to suggest that the provisions on the national supervisory authorities are in any way subordinate to the separate provisions on transfers set out in Chapter IV.

75. On the other hand, it is clearly stated in Article 25(1) of Directive 95/46, which is in Chapter IV, that the authorisation of the transfer of personal data to a third country ensuring an adequate level of protection is applicable only if the national provisions adopted pursuant to the other provisions of that directive are complied with.

76. Under that provision, the Member States are to lay down in their national legislation that the transfer to a third country of personal data which is undergoing processing or is 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 Directive 95/46, the third country in question ensures an adequate level of protection.

77. Under Article 28(1) of that directive, the national supervisory authorities are responsible for monitoring the application within the territory of each Member State of the provisions adopted by the Member States pursuant to the directive.

78. A comparison of those two provisions permits the view that the rule laid down in Article 25(1) of Directive 95/46 that the transfer of personal data may take place only if the third country to which it is sent ensures an adequate level of protection of that data is among the rules the application of which is to be monitored by the national supervisory authorities.

79. The powers of the national supervisory authorities to investigate, with complete independence, complaints submitted to them under Article 28 of Directive 95/46 must be interpreted broadly, in accordance with Article 8(3) of the Charter. Those powers cannot therefore be limited by the powers which the EU legislature has conferred on the Commission under Article 25(6) of that directive to find that the level of protection ensured by a third country is adequate.

80. In the light of the essential role which they play with regard to the protection of personal data, the national supervisory authorities must be able to investigate where they receive a complaint alleging matters that could call into question the level of protection ensured by a third country, including where the Commission has found, in a decision adopted on the basis of Article 25(6) of Directive 95/46, that the third country concerned ensures an adequate level of protection.

81. If, on completion of its investigations, a national supervisory authority considers that the contested transfer of data undermines the protection which citizens of the Union must enjoy with regard to the processing of their data, it has the power to suspend the transfer of data in question, irrespective of the general assessment made by the Commission in its decision.

82. It is undisputed, as set out in Article 25(2) of Directive 95/46, that the adequacy of the level of protection afforded by a third country is to be assessed in the light of a range of circumstances, both factual and legal. If one of those circumstances changes and appears to be such as to call into question the adequacy of the level of protection afforded by a third country, the national supervisory authority to which a complaint has been submitted must be able to draw the appropriate conclusions in relation to the contested transfer.

83. Admittedly, as Ireland has observed, the Commissioner, like the other State authorities, is bound by Decision 2000/520. Indeed, it follows from the fourth paragraph of Article 288 TFEU that a decision taken by an institution of the European Union is binding in its entirety. Consequently, Decision 2000/520 is binding on the Member States, to which it is addressed.

84. I would observe, in that regard, that Decision 2000/520 itself provides, in Article 5, that *'Member States shall take all the measures necessary to comply with this Decision at the end of a period of 90 days from the date of its notification to the Member States'*. In addition, Article 6 of Decision 2000/520 confirms that the decision *'is addressed to the Member States'*.
85. However, I consider that, in the light of the abovementioned provisions of Directive 95/46 and the Charter, the mandatory effect of Decision 2000/520 is not such as to preclude any investigation by the Commissioner of complaints alleging that transfers of personal data to the United States within the framework of that decision do not afford the necessary guarantees of protection that are required by EU law. In other words, such a binding effect cannot require that every complaint of that type be rejected summarily, that is to say, immediately and without any examination of its merits.
86. I should add that it is apparent, moreover, from the scheme of Article 25 of Directive 95/46 that the finding that a third country does or does not ensure an adequate level of protection may be made either by the Member States or by the Commission. The competence to make such a finding is therefore a shared competence.
87. It follows from Article 25(6) of that directive that, where the Commission finds that a third country ensures an adequate level of protection within the meaning of Article 25(2), the Member States are to take the necessary measures to comply with the Commission's decision.
88. As the effect of such a decision is to allow transfers of personal data to a third country whose level of protection is considered adequate by the Commission, the Member States must therefore, in principle, allow such transfers to be made by undertakings established on their territory.
89. However, Article 25 of Directive 95/46 does not attribute exclusive power to the Commission to find that the level of protection of the personal data transferred is adequate or inadequate. The scheme of that article shows that the Member States also have a role in that respect. A Commission decision does, admittedly, play an important role in ensuring uniformity in the transfer conditions applicable in the Member States. However, that uniformity can continue only while that finding is not called in question.
90. The argument that uniformity of the conditions for the transfer of personal data to a third country is necessary meets its limit, to my mind, in a situation such as that at issue in the main proceedings where not only is the Commission informed that its finding is the subject of criticism, but also the Commission itself makes such criticisms and enters into negotiations with a view to remedying the situation.
91. Assessment of whether or not the level of protection afforded by a third country is adequate may also give rise to cooperation between the Member States and the Commission. Article 25(3) of Directive 95/46 provides, in that regard, that *'[t]he Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2'*. As the Parliament observes, that clearly demonstrates that the Member States and the Commission have an equal role to play in identifying cases in which a third country does not ensure an adequate level of protection.
92. The purpose of an adequacy decision is to authorise the transfer of personal data to the third country concerned. That does not mean that citizens of the Union can no longer submit requests to the supervisory authorities aimed at protecting their personal data. I note, in that regard, that the first subparagraph of Article 28(4) of Directive 95/46, which provides that *'[e]ach supervisory authority shall hear claims lodged by any person ... concerning the protection of his rights and freedoms in regard to the processing of personal data'*, makes no provision for an exception to that principle where a decision has been adopted by the Commission under Article 25(6) of the directive.
93. Thus, although a decision adopted by the Commission under the implementing powers conferred on it by Article 25(6) of Directive 95/46 has the effect of allowing the transfer of personal data to a third country, such a decision cannot, on the other hand, have the effect of removing all power from the Member States, and in particular from their national supervisory authorities, or even of only restricting their powers, when they are faced with allegations of infringements of fundamental rights.
94. A national supervisory authority must be capable of exercising the powers provided for in Article 28(3) of Directive 95/46, including the power to impose a temporary or definitive ban on the processing of personal data. Although the list of powers set out in that provision does not expressly refer to powers relating to a transfer from a Member State to a third country, such a transfer must in my view be regarded as constituting the processing of data. (30) As is clear from the wording of that provision, the list, moreover, is not exhaustive. In any event, in the light of the essential role played by the national supervisory authorities in the system put in place by Directive 95/46, they must have the power to order the suspension of the transfer of data where there is a proven breach or a risk of a breach of fundamental rights.
95. I would add that to deprive the national supervisory authority of its investigative powers in circumstances such as those at issue in the present case would be contrary not only to the principle of independence but also to the objective of Directive 95/46 as resulting from Article 1(1) thereof.
96. As the Court has observed, *'[i]t is apparent from recitals 3, 8 and 10 of Directive 95/46 that the European Union legislature sought to facilitate the free movement of personal data by the approximation of the laws of the Member States while safeguarding the fundamental rights of individuals, in particular the right to privacy, and ensuring a high level of protection in the European Union. Article 1 of the directive thus*

requires the Member States to ensure the protection of the fundamental rights and freedoms of natural persons, in particular their privacy, with respect to the processing of personal data'. (31)

97. The provisions of Directive 95/46 must therefore be interpreted in accordance with its objective of guaranteeing a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data within the European Union.

