Provisional text

JUDGMENT OF THE GENERAL COURT (Tenth Chamber, Extended Composition)

3 September 2025 (*)

(Transfer of personal data to the United States – Commission Implementing Decision on the adequate level of protection of personal data ensured by the United States – Right to an effective remedy – Right to private and family life – Decisions based solely on the automated processing of personal data – Security of the processing of personal data)

In Case T-553/23,

Philippe Latombe, residing in Nantes (France), represented by N. Coutrelis, J.-B. Soufron and T. Lamballe, lawyers,

applicant,

v

European Commission, represented by D. Calleja Crespo, A. Bouchagiar, H. Kranenborg and C. Ladenburger, acting as Agents,

defendant,

supported by

Ireland, represented by M. Browne, S. Finnegan and A. Joyce, acting as Agents, and by S. Brittain, Barrister, and C. Donnelly, SC,

and by **United States of America,** represented by B. Walsh, S. Barton and A. Finlay, Solicitors, E. Barrington, SC, and D. Hardiman, Barrister,

interveners,

THE GENERAL COURT (Tenth Chamber, Extended Composition),

composed of O. Porchia, President, M. Jaeger (Rapporteur), L. Madise, P. Nihoul and S. Verschuur, Judges,

Registrar: I. Kurme, Administrator,

having regard to the order of 12 October 2023, *Latombe* v *Commission* (T-553/23 R, not published, EU:T:2023:621),

having regard to the written part of the procedure,

further to the hearing on 1 April 2025,

gives the following

Judgment

1 By his action under Article 263 TFEU, the applicant, Mr Philippe Latombe, seeks, in essence, annulment of Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of

protection of personal data under the EU-US Data Privacy Framework (OJ 2023 L 231, p. 118, 'the contested decision').

I. Background to the dispute

2 The applicant is a French citizen who claims to use various IT platforms that collect his personal data and transfer them to the United States.

3 As regards the transfer of personal data from the European Union to the United States, initially, by judgment of 6 October 2015, *Schrems* (C-362/14, 'the judgment in *Schrems I*', EU:C:2015:650), the Court of Justice declared invalid Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

4 Subsequently, by judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, 'the judgment in *Schrems II*', EU:C:2020:559), the Court of Justice declared invalid Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016 L 207, p. 1, 'the Privacy Shield adequacy decision').

5 In the judgments in *Schrems I* and *Schrems II*, the Court of Justice, hearing a reference for a preliminary ruling on validity, held, inter alia, that, contrary to the findings of the European Commission apparent from the adequacy decisions referred to in paragraphs 3 and 4 above, the safe harbour system and the Privacy Shield system for data protection ('the Privacy Shield') governing the transfer of personal data did not afford a level of protection of fundamental rights and freedoms essentially equivalent to that guaranteed by EU law.

6 Following the judgment in *Schrems II*, the Commission began talks with the United States Government with a view to adopting a new adequacy decision that would meet the requirements of Article 45(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, corrigendum OJ 2018 L 127, p. 2, 'the GDPR'), as they have been interpreted by the Court of Justice.

7 Accordingly, on 7 October 2022, the United States of America adopted Executive Order 14086 ('Executive Order 14086'), which strengthens the privacy safeguards governing signals intelligence activities carried out by the intelligence agencies established in the United States. That order was supplemented by Attorney General Order No 5517–2022 ('the Attorney General Order'), which added Part 201 to Title 28 of the Code of Federal Regulations (CFR), governing the establishment and functioning of the Data Protection Review Court ('the DPRC').

8 On 10 July 2023, after examining those regulatory developments in the United States and on the basis of Article 45(3) of the GDPR, the Commission adopted the contested decision, which establishes the new transatlantic framework for personal data flows between the European Union and the United States. Article 1 of that decision states that the United States of America ensures an adequate level of protection for personal data transferred from the European Union to organisations in the United States and included in the list relating to the 'EU-U.S. Data Privacy Framework' ('the DPF') maintained and made publicly available by the United States Department of Commerce ('the DPF organisations').

II. Forms of order sought

9 The applicant claims that the Court should:

– annul the contested decision, in essence, in its entirety;

– order the Commission to pay the costs.

10 The Commission, supported by Ireland and the United States of America, claims that the Court should:

– dismiss the action as inadmissible;

– in the alternative, dismiss the action as unfounded;

– order the applicant to pay the costs.

III. **Law**

A. **The plea of inadmissibility**

11 By a separate document lodged at the Court Registry on 1 December 2023, the Commission raised a plea of inadmissibility, on the basis of Article 130 of the Rules of Procedure of the General Court.

12 The Commission claims that the action is inadmissible, on the grounds that the applicant does not have *locus standi*, that he does not have an interest in bringing an action and that the part of the contested decision which he seeks to have annulled is inseparable from the rest of that decision.

13 The applicant disputes the Commission's arguments and submits that his action is admissible.

14 It should be borne in mind that the Courts of the European Union are entitled to assess, according to the circumstances of each case, whether the proper administration of justice justifies the dismissal of the action on the merits without a prior ruling on its admissibility (see, to that effect, judgment of 26 February 2002, *Council* v *Boehringer*, C-23/00 P, EU:C:2002:118, paragraphs 51 and 52).

15 Accordingly, taking account of the circumstances of the present case, the Court considers that as the action is, in any event and for the reasons set out in paragraphs 16 to 204 below, unfounded, it is appropriate, in the interests of the proper administration of justice, to examine whether it is well founded, without first ruling on its admissibility (see, to that effect, judgments of 10 October 2014, *Marchiani* v *Parliament*, T-479/13, not published, EU:T:2014:866, paragraph 23, and of 20 December 2023, *Naturstrom* v *Commission*, T-60/21, not published, EU:T:2023:839, paragraph 74).

B. **Substance**

16 In support of the action, the applicant relies on five pleas in law, alleging:

– first, infringement of Articles 3 and 4 of Council Regulation No 1 of 15 April 1958 determining the languages to be used by the European Economic Community (OJ English Special Edition 1952-1958, p. 59);

– second, infringement of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

– third, infringement of the second paragraph of Article 47 of that charter and of Article 45(2) of the GDPR;

– fourth, infringement of Article 22 of the GDPR;

– fifth, infringement of Article 32 of the GDPR, read in conjunction with Article 45(2) of that regulation.

17 At the hearing, the applicant withdrew his first plea in law, concerning the infringement of Articles 3 and 4 of Regulation No 1 of 1958. It is therefore appropriate to examine only his second to fifth pleas in law.

1. ***Preliminary observations***

18 In the first place, it should be noted that Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection. That provision is included in Chapter V of that regulation, which, as the Court of Justice has

already stated, is intended overall to ensure the continuity of the high level of protection of personal data which is guaranteed by EU law under that regulation, where those data are transferred to a third country (see, to that effect, the judgment in *Schrems II*, paragraph 93).

19 In that regard, the Court of Justice has made clear that, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' in Article 45(1) of the GDPR had to 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 was essentially equivalent to that guaranteed within the European Union by virtue of that regulation, read in the light of the Charter of Fundamental Rights (see, to that effect, the judgment in *Schrems II*, paragraphs 94 and 162).

20 The Court of Justice has also held that, even though the means to which that third country had recourse for the purpose of ensuring an adequate level of protection of personal data might 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 of Fundamental Rights were complied with, those means had nevertheless to prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union (the judgment in *Schrems I*, paragraph 74).

21 In addition, the Court of Justice has held 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, second, the large number of persons whose fundamental rights are liable to be infringed where personal data are transferred to a third country which does not ensure an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country was reduced, with the result that review by the Courts of the European Union of the legality of an adequacy decision had to be strict (the judgment in *Schrems I*, paragraph 78).

22 In the second place, it should be borne in mind that, according to settled case-law, the legality of an EU measure must be assessed on the basis of the facts and the law as they stood at the time when that measure was adopted, so that measures post-dating the adoption of a decision cannot affect that decision's validity (see judgments of 17 October 2019, *Alcogroup and Alcodis* v *Commission*, C-403/18 P, EU:C:2019:870, paragraph 45 and the case-law cited, and of 28 January 2021, *Qualcomm and Qualcomm Europe* v *Commission*, C-466/19 P, EU:C:2021:76, paragraph 82 and the case-law cited). In the present case, therefore, the Commission's findings concerning the legality of the contested decision must be examined solely by reference to the information available to it when it made them.

23 It is in that context that it is necessary to analyse the pleas in law raised by the applicant, examining first of all the third plea, followed by the second plea, then the fourth plea and finally the fifth plea.

2. *The third plea in law, alleging infringement of the second paragraph of Article 47 of the Charter of Fundamental Rights and of Article 45(2) of the GDPR*

24 By his third plea in law, the applicant maintains that the Commission infringed the second paragraph of Article 47 of the Charter of Fundamental Rights and Article 45(2) of the GDPR since, in the contested decision, it considered that the DPRC afforded an adequate level of protection as regards the right of EU individuals to an independent and impartial tribunal previously established by law.

25 As a preliminary point, it should be observed that the second paragraph of Article 47 of the Charter of Fundamental Rights is worded as follows:

'Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.'

26 According to the Explanations relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17), the second paragraph of Article 47 of that charter corresponds to Article 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 ('the ECHR'). That provision is worded as follows:

‘In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law.’

27 In that regard, it should be borne in mind that, according to the case-law, since the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law, the examination of the validity of an act of secondary law must be based solely on the fundamental rights guaranteed by the Charter of Fundamental Rights (judgment of 3 September 2015, *Inuit Tapiriit Kanatami and Others* v *Commission*, C-398/13 P, EU:C:2015:535, paragraphs 45 and 46).

28 However, the case-law recognises, first, that under Article 6(3) TEU fundamental rights recognised by the ECHR constitute general principles of EU law and, second, that it follows from Article 52(3) of the Charter of Fundamental Rights that the rights contained in that charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR (see judgment of 31 May 2018, *Korwin-Mikke* v *Parliament*, T-770/16, EU:T:2018:320, paragraph 38 and the case-law cited).

29 Consequently, according to the case-law, in the interests of coherence and without that circumstance undermining the autonomy of EU law and of the Court of Justice of the European Union, the rights contained in the Charter of Fundamental Rights which correspond to those guaranteed by the ECHR must also be interpreted in the light of the case-law of the European Court of Human Rights (‘the ECtHR’) (see, to that effect, judgments of 9 November 2023, *Staatssecretaris van Justitie en Veiligheid (Concept of serious harm)*, C-125/22, EU:C:2023:843, paragraph 59, and of 31 May 2018, *Korwin-Mikke* v *Parliament*, T-770/16, EU:T:2018:320, paragraph 38).

30 It follows, according to the case-law, that the Court of Justice must ensure, pursuant to Article 52(3) of the Charter of Fundamental Rights, that the interpretation which it gives to the second paragraph of Article 47 of that charter safeguards a level of protection which does not fall below the level of protection established in Article 6(1) ECHR, as interpreted by the ECtHR (see judgment of 6 October 2021, *W.Ż. (Chamber of Extraordinary Control and Public Affairs of the Supreme Court – Appointment*), C-487/19, EU:C:2021:798, paragraph 123 and the case-law cited).

31 It should also be noted that Article 45(2) of the GDPR provides that, when assessing the adequacy of the level of protection afforded by a third country, the Commission is, in particular, to take account of the following elements:

‘(a) … effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

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

32 It is in the light of those elements that it is necessary to examine the two complaints raised by the applicant in support of the present plea in law.

(a) ***The first complaint in the third plea in law, that the DPRC is not an independent and impartial tribunal***

33 By the first complaint in his third plea in law, the applicant maintains that the DPRC is not an independent and impartial tribunal within the meaning of the second paragraph of Article 47 of the Charter of Fundamental Rights, but a quasi-judicial body forming part of the executive branch.

34 The Commission, supported by Ireland and by the United States of America, disputes the applicant’s arguments.

35 As a preliminary point, it should be noted that, according to the case-law, the requirement that courts be independent, which is inherent in the task of adjudication, forms part of the essence of the right to effective judicial protection and the fundamental right to a fair trial, which is of cardinal importance as a guarantee that all the rights which individuals derive from EU law will be protected and that the values common to the Member States set out in Article 2 TEU, in particular the value of the rule of law, will be safeguarded (judgment of 15 July 2021, *Commission* v *Poland (Disciplinary regime for judges)*, C-791/19, EU:C:2021:596, paragraph 58 and the case-law cited). In accordance with the principle of the separation of powers which characterises the operation of the rule of law, the independence of the judiciary must in particular be ensured in relation to the legislature and the executive (see judgment of 18 May 2021, *Asociaţia 'Forumul Judecătorilor din România' and Others*, C-83/19, C-127/19, C-195/19, C-291/19, C-355/19 and C-397/19, EU:C:2021:393, paragraph 195 and the case-law cited).