98. The importance of that objective and the role which the Member States must play in attaining it mean that, when particular circumstances give rise to a serious doubt as to compliance with the fundamental rights guaranteed by the Charter where personal data is transferred to a third country, the Member States and therefore, within them, the national supervisory authorities cannot be absolutely bound by an adequacy decision adopted by the Commission.

99. The Court has already held that *'the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter'*. (32)

100. I would refer, moreover, to the case-law according to which *'the Member States must not only interpret their national law in a manner consistent with EU law but also make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the European Union legal order or with the other general principles of EU law'*. (33)

101. The Court thus held in its judgment in N.S. and Others (34) that *'an application of Regulation [EC] No 343/2000 [(35)] on the basis of the conclusive presumption that the asylum seeker's fundamental rights will be observed in the Member State primarily responsible for his application is incompatible with the duty of the Member States to interpret and apply Regulation No 343/2003 in a manner consistent with fundamental rights'*. (36)

102. In that regard, the Court accepted, in the context of the status of the Member States as safe countries of origin in respect to each other for all legal and practical purposes in relation to asylum matters, that it must be assumed that the treatment of asylum seekers in all Member States complies with the requirements of the Charter, the Convention relating to the Status of Refugees, signed in Geneva on 28 July 1951, (37) and the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950. (38) However, the Court held that *'[i]t is not ... inconceivable that that system may, in practice, experience major operational problems in a given Member State, meaning that there is a substantial risk that asylum seekers may, when transferred to that Member State, be treated in a manner incompatible with their fundamental rights'*. (39)

103. Consequently, the Court held that *'the Member States, including the national courts, may not transfer an asylum seeker to the "Member State responsible" within the meaning of Regulation No 343/2003 where they cannot be unaware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in that Member State amount to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of Article 4 of the Charter'*. (40)

104. To my mind, the contribution to the case-law made by the judgment in N.S. and Others (41) can be applied by extension to a situation such as that at issue in the main proceedings. Thus, an interpretation of secondary EU law based on an irrebuttable presumption that fundamental rights will be observed — whether by a Member State, by the Commission or by a third country — must be considered to be incompatible with the duty of the Member States to interpret and apply secondary EU law in a manner consistent with fundamental rights. Article 25(6) of Directive 95/46 therefore does not establish such an irrebuttable presumption that fundamental rights are observed as regards the Commission's assessment of the adequacy of the level of protection offered by a third country. On the contrary, the presumption underlying that provision — that the transfer of data to a third country complies with fundamental rights — must be regarded as rebuttable. (42) Consequently, that provision should not be interpreted as calling in question the guarantees laid down in, notably, Article 28(3) of Directive 95/46 and Article 8(3) of the Charter, relating to the protection of and compliance with the right to protection of personal data.

105. I therefore infer from that judgment that, where systemic deficiencies are found in the third country to which the personal data is transferred, the Member States must be able to take the measures necessary to safeguard the fundamental rights protected by Articles 7 and 8 of the Charter.

106. Furthermore, as the Italian Government stated in its observations, the fact that the Commission has adopted an adequacy decision cannot have the effect of reducing the protection of citizens of the Union with regard to the processing of their data when that data is transferred to a third country by comparison with the level of protection which those persons would enjoy if their data were processed within the European Union. The national supervisory authorities must therefore be in a position to intervene and to exercise their powers with respect to transfers of data to third countries covered by an adequacy decision. Were that not so, citizens of the Union would be less well protected than they would be if their data were processed within the European Union.

107. Thus, the adoption by the Commission of a decision under Article 25(6) of Directive 95/46 has the effect only of removing the general prohibition on

exporting personal data to third countries guaranteeing a level of protection comparable to that afforded by that directive. In other words, the point is not the creation of a special system of exceptions that offers less protection for citizens of the Union by comparison with the general system provided for in that directive for the processing of data within the European Union.

108. Admittedly, the Court has stated, in paragraph 63 of its judgment in Lindqvist, (43) that *'Chapter IV of Directive 95/46, in which Article 25 appears, sets up a special regime'*. However, that does not mean, in my view, that such a regime must afford less protection. On the contrary, in order to attain the objective of protecting data established in Article 1(1) of Directive 95/46, Article 25 of that directive imposes a series of obligations on the Member States and on the Commission (44) and it establishes the principle that where a third country does not ensure an adequate level of protection the transfer of personal data to that country must be prohibited. (45)

109. As regards more specifically the safe harbour scheme, the Commission envisages that the national supervisory authorities will intervene and suspend data flows only in the context outlined in Article 3(1)(b) of Decision 2000/520.

110. According to recital 8 of that decision, *'[i]n the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection'*.

111. In the context of the present case, it is, more specifically, the application of Article 3(1)(b) of Decision 2000/520 that has been discussed. Under that provision, the national supervisory authorities may decide to suspend data flows where *'there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable effects under the circumstances to provide the organisation with notice and an opportunity to respond'*.

112. That provision lays down a number of conditions which have been given various interpretations by the parties in the course of these proceedings. (46) Without going into detail on those interpretations, it is apparent from them that those conditions strictly circumscribe the national supervisory authorities' power to suspend data flows.

113. However, contrary to the Commission's submissions, Article 3(1)(b) of Decision 2000/520 must be interpreted in accordance with the objective of protecting personal data pursued by Directive 95/46, and also in the light of Article 8 of the Charter. The requirement that provisions be interpreted in a manner consistent with fundamental rights supports a broad interpretation of that provision.

114. It follows that the conditions laid down in Article 3(1)(b) of Decision 2000/520 cannot in my view prevent a national supervisory authority from exercising, in complete independence, the powers conferred on it by Article 28(3) of Directive 95/46.

115. As the Belgian and Austrian Governments submitted, in essence, at the hearing, the emergency exit that Article 3(1)(b) of Decision 2000/520 represents is so narrow that it is difficult to put into practice. It imposes cumulative criteria and sets the bar too high. In the light of Article 8(3) of the Charter, it is not possible for the national supervisory authorities' scope for manoeuvre in relation to the powers resulting from Article 28(3) of Directive 95/46 to be limited in such a way that they can no longer be exercised.

116. In that regard, the Parliament has correctly observed that it is the EU legislature that decided what powers were to devolve to the national supervisory authorities. The implementing power conferred by the EU legislature on the Commission in Article 25(6) of Directive 95/46 does not affect the powers which that legislature conferred on the national supervisory authorities in Article 28(3) of the directive. In other words, the Commission is not empowered to restrict the powers of the national supervisory authorities.

117. Consequently, in order to ensure appropriate protection of the fundamental rights of individuals with regard to the processing of personal data, the national supervisory authorities must have the power, where there are allegations regarding infringement of those rights, to conduct investigations. If, following such investigations, those authorities consider that, in a third country covered by an adequacy decision, there are strong indications of a breach of the right of citizens of the Union to the protection of their personal data, they must be able to suspend the transfer of data to the recipient established in that third country.

118. In other words, the national supervisory authorities must be able to carry out their investigations and, where appropriate, suspend the transfer of data, irrespective of the restrictive conditions laid down in Article 3(1)(b) of Decision 2000/520.

119. Furthermore, under their power provided for in Article 28(3) of Directive 95/46 to engage in legal proceedings where the national provisions adopted pursuant to that directive have been violated or to bring those violations to the attention of the judicial authorities, the national supervisory authorities should be able, where they are aware of facts showing that a third country does not ensure an adequate level of protection, to bring the matter before a national court, which will be able to decide, where appropriate, to request a preliminary ruling from the Court for the purpose of assessing the validity of a Commission adequacy decision.

120. It follows from all of the foregoing that Article 28 of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the

existence of a decision adopted by the Commission on the basis of Article 25(6) of that directive does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data.

121. Although the High Court stresses in its order for reference that Mr Schrems has not formally contested in the main proceedings either the validity of Directive 95/46 or the validity of Decision 2000/520, it is clear from that order for reference that Mr Schrems' main criticism seeks to challenge the finding that the United States ensures, under the safe harbour scheme, an adequate level of protection of the personal data transferred.

122. It is also apparent from the Commissioner's observations that Mr Schrems' complaint is intended to put Decision 2000/520 directly in issue. In filing that complaint, Mr Schrems wished to challenge the terms and the functioning of the safe harbour scheme itself on the ground that the mass surveillance of the personal data transferred to the United States shows that there is no meaningful protection of that data in the law and practice in force in that third country.

123. Furthermore, the referring court itself observes that the guarantee provided by Article 7 of the Charter and by the core values common to the constitutional traditions of the Member States would be compromised if the public authorities were allowed access to electronic communications on a casual and generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individuals concerned and attended by appropriate and verifiable safeguards. (47) The referring court thus indirectly casts doubts on the validity of Decision 2000/520.

124. The assessment of whether under the safe harbour scheme the United States guarantees an adequate level of protection of the personal data transferred therefore necessarily leads to consideration of the validity of that decision.

125. In that regard, it should be observed that in the context of the instrument of cooperation between the Court of Justice and national courts that is established by Article 267 TFEU, even where a request to the Court for a preliminary ruling relates solely to the interpretation of EU law the Court may, in certain specific circumstances, find it necessary to examine the validity of provisions of secondary law.

126. Accordingly, on a number of occasions, the Court has of its own motion declared invalid an act which it was asked only to interpret. (48) It has also held that, *'[i]f it appears that the real purpose of the questions submitted by a national court is concerned rather with the validity of [EU] measures than with their interpretation, it is appropriate for the Court to inform the national court at once of its view without compelling the national court to comply with purely formal requirements which would uselessly prolong the procedure under Article [267 TFEU] and would be contrary to its very nature'*. (49) The Court has already considered, moreover, that the doubts evinced by a referring court as to the compatibility of an act of secondary legislation with the rules concerning the protection of fundamental rights must be understood as questioning the validity of that act in the light of EU law. (50)

127. I would also observe that it follows from the case-law of the Court that the acts of the EU institutions, bodies, offices and agencies are presumed to be lawful, which means that they produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a request for a preliminary ruling or a plea of illegality. The Court alone has jurisdiction to declare an act of the European Union invalid and the purpose of that jurisdiction is to ensure legal certainty through the uniform application of EU law. In the absence of a declaration of invalidity, amendment or repeal by the Commission, the decision remains binding in its entirety and directly applicable in all Member States. (51)

128. In order to provide a full answer to the referring court and to dispel the doubts expressed during the present proceedings as to the validity of Decision 2000/520, I am of the view that the Court should therefore assess the validity of that decision.

129. That said, it should also be made clear that the examination of whether or not Decision 2000/520 is valid must be confined to the grounds of objection discussed in the context of the present proceedings. Not all aspects of the functioning of the safe harbour scheme have been discussed in that context, and for that reason I do not consider it possible to embark here on an exhaustive examination of the shortcomings of that scheme.

130. On the other hand, the question whether the United States intelligence services' generalised and untargeted access to the transferred data is capable of affecting the legality of Decision 2000/520 has been discussed before the Court in the context of the present proceedings. The validity of that decision can therefore be assessed from that point of view.

B – The validity of Decision 2000/520

1. The factors to be taken into consideration in assessing the validity of Decision 2000/520

131. It is appropriate to recall the case-law stating that, *'in the context of an application for annulment, the legality of a measure must be assessed on the basis of the facts and the law as they stood at the time when the measure was adopted, the Commission's assessment being open to criticism only if it appears manifestly incorrect in the light of the information available to it at the time when the measure in question was adopted'*. (52)

132. In its judgment in Gaz de France — Berliner Investissement, (53) the Court noted the principle that *'the assessment of the validity of a measure which the Court is called upon to undertake on a reference for a preliminary ruling must normally be based on the situation which existed at the time that measure was adopted'*. (54) However, the Court appears to have

recognised that *'the validity of a measure might, in certain cases, be assessed by reference to new factors which arose after its adoption'*. (55)

133. The more open approach thus outlined by the Court seems to me to be particularly relevant in the context of the present case.

134. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46 have particular characteristics. They are intended to assess whether or not the level of protection of personal data afforded by a third country is adequate. That assessment will necessarily evolve according to the factual and legal context prevailing in the third country.

135. In view of the fact that an adequacy decision is a particular type of decision, the rule that its validity might be assessed only by reference to the factors that existed at the time of its adoption must be qualified in this instance. Otherwise, such a rule would have the consequence that, a number of years after an adequacy decision has been adopted, the assessment of validity that the Court must carry out cannot take into account events that have occurred subsequently, even though there is no limit on the period within which a reference for a preliminary ruling on validity may be made and it may be prompted specifically by subsequent facts that reveal the deficiencies of the act in question.

136. In the present case, the fact that Decision 2000/520 has remained in force for around 15 years demonstrates the Commission's implicit confirmation of the assessment which it made in 2000. Where, in the context of a reference for a preliminary ruling, the Court is required to appraise the validity of an assessment which has been maintained over time by the Commission, it is therefore not only possible but also appropriate that it may compare that assessment with the new circumstances which have arisen since the adequacy decision was adopted.

137. Given the particular nature of an adequacy decision, it must be regularly reviewed by the Commission. If, following new events which have occurred in the meantime, the Commission does not amend its decision, that is because it confirms implicitly, but necessarily, the initial assessment. It thus reiterates its finding that the third country concerned ensures an adequate level of protection of the personal data transferred. It is for the Court to examine whether that finding continues to be valid in spite of the intervening circumstances.

138. In order to ensure effective judicial review of that type of decision, the assessment of its validity must therefore in my view be carried out by reference to the current factual and legal context.

2. The concept of an adequate level of protection

139. Article 25 of Directive 95/46 is based entirely on the principle that the transfer of personal data to a third country cannot take place unless that third country guarantees an adequate level of protection of such data. The objective of that article is thus to ensure the continuity of the protection afforded by that directive where personal data is transferred to a third country. It is appropriate, in that regard, to bear in mind that that directive affords a high level of protection of citizens of the Union with regard to the processing of their personal data.