36 The case-law makes clear that the requirement that courts be independent has two aspects. The first aspect, which is external in nature, requires that the court concerned exercise its functions wholly autonomously, without being subject to any hierarchical constraint or subordinated to any other body and without taking orders or instructions from any source whatsoever, thus being protected against external interventions or pressure liable to impair the independent judgment of its members and to influence their decisions. The second aspect, which is internal in nature, is linked to 'impartiality' and seeks to ensure that an equal distance is maintained from the parties to the proceedings and their respective interests with regard to the subject matter of those proceedings. That aspect requires objectivity and the absence of any interest in the outcome of the proceedings apart from the strict application of the rule of law (see judgment of 21 December 2021, *Euro Box Promotion and Others*, C-357/19, C-379/19, C-547/19, C-811/19 and C-840/19, EU:C:2021:1034, paragraph 224 and the case-law cited).

37 The guarantees of independence and impartiality required under EU law require rules, particularly as regards the composition of the body and the appointment, length of service and grounds for abstention, rejection and dismissal of its members, that are such as to dispel any reasonable doubt in the minds of individuals as to the imperviousness of that body to external factors and its neutrality with respect to the interests before it (see judgment of 15 July 2021, *Commission* v *Poland (Disciplinary regime for judges)*, C-791/19, EU:C:2021:596, paragraph 59 and the case-law cited).

38 It is in that context that the three arguments put forward by the applicant in support of the present complaint must be examined.

(1) *The first argument, that the DPRC is not an independent and impartial tribunal since its mission is to review decisions of the 'Civil Liberties Protection Officer of the Director of National Intelligence'*

39 By his first argument, the applicant claims, in essence, that the DPRC is not an independent and impartial tribunal since its mission is to review decisions of the 'Civil Liberties Protection Officer of the Director of National Intelligence' ('the CLPO', United States), who is attached to the Office of the Director of National Intelligence of the United States ('the Director of National Intelligence').

40 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

41 In the interests of clarity, it should be stated that the first argument of the first complaint in the third plea in law must be interpreted as meaning that, in essence, according to the applicant, first, when dealing with a complaint concerning personal data filed by a data subject in the European Union seeking to rely on an infringement of United States law governing signal intelligence activities which adversely affect his or her interests in relation to the protection of privacy and civil liberties ('the complaint concerning personal data'), the CLPO does not have sufficient guarantees designed to ensure his or her independence, on the ground that he or she is attached to the Office of the Director of National Intelligence, and, second, that the DPRC is not an independent and impartial tribunal because the guarantees applicable to the CLPO are insufficient.

42 It should be observed at the outset that examination of the guarantees relating to the independence of the CLPO is irrelevant for the purposes of determining whether the DPRC is an independent and impartial tribunal. The DPRC was established as a review body independent of the CLPO to which, as

is apparent from recital 184 of the contested decision, a person who has filed a complaint concerning personal data and every element of the intelligence community may apply for review of the CLPO's decision, and several guarantees were set out in Executive Order 14086 enabling decisions of the CLPO to be reviewed and, where appropriate, altered independently and impartially by the DPRC.

43 First, it is apparent from recitals 185 and 186 of the contested decision, and is not disputed by the applicant, that the DPRC is composed of at least six judges, who are appointed by the United States Attorney General ('the Attorney General'), after consulting the Privacy and Civil Liberties Oversight Board ('the PCLOB', United States), the United States Secretary of Commerce and the Director of National Intelligence, for renewable terms of four years, using the same criteria as those that apply to members of the federal judiciary, giving weight to any prior judicial experience. Accordingly, the judges must be legal practitioners, that is to say, active members in good standing of the bar and duly licensed to practise law and have appropriate experience in privacy and national security law. Furthermore, the Attorney General must endeavour to ensure that at least half of the judges at any given time have prior judicial experience and all judges must hold security clearance to be able to access classified national security information. Only individuals who meet the qualifications mentioned above and are not employees of the executive branch at the time of their appointment or in the preceding two years can be appointed to the DPRC. Similarly, during their term of office, the DPRC judges may not have any official duties or employment within the United States Government.

44 Second, it is apparent from recitals 188 and 189 of the contested decision, and is not disputed by the applicant, that decisions of the CLPO are reviewed, in full, by a panel of three DPRC judges assisted by a Special Advocate. In that review, the DPRC does not rely solely on the file supplied by the CLPO but also relies on information and submissions provided by the complainant, by the Special Advocate who assists its judges and by the intelligence agencies and also, where appropriate, on additional information which it has requested during the investigation of the complaint concerning personal data. In addition, in that review, it must apply the relevant case-law of the Supreme Court of the United States.

45 Third, it is apparent from recitals 190 and 191 of the contested decision, and is not disputed by the applicant, that the DPRC has power to alter a decision, is not bound by the decision of the CLPO and, in the event of disagreement with the CLPO, may adopt its own determination on the complaint concerning personal data. In addition, whatever decision is adopted by the DPRC, it is binding and final. Both the intelligence agencies and the United States Government are therefore required to comply with it.

46 It follows from the foregoing that the guarantees provided for by Executive Order 14086 as regards the functioning and powers of the DPRC allow an independent and impartial review of the decisions adopted by the CLPO. The applicant cannot therefore validly maintain that a lack of sufficient guarantees applicable to the CLPO impairs the independence and impartiality of the DPRC.

47 In any event, as regards the allegedly insufficient guarantees designed to ensure the independence of the CLPO, it is necessary to make the following observations.

48 It should be noted, as is apparent from recitals 176 to 181 of the contested decision, and is not disputed by the applicant, that Executive Order 14086, supplemented by the Attorney General Order, established a specific redress mechanism in order to deal with complaints concerning personal data. The complaint must be filed with the supervisory authority competent, in each Member State, for the oversight of the processing of personal data, which then channels the complaint to the CLPO, provided that it contains the information set out in recital 178 of the contested decision, namely information relating to the personal data reasonably believed to have been transferred to the United States, the means by which they are believed to have been transferred, the identities of the United States Government entities believed to be involved in the alleged infringement, if known, the basis for alleging that an infringement of United States law has occurred and the nature of the relief sought. In that context, the CLPO must determine whether the intelligence agencies infringed the applicable United States law and, where that is the case, may order them to implement remedial measures. The decision of the CLPO on the complaint is binding.