140. In view of the important role played by the protection of personal data with regard to the fundamental right to privacy, this kind of high level of protection must, therefore, be guaranteed, including where personal data is transferred to a third country.

141. It is for that reason that I consider that the Commission can find, on the basis of Article 25(6) of Directive 95/46, that a third country ensures an adequate level of protection only where, following a global assessment of the law and practice in the third country in question, it is able to establish that that third country offers a level of protection that is essentially equivalent to that afforded by the directive, even though the manner in which that protection is implemented may differ from that generally encountered within the European Union.

142. Although the English word *'adequate'* may be understood, from a linguistic viewpoint, as designating a level of protection that is just satisfactory or sufficient, and thus as having a different semantic scope from the French word *'adéquat'* (*'appropriate'*), the only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights, as required by Directive 95/46.

143. Examination of the level of protection afforded by a third country must focus on two fundamental elements, namely the content of the applicable rules and the means of ensuring compliance with those rules. (56)

144. To my mind, in order to attain a level of protection essentially equivalent to that in force in the European Union, the safe harbour scheme, which is largely based on self-certification and self-assessment by the organisations participating voluntarily in that scheme, should be accompanied by adequate guarantees and a sufficient control mechanism. Thus, transfers of personal data to third countries should not be given a lower level of protection than processing within the European Union.

145. In that regard, I would observe at the outset that within the European Union the prevailing notion is that an external control mechanism in the form of an independent authority is a necessary component of any system designed to ensure compliance with the rules on the protection of personal data.

146. Furthermore, in order to ensure that Article 25(1) to (3) of Directive 95/46 is effective, account should be taken of the fact that the adequacy of the level of protection afforded by a third country involves a developing situation that may change with the passage of time, depending on a series of factors. The Member States and the Commission must therefore be constantly alert to any change of circumstances that may necessitate a reassessment of whether the level of protection afforded by a third country is adequate. An assessment of the adequacy of that level of protection cannot be fixed at a specific time and then be

maintained indefinitely, irrespective of any change in circumstances showing that in reality the level of protection afforded is no longer adequate.

147. The obligation for the third country to ensure an adequate level of protection is thus an ongoing obligation. While the assessment is made at a specific time, retention of the adequacy decision presupposes that no circumstance that has since arisen is such as to call into question the initial assessment made by the Commission.

148. Indeed, it must not be forgotten that the objective of Article 25 of Directive 95/46 is to prevent personal data from being transferred to a third country that does not ensure an adequate level of protection, in breach of the fundamental right to protection of personal data guaranteed by Article 8 of the Charter.

149. It must be emphasised that the power conferred on the Commission by the EU legislature in Article 25(6) of Directive 95/46 to find that a third country ensures an adequate level of protection is expressly conditional on the requirement that that third country ensures such a level of protection, within the meaning of Article 25(2). If new circumstances are such as to call the Commission's initial assessment into question, it should adapt its decision accordingly.

3. My assessment

150. It is to be remembered that, under Article 25(6) of Directive 95/46, *'[t]he 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'*. Read in conjunction with Article 25(2) of that directive, Article 25(6) means that, in order to find that a third country ensures an adequate level of protection, the Commission must undertake a global assessment of the rules of law in force in that third country and of their application.

151. We have seen that the fact that the Commission has maintained Decision 2000/520, in spite of changes in the factual and legal position, must be understood as willingness on its part to confirm its initial assessment.

152. It is not for the Court, in the context of a reference for a preliminary ruling, to assess the facts underlying the dispute that led the national court to make that reference. (57)

153. I shall therefore rely on the facts stated by the referring court in its request for a preliminary ruling, facts which, moreover, are largely accepted by the Commission itself as established. (58)

154. The matters put forward before the Court to challenge the Commission's assessment that the safe harbour scheme ensures an adequate level of protection of the personal data transferred from the European Union to the United States may be described as follows.

155. In its request for a preliminary ruling, the referring court proceeds on the basis of the following two findings of fact. First, personal data transferred by undertakings such as Facebook Ireland to their parent company established in the United States is then capable of being accessed by the NSA and by other United States security agencies in the course of a mass and indiscriminate surveillance and interception of such data. Indeed, in the wake of Edward Snowden's revelations, the evidence now available would admit of no other realistic conclusion. (59) Second, citizens of the Union have no effective right to be heard on the question of the surveillance and interception of their data by the NSA and other United States security agencies. (60)

156. The findings of fact thus made by the High Court are supported by the statements of the Commission itself.

157. Thus, in the Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, referred to above, the Commission proceeded on the basis of the finding that in the course of 2013 information on the scale and scope of United States surveillance programmes raised concerns over the continuity of protection of personal data lawfully transferred to the United States under the safe harbour scheme. It observed that all companies involved in the PRISM programme, which grant access to United States authorities to data stored and processed in the United States, appear to be certified under the safe harbour scheme. According to the Commission, this has made the safe harbour scheme one of the conduits through which access is given to United States intelligence authorities to the collecting of personal data initially processed in the European Union. (61)

158. It follows from these factors that the law and practice of the United States allow the large-scale collection of the personal data of citizens of the Union which is transferred under the safe harbour scheme, without those citizens benefiting from effective judicial protection.

159. Those findings of fact demonstrate, in my view, that Decision 2000/520 does not contain sufficient guarantees. Owing to that lack of guarantees, Decision 2000/520 has been implemented in a manner that does not satisfy the requirements of the Charter or of Directive 95/46.

160. The purpose of a decision adopted by the Commission on the basis of Article 25(6) of Directive 95/46 is to find that a third country *'ensures'* an adequate level of protection. The word *'ensures'*, conjugated in the present tense, implies that, in order to be able to be maintained, such a decision must relate to a third country which, after the adoption of that decision, continues to guarantee an adequate level of protection.

161. In reality, the revelations referred to concerning the activities of the NSA, to the effect that it uses the data transferred under the safe harbour scheme, have

shed light on the shortcomings of the legal basis represented by Decision 2000/520.

162. The insufficiencies highlighted in the course of the present proceedings are to be found, more specifically, in the fourth paragraph of Annex I to that decision.

163. Under that provision, *'[a]dherence to [the Safe Harbour] Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'*.

164. The problem arises essentially from the United States authorities' use of the derogations provided for in that provision. Because their wording is too general, the implementation of those derogations by the United States authorities is not limited to what is strictly necessary.

165. In addition to that too general wording is the fact that citizens of the Union have no appropriate remedy against the processing of their personal data for purposes other than those for which it was initially collected and then transferred to the United States.

166. The derogations laid down in Decision 2000/520 from the application of the safe harbour principles, in particular for requirements of national security, ought to have been accompanied by the putting in place of an independent control mechanism suitable for preventing the breaches of the right to privacy that have been found.

167. Thus, the revelations about the practices of the United States intelligence services as regards the generalised surveillance of data transferred under the safe harbour scheme have shed light on certain insufficiencies specific to Decision 2000/520.

168. The allegations relied on in the context of the present case do not amount to a breach by Facebook of the safe harbour principles. If a certified undertaking, such as Facebook USA, gives the United States authorities access to the data transferred to it from a Member State, it may be considered that it does so in order to comply with United States legislation. Since such a situation is expressly accepted by Decision 2000/520, owing to the broad wording of the derogations contained in that decision, it is in reality the question of the compatibility of such derogations with primary EU law that is raised in the present case.

169. It should be pointed out, in that regard, that the Court has consistently held that respect for human rights is a condition of the lawfulness of EU acts and that measures incompatible with respect for human rights are not acceptable in the European Union. (62)

170. It also follows from the case-law of the Court that the communication of the personal data collected to third parties, whether public or private, constitutes an interference with the right to respect for private life, *'whatever the subsequent use of the information thus communicated'*. (63) Furthermore, in its judgment in Digital Rights Ireland and Others, (64) the Court confirmed that authorising the competent national authorities to access such data constitutes a further interference with that fundamental right. (65) In addition, any form of processing of personal data is covered by Article 8 of the Charter and constitutes an interference with the right to the protection of such data. (66) The access enjoyed by the United States intelligence services to the transferred data therefore also constitutes an interference with the fundamental right to protection of personal data guaranteed in Article 8 of the Charter, since such access constitutes a processing of that data.

171. Similarly to the findings of the Court in that judgment, the interference thus identified is wide-ranging and must be considered to be particularly serious, given the large number of users concerned and the quantities of data transferred. Those factors, associated with the secret nature of the United States authorities' access to the personal data transferred to the undertakings established in the United States, make the interference extremely serious.

172. An additional factor is that the citizens of the Union who are Facebook users are not informed that their personal data will be generally accessible to the United States security agencies.

173. It should also be emphasised that the referring court found that in the United States citizens of the Union have no effective right to be heard on the question of the surveillance and interception of their data. There is oversight on the part of the FISC, but the proceedings before it are secret and ex parte. (67) I consider that that amounts to an interference with the right of citizens of the Union to an effective remedy, protected by Article 47 of the Charter.

174. The interference with the fundamental rights protected by Articles 7, 8 and 47 of the Charter which is permitted by the derogations from the safe harbour principles, set out in the fourth paragraph of Annex I to Decision 2000/520, is therefore made out.

175. It is now necessary to ascertain whether or not that interference is justified.

176. In accordance with Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law and must respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

177. In the light of the conditions thus laid down that must be satisfied in order for limitations on the exercise of the rights and freedoms protected by the Charter to be accepted, I find it extremely doubtful that the limitations at issue in the present case may be regarded as respecting the essence of Articles 7 and 8 of the Charter. The United States intelligence services' access to the data transferred seems to extend to the content of

the electronic communications, which would compromise the essence of the fundamental right to respect for privacy and the other rights enshrined in Article 7 of the Charter. Furthermore, since the broad wording of the limitations provided for in the fourth paragraph of Annex I to Decision 2000/520 potentially allows all the safe harbour principles to be disapplied, it could be considered that those limitations compromise the essence of the fundamental right to protection of personal data. (68)

178. As to whether the interference found meets an objective of general interest, I would recall first of all that, under point (b) in the fourth paragraph of Annex I to Decision 2000/520, adherence to the safe harbour principles may be limited by *'statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'*.

179. It must be stated that the *'legitimate interests'* referred to in that provision are not defined. That leads to uncertainty as to the — potentially very wide — scope of that derogation from the application of the safe harbour principles by the undertakings that adhere to them.

180. That impression is confirmed on reading the explanations in Part B of Annex IV to Decision 2000/520, headed *'Explicit Legal Authorisations'*, in particular the assertion that, *'[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'*. It is further stated, as regards explicit authorisations, that, *'while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers'*.

181. It follows that, to my mind, that derogation is contrary to Articles 7, 8 and 52(1) of the Charter since it does not pursue an objective of general interest defined with sufficient precision.

182. In any event, the ease and generality with which Decision 2000/520 itself, in point (b) in the fourth paragraph of Annex I and in Part B of Annex IV, provides that the safe harbour principles may be disregarded pursuant to provisions of United States law are incompatible with the condition that derogations from the rules on the protection of personal data must be limited to what is strictly necessary. The *'necessity'* condition is certainly mentioned, but, quite apart from the fact that it is the undertaking concerned that is responsible for demonstrating that that condition is satisfied, I fail to see how such an undertaking could escape an obligation to disregard the safe harbour principles which arises under the legal rules which it is required to apply.

183. I am therefore of the view that Decision 2000/520 must be declared invalid since the existence of a derogation which allows in such general and imprecise terms the principles of the safe harbour scheme to be disregarded prevents in itself that scheme from being considered to ensure an adequate level of protection of the personal data which is transferred to the United States from the European Union.

184. As regards, now, the first category of limits, provided for in point (a) in the fourth paragraph of Annex I to Decision 2000/520 on account of national security, public interest or law enforcement requirements, only the first objective seems to me to be sufficiently precise to be regarded as an objective of general interest recognised by the European Union within the meaning of Article 52(1) of the Charter.

185. It is now appropriate to ascertain the proportionality of the interference found.

186. In that regard, it should be borne in mind that, *'according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and not exceed the limits of what is appropriate and necessary in order to achieve those objectives'*. (69)

187. As regards judicial review of compliance with those conditions, *'where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference'*. (70)

188. I am of the view that decisions which the Commission adopts on the basis of Article 25(6) of Directive 95/46 are subject to comprehensive review by the Court as regards the proportionality of the assessment made by the Commission in relation to the adequacy of the level of protection afforded by a third country by reason *'of its domestic law or of the international commitments it has entered into'*.

189. It should be noted, in that regard, that in its judgment in Digital Rights Ireland and Others (71) the Court held that, *'in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by [the directive at issue], the EU legislature's discretion is reduced, with the result that review of that discretion should be strict'*. (72)

190. Such an interference must be an appropriate means of attaining the objective pursued by the EU measure at issue and be necessary for the purpose of attaining that objective.

191. In that regard, *'[s]o far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law …, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary'*. (73)

192. In carrying out its review, the Court also takes into account the fact that *'the protection of personal data*

resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter'. (74)

193. According to the Court, which refers, in that regard, to the case-law of the European Court of Human Rights, *'the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data [has] been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data'*. (75) The Court states that *'[t]he need for such safeguards is all the greater where ... personal data [is] subjected to automatic processing and where there is a significant risk of unlawful access to [that] data'*. (76)

194. In my view, an analogy can be drawn between point (a) in the fourth paragraph of Annex I to Decision 2000/520 and Article 13(1) of Directive 95/46. In the first provision, it is stated that adherence to the safe harbour principles may be limited by *'national security, public interest, or law enforcement requirements'*. In the second, it is provided that 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 of that directive, when such a restriction constitutes a necessary measure to safeguard, in particular, national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

195. As the Court observed in its judgment in IPI, (77) it is apparent from the wording of Article 13(1) of Directive 95/46 that the Member State may lay down the measures referred to in that provision only when they are necessary. The requirement that the measures be *'necessary'* is thus a precondition for the option granted to Member States by that provision. (78) For the processing of personal data within the European Union, the limits laid down in Article 13 of the directive must be understood as being confined to what is strictly necessary in order to achieve the objective pursued. The same must in my view apply to the limits to the safe harbour principles provided for in the fourth paragraph of Annex I to Decision 2000/520.