49 Admittedly, in recital 179 of the contested decision, the Commission indicates that the CLPO forms part of the Office of the Director of National Intelligence and that, in addition to his or her specific task

of reviewing complaints concerning personal data, the CLPO is required, more generally, to ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures of that office and of the intelligence agencies and that those bodies comply with the applicable requirements in relation to the protection of privacy and civil liberties. However, first, it should be noted that, as stated in that recital, in order to ensure the independence of the CLPO, Executive Order 14086 provides that the CLPO can be dismissed only by that director and for cause, that is to say, in the event of misconduct, malfeasance, breach of security, neglect of duty or incapacity. Second, as is apparent from recital 180 of the contested decision, the intelligence agencies and the Director of National Intelligence are prohibited from impeding or improperly influencing the work of the CLPO, who, when reviewing complaints concerning personal data, must apply the law impartially, having regard to both national security interests and the protection of privacy.

50 In those circumstances, the present argument must be rejected.

(2) *The second argument, that the DPRC is not an independent and impartial tribunal since it is composed of judges appointed by the Attorney General after consulting the PCLOB*

51 By his second argument, the applicant maintains, in essence, that the DPRC is not an independent and impartial tribunal since it is composed of judges appointed by the Attorney General after consulting the PCLOB, which is a body dependent on the executive branch.

52 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

53 In the first place, it is apparent from recital 110 of the contested decision that the PCLOB is an independent agency, set up within the executive branch. The independence of that agency is apparent in particular from its composition. It is composed of a bipartisan, five-member board appointed by the President of the United States, with Senate approval, for a fixed six-year term. Those members must be selected on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy and their experience, without regard to political affiliation. There may not be more than three members of the PCLOB that belong to the same political party. An individual appointed to the PCLOB may not, while serving as a member, be an elected official, officer or employee of the Federal Government, other than in the capacity as a member of the PCLOB.

54 It follows that, although the PCLOB was established within the executive branch, it was conceived, by its founding statute, as an independent agency whose mission consists in the impartial supervision of the work carried out by the executive with a view to protecting, in particular, privacy and civil liberties. Accordingly, as stated in recital 194 of the contested decision, and not disputed by the applicant, it must determine every year whether the CLPO and the DPRC have dealt with the cases received in a timely manner, whether they obtained full access to the necessary information, whether they considered all the safeguards provided for in Executive Order 14086 and whether the intelligence agencies have fully complied with their determinations. Following that verification, it must certify publicly that the CLPO and the DPRC have respected those safeguards. In addition, it must submit a report to the President of the United States, the Attorney General, the Director of National Intelligence, the heads of the intelligence agencies, the CLPO and the intelligence committees of the United States Congress. That report is made public in an unclassified version. The Attorney General, the Director of National Intelligence, the CLPO and the heads of the intelligence agencies are required to implement all recommendations made in that report.

55 In those circumstances, the fact that the PCLOB was established within the executive branch does not in itself permit the inference that, because the PCLOB is consulted before the DPRC judges are appointed, the DPRC is not an independent and impartial tribunal.

56 In the second place, it should be noted that, in order to ensure that the DPRC judges are independent of the executive branch, Executive Order 14086 provides that, when they are appointed, the Attorney General must observe the criteria and conditions set out in paragraph 43 above. Furthermore, as is apparent from recital 187 of the contested decision, the DPRC judges may be dismissed only by the Attorney General and only for cause, namely misconduct, malfeasance, breach of security, neglect of

duty or incapacity, after taking due account of the standards applicable to federal judges laid down in the Rules for Judicial Conduct and Judicial Disability Proceedings.

57 It follows that the rules on the appointment and dismissal of the judges of the DPRC cannot call its independence and its impartiality into question.

58 In the third place, it should be observed that, according to Article 3(1) of the contested decision, the Commission is required continuously to monitor the application of the legal framework to which that decision relates, including the conditions under which onward transfers of personal data are carried out, individual rights are exercised and United States public authorities have access to data transferred on the basis of that decision, with the aim of assessing whether the United States of America continues to ensure an adequate level of protection. Accordingly, in accordance with paragraph 5 of that article, where the Commission has indications that an adequate level of protection is no longer ensured, it is to inform the competent United States authorities and, if necessary, decide to suspend, amend or repeal the contested decision, or to limit its scope. It follows that, if there is a change in the legal framework in force in the United States at the time of adoption of the contested decision that led the Commission to consider, in that decision, that the DPRC afforded legal protection essentially equivalent to that guaranteed by EU law, the Commission is to decide, if necessary, to suspend, amend or repeal the contested decision or to limit its scope.

59 In the light of all those considerations, the present argument must be rejected.

(3) *The third argument, that the DPRC is not an independent and impartial tribunal since the Attorney General Order does not preclude the possibility that its judges may be subject to forms of supervision, other than day-to-day supervision, on the part of the executive branch*

60 By his third argument, the applicant claims, in essence, that the DPRC is not an independent and impartial tribunal since the Attorney General Order does not preclude the possibility that its judges may be subject to forms of supervision, other than day-to-day supervision, on the part of the executive branch.

61 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

62 It should be noted that, while it is apparent from the case file that, according to Part 201.7(d) of the Attorney General Order, the DPRC judges must not be subject to day-to-day supervision by the Attorney General, recital 187 of the contested decision also states that, under Executive Order 14086, the intelligence agencies and the Attorney General must not interfere with or improperly influence the work of the DPRC. In addition, it is apparent from the case file that Executive Order 14086 and the Attorney General Order limit the possibility for the executive branch to influence the work of the DPRC, by establishing that its judges may be removed only by the Attorney General and solely for the reasons set out in paragraph 56 above.

63 In that context, the present argument and, accordingly, the first complaint in the third plea in law in its entirety, must be rejected.

(b) ***The second complaint in the third plea in law, that the DPRC is not a tribunal previously established by law***

64 By the second complaint in his third plea in law, the applicant submits that the DPRC was not previously established by law within the meaning of the second paragraph of Article 47 of the Charter of Fundamental Rights, since it was not created by a law adopted by the United States Congress but by an act of the executive, namely a decision of the Attorney General.