196. It must be pointed out that not all the language versions mention the criterion of necessity in the wording of point (a) in the fourth paragraph of Annex I to Decision 2000/520. That applies, in particular, to the French language version, which states that *'[l]'adhésion aux principes peut être limitée par ... les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis'*, whereas, by way of example, the Spanish, German and English language versions state that the limitations imposed must be necessary to achieve the abovementioned objectives.

197. Be that as it may, the facts set out by the referring court and by the Commission in the communications referred to above clearly show that, in practice, the implementation of those limitations is not confined to what is strictly necessary to achieve the objectives referred to.

198. I note, in that regard, that the access which the United States intelligence authorities may have to the personal data transferred covers, in a generalised manner, all persons and all means of electronic communication and all the data transferred, including the content of the communications, without any differentiation, limitation or exception according to the objective of general interest pursued. (79)

199. Indeed, the access of the United States intelligence services to the data transferred covers, in a comprehensive manner, all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security. (80)

200. Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter.

201. As the Parliament has correctly observed in its observations, since it is excluded for the EU legislature or the Member States to adopt legislation, contrary to the Charter, providing for mass and indiscriminate surveillance, it must follow, a fortiori, that third countries cannot under any circumstances be regarded as ensuring an adequate level of protection of personal data of citizens of the Union where their rules of law do in fact permit the mass and indiscriminate surveillance and interception of such data.

202. It should be emphasised, moreover, that the safe harbour scheme, as defined in Decision 2000/520, does not contain appropriate guarantees for preventing mass and generalised access to the transferred data.

203. I observe, in that regard, that in its judgment in Digital Rights Ireland and Others (81) the Court stressed the importance of providing *'clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter'*. (82) Such an interference must, according to the Court, be *'precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary'*. (83) The Court also drew attention in that judgment to the need to make provision for *'sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the [personal data] against the risk of abuse and against any unlawful access and use of that data'*. (84)

204. However, the private dispute resolution mechanisms and the FTC, owing to its role limited to commercial disputes, are not means of challenging access by the United States intelligence services to personal data transferred from the European Union.

205. The FTC's jurisdiction covers unfair or deceptive acts and practices in commerce and therefore does not extend to the collection and use of personal information for non-commercial purposes. (85) The FTC's limited area of competence restricts the individual's right to protection of personal data. The FTC was established not, as is the case within the European Union of the

national supervisory authorities, to ensure the protection of the individual right to privacy, but to ensure fair and trustworthy commerce for consumers, which limits de facto its capacity to intervene in the sphere of personal data protection. The FTC therefore does not play a role comparable to that of the national supervisory authorities which are provided for in Article 28 of Directive 95/46.

206. Citizens of the Union whose data has been transferred may approach specialist dispute resolution bodies established in the United States, such as TRUSTe and BBBOnline, to request information as to whether the undertaking holding their personal data is infringing the conditions of the self-certification regime. The private dispute resolution carried out by bodies such as TRUSTe cannot deal with breaches of the right to protection of personal data by bodies or authorities other than self-certified undertakings. Those dispute resolution bodies have no power to rule on the lawfulness of the activities of the United States security agencies.

207. Neither the FTC nor the private dispute resolution bodies therefore have the power to monitor possible breaches of principles for the protection of personal data by public actors such as the United States security agencies. Such a power is, however, essential in order to guarantee in full the right to effective protection of that data. The Commission was therefore not entitled to find, in adopting Decision 2000/520 and maintaining it in force, that there would be adequate protection for all personal data transferred to the United States of the right granted by Article 8(3) of the Charter, that is to say, that an independent authority would effectively monitor compliance with the requirements for the protection and security of that data.

208. It should therefore be found that within the safe harbour scheme provided for by Decision 2000/520 there is no independent authority capable of verifying that the implementation of the derogations from the safe harbour principles is limited to what is strictly necessary. Yet we have seen that such control by an independent authority is, from the point of view of EU law, an essential component of the protection of individuals with regard to the processing of personal data. (86)

209. It is appropriate, in that regard, to note the role played, in the system of personal data protection in force in the European Union, by the national supervisory authorities in monitoring the limitations provided for by Article 13 of Directive 95/46. According to the second subparagraph of Article 28(4) of that directive, *'[e]ach supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply'*. By analogy, I consider that the reference in the fourth paragraph of Annex I to Decision 2000/520 to limits to the application of the safe harbour principles ought to have been accompanied by the establishment of a control mechanism operated by an independent authority specialising in personal data protection.

210. The intervention of independent supervisory authorities is in fact at the heart of the European system of personal data protection. It is therefore natural that the existence of such authorities was considered from the outset to be one of the conditions necessary for a finding that the level of protection afforded by third countries was adequate; and it is a condition that must be satisfied in order for data flows from the territory of the Member States to the territory of third countries not to be prohibited under Article 25 of Directive 95/46. (87) As noted in the working document adopted by the Working Party established by Article 29 of that directive, in Europe there is broad agreement that *'a system of "external supervision" in the form of an independent authority is a necessary feature of a data protection compliance system'*. (88)

211. I observe, moreover, that the FISC does not offer an effective judicial remedy to citizens of the Union whose personal data is transferred to the United States. The protection against surveillance by government services provided for in section 702 of the Foreign Intelligence Surveillance Act of 1978 applies only to United States citizens and to foreign citizens legally resident on a permanent basis in the United States. As the Commission itself has observed, the oversight of United States intelligence collection programmes would be improved by strengthening the role of the FISC and by introducing remedies for individuals. Those mechanisms could reduce the processing of personal data of citizens of the Union that is not relevant for national security purposes. (89)

212. Furthermore, the Commission has itself pointed out that there are no opportunities for citizens of the Union to obtain access to or rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the United States surveillance programmes. (90)

213. It should be observed, last, that the United States rules on the protection of privacy may be applied differently to United States citizens and to foreign citizens. (91)

214. It follows from the foregoing that Decision 2000/520 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be found that that decision and the way in which it is applied entail a wide-ranging and particularly serious interference with those fundamental rights, without that interference being precisely circumscribed by provisions to ensure that it is in fact limited to what is strictly necessary.

215. By adopting Decision 2000/520 and then maintaining it in force, the Commission therefore exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter. To that must be added the finding of an unwarranted interference with the right of

citizens of the Union to an effective remedy as protected by Article 47 of the Charter.

216. That decision must therefore be declared invalid since, owing to the breaches of fundamental rights described above, the safe harbour scheme which it establishes cannot be regarded as ensuring an adequate level of protection of the personal data transferred from the European Union to the United States under that scheme.

217. Given such a finding of infringements of the fundamental rights of citizens of the Union, I consider that the Commission ought to have suspended the application of Decision 2000/520.