65 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

66 In the first place, it is apparent from the case-law of the Court of Justice, developed in the light of that of the ECtHR on Article 6(1) ECHR (ECtHR, 1 December 2020, *Guðmundur Andri Ástráðsson v.*

Iceland, CE:ECHR:2020:1201JUD002637418, §§ 231 and 233), that, while the right to a tribunal previously established by law constitutes an independent right, it is nevertheless inextricably linked to the guarantees of independence and impartiality set out in that provision. In particular, although all the requirements imposed by those concepts have specific aims which render them specific guarantees of a fair trial, those safeguards seek to observe the fundamental principles of the rule of law and the separation of powers. The need to maintain confidence in the judiciary and to safeguard its independence vis-à-vis the other powers thus underlies each of those requirements (see judgments of 22 February 2022, *Openbaar Ministerie (Tribunal established by law in the issuing Member State)*, C-562/21 PPU and C-563/21 PPU, EU:C:2022:100, paragraph 56 and the case-law cited, and of 29 March 2022, *Getin Noble Bank*, C-132/20, EU:C:2022:235, paragraph 117 and the case-law cited).

67 The Court of Justice has also made clear, echoing the case-law of the ECtHR (ECtHR, 8 July 2014, *Biagioli v. San Marino*, CE:ECHR:2014:0708DEC000816213, §§ 72 to 74; see, also, ECtHR, 2 May 2019, *Pasquini v. San Marino*, CE:ECHR:2019:0502JUD005095616, §§ 100 and 101 and the case-law cited), that the term 'established by law' is intended to ensure that the organisation of the judicial system does not depend on the discretion of the executive, but that it is regulated by law emanating from the legislature in compliance with the rules governing its jurisdiction. That phrase thus reflects, in particular, the principle of the rule of law and covers not only the legal basis for the very existence of a tribunal, but also the composition of the bench in each case and any other provision of domestic law which, if infringed, would render the participation of one or more judges in the examination of a case irregular, including, in particular, provisions concerning the independence and impartiality of the members of the court concerned (see judgment of 29 March 2022, *Getin Noble Bank*, C-132/20, EU:C:2022:235, paragraph 121 and the case-law cited).

68 In that context, the Court of Justice has held that a finding that there has been a breach of the requirement for a tribunal previously established by law and relating to the consequences of such a breach was subject to an overall assessment of a number of factors which, taken together, served to create in the minds of individuals reasonable doubt as to the independence and impartiality of the judges (see judgment of 22 February 2022, *Openbaar Ministerie (Tribunal established by law in the issuing Member State)*, C-562/21 PPU and C-563/21 PPU, EU:C:2022:100, paragraph 74 and the case-law cited).

69 Accordingly, the Court of Justice has held that the fact that a body, such as a national council of the judiciary, which is involved in the procedure for the appointment of judges is, for the most part, made up of members chosen by the legislature cannot, in itself, give rise to any doubt as to the independence of the judges appointed at the end of that procedure, but that, however, the situation may be different where that fact, combined with other relevant factors and the conditions under which those choices were made, leads to such doubts being raised (see judgment of 22 February 2022, *Openbaar Ministerie (Tribunal established by law in the issuing Member State)*, C-562/21 PPU and C-563/21 PPU, EU:C:2022:100, paragraph 75 and the case-law cited).

70 Furthermore, in its judgment of 1 December 2020, *Guðmundur Andri Ástráðsson v. Iceland* (CE:ECHR:2020:1201JUD002637418, §§ 207 and 212), the ECtHR held that the appointment of judges by the executive or the legislature is permissible, provided that the appointees are free from influence or pressure when carrying out their adjudicatory role.

71 It follows, in essence, from that case-law that, in order to determine whether the requirements flowing from the second paragraph of Article 47 of the Charter of Fundamental Rights are met, it is necessary not merely to assess the formal nature of the legal instrument establishing a tribunal and defining its operating rules, but to ascertain whether that legal instrument provides sufficient safeguards to ensure its independence and its impartiality vis-à-vis the other branches, in particular vis-à-vis the executive branch.

72 In the second place, it should be borne in mind that, as the Court of Justice held in the judgment in *Schrems I* and in the judgment in *Schrems II*, in the context of an adequacy decision, the Commission is not required to satisfy itself that the relevant provisions of the third country are identical to those in force in the European Union, but that they are essentially equivalent to those guaranteed by EU law by virtue of the GDPR, read in the light of the Charter of Fundamental Rights (see paragraphs 19 and 20 above). It follows that, in the present case, the General Court is required to verify the merits of the

adequacy finding made by the Commission in the contested decision, according to which the provisions of United States law concerning the establishment and functioning of the DPRC afford guarantees essentially equivalent to those laid down by EU law in the second paragraph of Article 47 of that charter. Such guarantees are afforded, in particular, where the legal instrument establishing the tribunal in question and defining its operating rules are intended to ensure its independence and impartiality vis-à-vis the other branches, in particular the executive branch, notwithstanding the fact that, from a formal perspective, that instrument does not constitute a law.

73 In the present case, it is apparent from recital 185 of the contested decision, and is not disputed by the applicant, that the DPRC was established by the Attorney General Order. It follows that the DPRC was constituted not by a law adopted by the legislative branch, namely the United States Congress, but by an act issued by the executive branch. The Attorney General is, indeed, the head of the United States Department of Justice and has primary responsibility for the application of the law within the United States Federal Government. He or she is the principal adviser to the President of the United States on all legal questions and is part of the cabinet of the president.

74 In that context, it is necessary to ascertain whether, in a manner essentially equivalent to EU law, Executive Order 14086 and the Attorney General Order establish safeguards to ensure the independence and impartiality of the DPRC.

75 In that regard, first, it should be noted that it is apparent from the case file, and is not disputed, that:

– the Attorney General adopted the Attorney General Order on the basis of his statutory power to issue binding decisions on questions of United States law, including those relating to the transfer of data from the European Union governed by Executive Order 14086;

– on establishing the DPRC, the Attorney General delegated to it his power to rule on the legality of signals intelligence activities disputed by a citizen of the European Union; the Attorney General is therefore no longer legally authorised to exercise the power delegated, by the Attorney General, to the DPRC as long as the latter exists;

– as stated in footnote 366, on page 63 of the contested decision, the Supreme Court of the United States has recognised that the Attorney General can establish independent bodies with decision-making power, such as the DPRC; in addition, it has held that the delegation of power by the Attorney General to his or her agent is binding on the executive branch; accordingly, it follows from the case-law of the Supreme Court of the United States that, as long as the Attorney General Order remains in force, the executive branch is bound by it and that neither the intelligence agencies nor the Government of the United States can review or revoke its decisions.

76 Second, it should be borne in mind that it is apparent from the contested decision, in essence, that:

– the DPRC judges are appointed by the Attorney General on the basis of the criteria and in compliance with the conditions referred to in paragraph 43 above;

– the DPRC judges can be dismissed only by the Attorney General and solely on the grounds set out in paragraph 56 above, in accordance with the standards applicable to federal judges laid down in the Rules for Judicial Conduct and Judicial Disability Proceedings;

– the decision adopted by the DPRC is binding and final. Accordingly, both the executive branch and the intelligence agencies are required to comply with it;

– the work of the DPRC is subject to oversight by the PCLOB, within the limits indicated in paragraph 54 above.

77 Furthermore, as is apparent from recitals 187 to 189 of the contested decision, the DPRC judges, when carrying out their duties as part of that court, must observe the following procedural guarantees:

– they must examine the complaint concerning personal data as part of a panel composed of three judges, including a presiding judge; for each case, the composition of the three-judge panel is

chosen, on a rotation basis, by the Office of Privacy and Civil Liberties of the Department of Justice, which is responsible for providing administrative support to the DPRC, seeking to ensure that each panel has at least one judge with prior judicial experience;

– when examining the complaint relating to personal data, they are assisted by a Special Advocate appointed by the Attorney General, after consultation with the Secretary of Commerce, the Director of National Intelligence and the PCLOB, for a two-year renewable term; the Special Advocate must have appropriate experience in the field of privacy and national security law, be an experienced attorney and an active member in good standing of the bar; in addition, at the time of their appointment, they must not have been employees of the Executive Branch in the course of the preceding two years; the Special Advocate has access to all information, including classified information, and although he or she does not defend the interests of the complainant and does not have a lawyer-client relationship with that person, the Special Advocate must ensure that, in each case, the complainant's interests are represented and the DPRC judges are well informed on all relevant questions of law and of fact;

– in order to deliver their decision, they must take into account the investigation file, any information and submissions provided by the complainant, the Special Advocate, the intelligence agencies and the CLPO and also, where relevant, any additional information provided by the CLPO at the request of the DPRC;

– they must adopt a decision on the complaint concerning personal data in writing and by a majority of votes.

78 Third, it should be noted that remedies have been provided for the shortcomings identified by the Court of Justice in the judgment in *Schrems II* as regards the absence of guarantees relating to the dismissal, by the executive branch, of the Privacy Shield Ombudsperson and the fact that the latter's decisions were not binding. It is apparent from the case file that Executive Order 14086 limits the situations in which the Attorney General may dismiss the judges of the DPRC and provides that its decisions are to be binding.

79 In that context, the second complaint in the third plea in law must be rejected.

80 That conclusion cannot be called into question by the fact that it is apparent from the case file that, on the same basis as other courts in the United States legal system, the DPRC, although empowered to rule on legal questions, does not constitute a court established under Article III of the Constitution of the United States.

81 In the judgment in *Schrems II*, the Court of Justice held that effective judicial protection could be ensured not only by a court belonging to the judicial order, but also by any other 'body' that offered the persons whose data were transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter of Fundamental Rights (the judgment in *Schrems II*, paragraph 197).

82 In the light of all of the foregoing considerations, the third plea in law must be rejected in its entirety.

3. *The second plea in law, alleging infringement of Articles 7 and 8 of the Charter of Fundamental Rights*

83 By his second plea in law, the applicant claims that the Commission infringed Articles 7 and 8 of the Charter of Fundamental Rights since, in the contested decision, it considered that the United States of America ensured an adequate level of protection with respect to bulk collection of personal data by that country's intelligence agencies.

(a) *Subject matter of the second plea in law*

84 It should be noted that, on pages 2 and 23 of the application and on page 4 of the reply, where he sets out the terms of his second plea, the applicant refers to infringement by the Commission of Articles 7 and 8 of the Charter of Fundamental Rights with respect not only to bulk collection but also to mass

collection of personal data. However, in the discussion that follows the setting out of the terms that plea, the applicant concentrates his arguments solely on bulk collection of personal data.

85 It is apparent from footnote 250, on page 46 of the contested decision, from recital 141 of that decision, without being disputed, and also from the parties' answers to the questions put to them by means of a measure of organisation of procedure and at the hearing, that:

– in the United States, the collection of signals intelligence for national security purposes, including with regard to data transferred from the European Union, may only take the form of 'targeted collection'; that expression is not defined in United States law, but is generally used to describe the collection of intelligence relating to a specific person, a communication account or another identified target carried out by the intelligence agencies pursuant to the Foreign Intelligence Surveillance Act ('the FISA') and Executive Order 14086.

– outside the United States, including where personal data are in transit from the European Union to DPF organisations, the collection of signals intelligence for national security purposes is carried out, primarily, by means of targeted collection; where it is necessary to advance a validated intelligence priority within the meaning of section 2(b)(iii) of Executive Order 14086 which cannot reasonably be achieved by targeted collection, the intelligence agencies may engage in 'bulk collection' of personal data; bulk collection is defined in United States law by section 4(b) of Executive Order 14086 as the authorised collection of large quantities of signal intelligence data that, due to technical or operational considerations, are acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms; bulk collection is governed by Executive Order 14086 and by Executive Order 12333, United States intelligence activities, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008), which impose on it a number of safeguards and limitations;

– the 'mass collection' of personal data to which the Commission refers in footnote 250 of the contested decision as being collection taking place on a generalised and indiscriminate basis is not authorised in the United States and cannot be carried out either within or outside its territory.

86 It follows from the foregoing that, since mass collection is not authorised in the United States and since bulk collection may be carried out only outside the United States, the subject matter of the present plea is limited, in the circumstances of the present case, to determining whether the Commission infringed Articles 7 and 8 of the Charter of Fundamental Rights in respect of the bulk collection, by the United States intelligence agencies, of personal data in transit from the European Union to the DPF organisations, excluding the collection, if any, of personal data carried out on the territory of the European Union by intelligence agencies of the United States or of the Member States.

(b) ***The first complaint in the second plea in law, that intelligence activities carried out pursuant to Section 702 of the FISA are not subject to the safeguards provided for in Executive Order 14086***

87 By the first complaint in his second plea in law, the applicant claims that the Commission infringed Articles 7 and 8 of the Charter of Fundamental Rights since, in the contested decision, it considered, in essence, that the United States of America offered a level of protection essentially equivalent to that guaranteed by EU law by virtue of the GDPR, read in the light of the Charter of Fundamental Rights, in spite of the fact that Section 702 of the FISA permits the United States intelligence agencies to collect in bulk the personal data of nationals of other countries.