218. That decision is of indefinite duration. The present case shows that the adequacy of the level of protection afforded by a third country may change over time, according to the change in both the factual and the legal circumstances on which the decision was based.

219. I observe that Decision 2000/520 itself contains provisions allowing for the Commission to adapt the decision according to the circumstances.

220. Thus, recital 9 of that decision states that *'[t]he "safe harbour" created by the Principles and the FAQs may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved'*.

221. Also, as stated in Article 3(4) of that decision, *'[i]f the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures ... with a view to reversing or suspending the present Decision or limiting its scope'*.

222. Furthermore, according to Article 4(1) of Decision 2000/520, that decision *'may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation. The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46..., including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46'*. Under Article 4(2) of Decision 2000/520, *'[t]he Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46'*.

223. The Commission has stated in its observations that *'there is a substantial likelihood that adherence to the Safe Harbour Privacy Principles [has] been limited in a way that fails to comply with the strictly tailored national security exemption'*. (92) It observes, in that regard, that *'[t]he revelations in question point to a level of surveillance of a massive and indiscriminate scale incompatible with the standard of necessity laid down in that exemption as well as, more generally, with the right to personal data protection as enshrined in Article 8 of the Charter'*. (93) The Commission itself has stated, moreover, that *'[t]he reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement'*. (94)

224. In addition, the Commission expressly acknowledged at the hearing that, under Decision 2000/520, as currently applied, there is no guarantee that the right of citizens of the Union to protection of their data will be ensured. However, in the Commission's submission, that finding is not such as to render that decision invalid. While the Commission agrees with the statement that it must act when faced with new circumstances, it maintains that it has taken appropriate and proportionate measures by entering into negotiations with the United States in order to reform the safe harbour scheme.

225. I do not share that view. In the meantime, it must be possible for transfers of personal data to the United States to be suspended at the initiative of the national supervisory authorities or following complaints lodged with them.

226. In addition, I consider that, faced with such findings, the Commission ought to have suspended the application of Decision 2000/520. The objective of protecting personal data pursued by Directive 95/46 and Article 8 of the Charter places obligations not only on the Member States but also on the EU institutions, as follows from Article 51(1) of the Charter.

227. In its assessment of the level of protection afforded by a third country, the Commission must examine not only the internal laws and international commitments of that third country, but also the manner in which the protection of personal data is guaranteed in practice. Where the examination of practice reveals that the arrangements are not working correctly, the Commission must take action and, where appropriate, suspend its decision or adapt it without delay.

228. As we have seen above, the obligation owed by the Member States consists mainly in ensuring, by the action of their national supervisory authorities, compliance with the rules laid down in Directive 95/46.

229. The obligation owed by the Commission is to suspend the application of a decision which it has adopted on the basis of Article 25(6) of that directive in the case of proven shortcomings on the part of the third country concerned, while it conducts negotiations with that country in order to put an end to those shortcomings.

230. It will be recalled that the purpose of a decision adopted by the Commission on the basis of that provision is to find that a third country *'ensures'* an adequate level of protection of the personal data which is transferred to that country. The word *'ensures'*,

conjugated in the present tense, implies that, in order to be able to be maintained, such a decision must relate to a third country which, after the adoption of the decision, continues to guarantee such an adequate level of protection.

231. According to recital 57 of Directive 95/46, *'the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited'*.

232. Under Article 25(4) of that directive, *'[w]here the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question'*. Furthermore, Article 25(5) of the directive provides that *'[a]t the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4'*.

233. It follows from the latter provision that, in the system put in place by Article 25 of Directive 95/46, the purpose of the negotiations entered into with a third country is to remedy the absence of an adequate level of protection found in accordance with the procedure laid down in Article 31(2) of that directive. In the case with which we are concerned, the Commission did not formally find, in accordance with that procedure, that the safe harbour scheme no longer ensured an adequate level of protection. None the less, if the Commission decided to enter into negotiations with the United States, that is because it considered beforehand that the level of protection ensured by that third country was no longer adequate.

234. Although it was aware of shortcomings in the application of Decision 2000/520, the Commission neither suspended nor adapted that decision, thus entailing the continuation of the breach of the fundamental rights of the persons whose personal data was and continues to be transferred under the safe harbour scheme.

235. The Court has already held, admittedly in a different context, that the Commission has the task of bringing about an amendment to the rules in the light of new information. (95)

236. Such a failure to act on the part of the Commission, which directly impairs the fundamental rights protected by Articles 7, 8 and 47 of the Charter, is to my mind an additional ground on which to declare Decision 2000/520 invalid in the context of the present reference for a preliminary ruling. (96)

III – Conclusion

237. In the light of the foregoing, I propose that the Court should answer the questions referred by the High Court as follows:

Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the existence of a decision adopted by the European Commission on the basis of Article 25(6) of Directive 95/46 does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the Department of Commerce of the United States of America is invalid.

---

1 – Original language: French.

2 – Communication from the Commission to the European Parliament and the Council, entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final).

3 – P. 2.

4 – OJ 2000 L 215, p. 7, and corrigendum at OJ 2001 L 115, p. 14.

5 – OJ 1995 L 281, p. 31. Directive 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').

6 – 'FAQs'.

7 – Second paragraph of Annex I to Decision 2000/520.

8– See Annex I, under the heading 'Notice'.

9– See Annex I, under the heading 'Choice'.

10– See Annex I, under the heading 'Onward transfer'.

11– See Annex I, under the heading 'Security'.

12– See Annex I, under the heading 'Data integrity'.

13– See Annex I, under the heading 'Access'.

14– See Annex I, under the heading 'Enforcement'.

15 – Article 1(2) and (3) of Decision 2000/520. See also Annex II, FAQ 6.

16 – Third paragraph of Annex I.

17 – See also Part B of Annex IV.

18 – See section 702 of that Act, as amended by the Foreign Intelligence Surveillance Act of 2008. It is under that section that the NSA maintains a database known as 'PRISM' (see Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013).

19 – The High Court mentions, in particular, respect for the dignity and freedom of the individual (preamble), personal autonomy (Article 40.3.1 and Article 40.3.2), the inviolability of the dwelling (Article 40.5) and the protection of family life (Article 41).

20 – The High Court points out in that regard that the key ground advanced by Mr Schrems before it was to the effect that, in the light of the recent revelations of Edward Snowden and the fact that private data was made available on a large scale to the United States intelligence services, the Commissioner could not

properly conclude that an adequate level of protection of that data is in place in that third country.

21 – C‑293/12 and C‑594/12, EU:C:2014:238, paragraphs 65 to 69.

22 – See, in particular, judgment in Koushkaki (C‑84/12, EU:C:2013:862, paragraph 34 and the case-law cited).

23 – See judgments in Commission v Austria (C‑614/10, EU:C:2012:631, paragraph 36) and Commission v Hungary (C‑288/12, EU:C:2014:237, paragraph 47).

24 – See, in particular, judgment in Commission v Hungary (C‑288/12, EU:C:2014:237, paragraph 48 and the case-law cited). See also, to that effect, judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 68 and the case-law cited).