88 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

89 It should be noted that Section 702 of the FISA does not authorise bulk collection, but rather only targeted collection, of personal data.

90 It follows that, as Section 702 of the FISA is not concerned with bulk collection of personal data, it has no relevance in the present case.

91 The first complaint in the second plea in law must therefore be rejected.

(c) ***The second complaint in the second plea in law, that Executive Order 14086 does not render bulk collection of personal data subject to prior authorisation by a judicial or administrative authority***

92 By the second complaint in his second plea in law, the applicant claims that the Commission infringed Articles 7 and 8 of the Charter of Fundamental Rights since, in the contested decision, it considered that the United States of America offered a level of protection essentially equivalent to that guaranteed by EU law by virtue of the GDPR, read in the light of the Charter of Fundamental Rights, in spite of the fact that Executive Order 14086 does not establish an obligation on the United States intelligence agencies, before carrying out bulk collection of personal data, to obtain prior authorisation by a judicial or administrative authority.

93 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

94 In the present case, it is apparent from the case file, and is not disputed by the parties, that United States law does not impose an obligation on the intelligence agencies to obtain prior authorisation from a judicial or administrative authority before carrying out bulk collection of personal data in transit from the European Union to the DPF organisations.

95 It is appropriate to establish whether that absence of prior authorisation is capable of affecting the legality of the contested decision because it might call into question the finding in Article 1 of that decision, that the United States of America offers an adequate level of protection for personal data.

96 As a preliminary point, it should be borne in mind that, as the Court of Justice held in the judgment in *Schrems II*, in order to assess the legality of an adequacy decision, it is necessary to determine whether the law of the third country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the GDPR, read in the light of the Charter of Fundamental Rights (see paragraph 19 above).

97 It is in that context that it is necessary to examine the four arguments put forward by the applicant in support of the present complaint.

(1) *The first argument, based on the judgment in* Schrems II

98 By his first argument, the applicant claims, in essence, that, as was true in connection with the Privacy Shield adequacy decision that was annulled by the Court of Justice in the judgment in *Schrems II* owing, in particular, to the failure to provide for judicial review, the bulk collection of personal data carried out, in the present case, by the United States intelligence agencies is not subject to judicial oversight and is not delimited by rules that are sufficiently clear and precise.

99 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

100 It should be noted that, in the judgment in *Schrems II*, the Court of Justice held that Articles 7 and 8 of the Charter of Fundamental Rights contributed to the level of protection required within the European Union, compliance with which must be established by the Commission before it adopts an adequacy decision under Article 45(1) of the GDPR. According to the Court of Justice, any processing of the personal data of a natural person, including the transfer of such data to a third country within the framework of an adequacy decision, affects both the fundamental right of the person concerned to respect for his or her private life, guaranteed in Article 7 of that Charter, and that person's right to the protection of his or her personal data, set out in Article 8 of that charter (the judgment in *Schrems II*, paragraphs 169 to 171).

101 However, the Court of Justice made clear that the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights were not absolute rights, but had to be considered in relation to their function in society (the judgment in *Schrems II*, paragraph 172).

102 Therefore, in accordance with Article 52(1) of the Charter of Fundamental Rights, any limitation on the exercise of the rights and freedoms recognised by Articles 7 and 8 of that Charter must be provided for

by law and respect the essence of those rights and freedoms. Furthermore, 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 (the judgment in *Schrems II*, paragraph 174).

103 In that context, the Court of Justice held that the possibility which Executive Order 12333, as amended, afforded to the United States intelligence agencies to have access to personal data in transit from the European Union, without that access being subject to any judicial review, did not enable the scope of bulk collection of personal data carried out by the intelligence agencies to be delimited in a sufficiently clear and precise manner. Accordingly, it found that that Executive Order did not correlate to the minimum safeguards resulting, under EU law, from the principle of proportionality and that the surveillance programmes based on that order were not limited to what was strictly necessary (the judgment in *Schrems II*, paragraphs 183 and 184).

104 It is appropriate to clarify the interpretation that should be given to the expression 'any judicial review' in paragraph 183 of the judgment in *Schrems II*.

105 In that regard, it should be observed that there is nothing in the judgment in *Schrems II*, in particular in paragraph 183 of that judgment or in the expression 'any judicial review', to suggest that the bulk collection of personal data must necessarily be the subject matter of prior authorisation issued by an independent authority. On the contrary, it is apparent from reading that expression in conjunction with paragraphs 186 to 197 of that judgment that the decision authorising bulk collection must be subject, as a minimum, to an *ex post facto* judicial review.

106 In the present case, as indicated in paragraphs 24 to 82 above, by virtue of Executive Order 14086 and the Attorney General Order the signals intelligence activities carried out by the United States intelligence agencies, including where those agencies carry out bulk collection of personal data, are subject to *ex post facto* judicial oversight by the DPRC, whose decisions are final and binding and must be complied with both by the United States Government and by those agencies. Contrary to the applicant's claims, therefore, it cannot be found that the bulk collection of personal data engaged in by the intelligence agencies on the basis of the contested decision does not satisfy the requirements flowing from the judgment in *Schrems II* in that respect.

107 Furthermore, in the first place, it should be borne in mind that, as is apparent from recital 141 of the contested decision, and is not disputed by the applicant, Executive Order 14086 establishes that the intelligence agencies must give priority to the targeted collection of personal data. Accordingly, bulk collection is authorised only for the purpose of advancing a validated intelligence priority that cannot reasonably be achieved by targeted collection. In that regard, it should be noted that it is apparent from recital 135 of the contested decision that validated intelligence priorities are established through a dedicated process aimed at ensuring compliance with the applicable legal requirements, including those relating to privacy and civil liberties. Specifically, intelligence priorities are developed by the Director of National Intelligence and submitted to the President of the United States for approval. Before proposing intelligence priorities to the President of the United States, the Director of National Intelligence must obtain an assessment from the CLPO for each priority. In the context of that assessment, the CLPO must determine whether the priority in question advances one or more of the legitimate objectives listed in Executive Order 14086, whether it was designed to collect signals intelligence for a prohibited objective and whether it was established after appropriate consideration of the privacy and civil liberties of all data subjects, regardless of their nationality or wherever they might reside.

108 In the second place, it should be observed that, as highlighted by recitals 127 to 131, 134 and 135 of the contested decision, and not disputed by the applicant, Executive Order 14086 sets certain fundamental requirements that apply to all signals intelligence activities, including where they are carried out by means of the bulk collection of personal data.