25 – See, in particular, judgment in Commission v Hungary (C‑288/12, EU:C:2014:237, paragraph 51 and the case-law cited).

26 – Judgment in Commission v Germany (C‑518/07, EU:C:2010:125, paragraph 25).

27 – Ibid.

28 – Ibid. (paragraph 22 and the case-law cited).

29 – Ibid. (paragraph 23). See also, to that effect, judgments in Commission v Austria (C‑614/10, EU:C:2012:631, paragraph 52) and Commission v Hungary (C‑288/12, EU:C:2014:237, paragraph 53).

30 – See Opinion of Advocate General Léger in Parliament v Council and Commission (C‑317/04 and C‑318/04, EU:C:2005:710, points 92 to 95). See also judgment in Parliament v Council and Commission (C‑317/04 and C‑318/04, EU:C:2006:346, paragraph 56).

31 – See, in particular, judgment in IPI (C‑473/12, EU:C:2013:715, paragraph 28 and the case-law cited).

32 – See, in particular, judgment in Google Spain and Google (C‑131/12, EU:C:2014:317, paragraph 68 and the case-law cited).

33 – See, in particular, judgment in N.S.and Others (C‑411/10 and C‑493/10, EU:C:2011:865, paragraph 77 and the case-law cited).

34 – C‑411/10 and C‑493/10, EU:C:2011:865.

35 – Council Regulation of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ 2003 L 50, p. 1).

36 – Paragraph 99 of that judgment.

37 – United Nations Treaty Series, Vol. 189, p. 150, No 2545 (1954).

38 – See judgment in N.S.and Others (C‑411/10 and C‑493/10, EU:C:2011:865, paragraph 80).

39 – Ibid. (paragraph 81).

40 – Ibid. (paragraph 94).

41 – C‑411/10 and C‑493/10, EU:C:2011:865.

42 – Paragraph 104 of that judgment.

43 – C‑101/01, EU:C:2003:596.

44 – Paragraph 65.

45 – Paragraph 64.

46 – According to Mr Schrems, the first condition, that ‘there is a substantial likelihood that the Principles are being violated’, is not satisfied. It is not alleged that Facebook USA, as a self-certifying entity to which data is transferred, has itself violated the safe harbour principles because of the mass and indiscriminate access of the United States authorities to the data which it holds. The safe harbour principles are expressly limited by United States law, which the fourth paragraph of Annex I to Decision 2000/520 defines by referring to statute, government regulation or case-law.

47 – Paragraph 24 of the order for reference.

48 – See, in particular, judgments in Strehl (62/76, EU:C:1977:18, paragraphs 10 to 17); Roquette Frères (145/79, EU:C:1980:234, paragraph 6); and Schutzverband der Spirituosen-Industrie (C‑457/05, EU:C:2007:576, paragraphs 32 to 39).

49 – Judgment in Schwarze (16/65, EU:C:1965:117, p. 886).

50– See judgment in Hauer (44/79, EU:C:1979:290, paragraph 16).

51 – See, in particular, judgment in CIVAD (C‑533/10, EU:C:2012:347, paragraphs 39 to 41 and the case-law cited).

52 – See, in particular, judgment in BVGD v Commission (T‑104/07 and T‑339/08, EU:T:2013:366, paragraph 291), referring to the judgment in IECC v Commission (C‑449/98 P, EU:C:2001:275, paragraph 87).

53 – C‑247/08, EU:C:2009:600.

54 – Paragraph 49 and the case-law cited.

55 – Paragraph 50 and the case-law cited. See, to that effect, Lenaerts, K., Maselis, I., and Gutman, K., EU Procedural Law, Oxford University Press, 2014, where the authors state that, ‘in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court’ (paragraph 10.16, p. 471).

56 – See p. 5 of Commission Working Document WP 12, entitled ‘Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive’, adopted by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data on 24 July 1998.

57 – See, in particular, judgment in Fallimento Traghetti del Mediterraneo (C‑140/09, EU:C:2010:335, paragraph 22 and the case-law cited).

58 – See the Commission communication referred to in footnote 2 and the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final).

59 – Paragraph 7(c) of the order for reference.

60 – Paragraph 7(b) of the order for reference.

61 – P. 16 of the communication.

62 – See, in particular, judgment in Kadi and Al Barakaat International Foundation v Council and Commission (C‑402/05 P and C‑415/05 P, EU:C:2008:461, paragraph 284 and the case-law cited).
63 – Judgment in Österreichischer Rundfunk and Others (C‑465/00, C‑138/01 and C‑139/01, EU:C:2003:294, paragraph 74).
64 – C‑293/12 and C‑594/12, EU:C:2014:238.
65 – Paragraph 35.
66 – Paragraph 36.
67 – Paragraph 7(b) of the order for reference.
68 – See, in that regard, judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraphs 39 and 40).
69 – Judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 46 and the case-law cited).
70 – Ibid. (paragraph 47 and the case-law cited).
71 – C‑293/12 and C‑594/12, EU:C:2014:238.
72 – Paragraph 48.
73 – Judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 52 and the case-law cited).
74 – Ibid., paragraph 53.
75 – Ibid., paragraph 54 and the case-law cited.
76 – Ibid., paragraph 55 and the case-law cited.
77 – C‑473/12, EU:C:2013:715.
78 – Paragraph 32.
79 – See, by analogy, judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 57 and the case-law cited).
80 – Ibid. (paragraphs 58 and 59).
81 – C‑293/12 and C‑594/12, EU:C:2014:238.
82 – Paragraph 65.
83– Idem.
84– Ibid. (paragraph 66).
85 – See, in that regard, FAQ 11 in Annex II to Decision 2000/520, under the heading ‘FTC Action’, and Annexes III, V and VII to that decision.
86 – See judgment in Digital Rights Ireland and Others (C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 68 and the case-law cited).
87 – See Poullet, Y., ‘L’autorité de contrôle: “vues” de Bruxelles’, Revue française d’administration publique, No 89, January-March 1999, p. 69, especially p. 71.
88 – See p. 7 of Commission Working Document WP 12, referred to in footnote 56.
89 – P. 9 of the Commission communication referred to in footnote 2.
90 – See p. 20, paragraph 7.2, of Commission Communication COM(2013) 847 referred to in footnote 58.
91 – See, on that issue, Kuner, C., ‘Foreign Nationals and Data Protection Law: A Transatlantic Analysis’, Data Protection Anno 2014: How To Restore Trust?, Intersentia, Cambridge, 2014, p. 213, especially p. 216 et seq.
92– Paragraph 44.
93– Idem.
94 – See p. 5 of the Commission communication referred to in footnote 2.
95 – See, to that effect, judgment in Agrarproduktion Staebelow (C‑504/04, EU:C:2006:30, paragraph 40).
96– Although the Court held in its judgment in T. Port (C‑68/95, EU:C:1996:452) that ‘the Treaty makes no provision for a reference for a preliminary ruling by which a national court asks the Court of Justice to rule that an institution has failed to act’ (paragraph 53), it seems to have looked more favourably on that possibility in its judgment in Ten Kate Holding Musselkanaal and Others (C‑511/03, EU:C:2005:625, paragraph 29).