109 First, signals intelligence activities must be based on statute or presidential authorisation and must be undertaken in accordance with the law of the United States, including its Constitution.

110 Second, signals intelligence activities may be carried out only following a determination, based on a reasonable assessment of all relevant factors, that they are necessary to advance a validated intelligence priority.

111 Third, signals intelligence activities must be carried out in a manner that is proportionate to the validated intelligence priority for which they have been authorised, in order to strike a proper balance between the importance of the intelligence priority pursued and the impact on the privacy and civil liberties of the data subject, regardless of his or her nationality and wherever he or she might reside.

112 Fourth, Executive Order 14086 lists the general objectives that cannot be pursued by signal intelligence activities. They include objectives consisting in fettering criticism, dissent or the free expression of ideas or political opinions by individuals or the press, disadvantaging persons on the basis of their ethnicity, race, gender, gender identity, sexual orientation or religion, or affording a competitive advantage to undertakings established in the United States.

113 In the third place, it is apparent from recital 141 of the contested decision, and is not disputed by the applicant, that Executive Order 14086 establishes specific guarantees that apply to the bulk collection of personal data.

114 First of all, Executive Order 14086 provides that methods and technical measures must be applied in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimising the collection of non-pertinent information.

115 Next, Executive Order 14086 states that bulk collection of personal data can be carried out only in order to meet six specific objectives ('the specific objectives of bulk collection'), namely protection against terrorism, espionage, weapons of mass destruction, cyber threats, threats against the personnel of the United States or its allies and transnational crime. It provides that the President of the United States may update those specific objectives if new national security requirements emerge, such as new threats or increased threats to national security for which the President considers that bulk collection of personal data might be used. Those updates must, in principle, be made public by the Director of National Intelligence, unless the President of the United States considers that making them public would in itself constitute a risk for the national security of the country.

116 Last, Executive Order 14086 provides that any queries of signals intelligence obtained in bulk may be conducted only where necessary to pursue a validated intelligence priority, in pursuit of the specific objectives of bulk collection and in accordance with policies and procedures that appropriately take into account the impact of the queries on the privacy and civil liberties of all data subjects, regardless of their nationality or wherever they might reside.

117 In those circumstances, it cannot properly be maintained that the implementation of bulk collection is not delimited in a sufficiently clear and precise manner.

118 In the light of all those considerations, the present argument must be rejected.

(2) *The second argument, based on the judgment of 6 October 2020,* La Quadrature du Net and Others *(C-511/18, C-512/18 and C-520/18)*

119 By his second argument, the applicant, referring expressly to paragraph 189 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), maintains that the Court of Justice has established the obligation, on intelligence agencies, to obtain prior authorisation from a judicial or administrative authority before collecting connection data from operators holding such data. According to the applicant, bulk collection by the United States intelligence agencies of personal data in transit from the European Union is not, in the circumstances of the present case, subject to such prior authorisation.

120 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

121 It should be observed that, in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court of Justice held, inter alia, that Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11), read in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights, had to be interpreted as not precluding national rules which required providers of electronic communications services to have recourse to the real-time collection of traffic and location data, where such recourse was limited to persons in respect of whom there was a valid reason to suspect that they were involved in terrorist activities and was subject to a prior review carried out either by a court or by an independent administrative body (paragraph 192 of that judgment).

122 It follows that the situation at issue in the case that gave rise to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), differs from that at issue in the present case. In this instance, what falls to be determined is not whether it is necessary that the collection, by electronic service providers, of traffic and location data of users suspected of being involved in one way or another in terrorist activities be made subject to prior review by a judicial or administrative authority, but whether the fact that United States law does not require the intelligence agencies to obtain prior authorisation by a judicial or administrative authority before the bulk collection of personal data in transit to the United States calls into question the validity of the adequacy finding made by the Commission in the contested decision.

123 In those circumstances, it must be concluded that the reference to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), is not relevant in the present case.

124 That conclusion cannot be called into question by consideration of the judgment of 30 April 2024, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (C-470/21, EU:C:2024:370), on which the parties to the present case were invited to comment by way of a measure of organisation of procedure.

125 What was at issue in the case that gave rise to the judgment of 30 April 2024, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (C-470/21, EU:C:2024:370), was the legality of access by a national public authority responsible for the protection of copyright and related rights against infringements of those rights committed on the internet, to the data retained by electronic communications services relating to the civil identity associated with IP addresses for the purpose of combating counterfeiting. Specifically, that access was justified in view of the objective of identifying the holder of an IP address who had engaged in an activity that infringed copyright or related rights, since he or she had unlawfully made protected works available on the internet for downloading by others. In those circumstances, the Court of Justice held that prior review by a court or by an independent administrative body:

– was not required to be put in place where the competent national authority had access to data relating to the civil identity of a person corresponding to an IP address for the sole purpose of identifying the user concerned and without it being possible for those data to be associated with information on the communications made, since the interference entailed by such access could not be classified as serious (paragraphs 133 and 134 of that judgment);

– was required to be put in place before the competent national authority makes a link between the civil identity data of a person associated with an IP address and the file relating to the work unlawfully made available on the internet for downloading by others, and before it sends a letter to the person concerned stating that he or she had engaged in unlawful conduct (see, to that effect, paragraph 141 of that judgment).

126 It follows that the case that gave rise to the judgment of 30 April 2024, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (C-470/21, EU:C:2024:370), concerns access, by the national authorities, to an IP address for the purpose of combating counterfeiting and that that purpose can be distinguished from bulk collection, by the intelligence agencies, of personal data in

transit from the European Union. Accordingly, it cannot be found, in the light of that judgment, that bulk collection, by the United States intelligence agencies, of personal data in transit from the European Union must be subject to prior authorisation.

127 The present argument must therefore be rejected.

(3) *The third argument, based on the judgment of the ECtHR of 25 May 2021,* Big Brother Watch and Others v. United Kingdom *(CE:ECHR:2021:0525JUD005817013)*

128 By his third argument, the applicant claims, in essence, that in the judgment of the ECtHR of 25 May 2021, *Big Brother Watch and Others v. United Kingdom* (CE:ECHR:2021:0525JUD005817013, 'the judgment in *Big Brother Watch*'), the ECtHR held that bulk interception of personal data should be subject to prior authorisation by an independent authority from the time when the objectives and scope of the surveillance operation were defined. According to the applicant, bulk collection by the United States intelligence agencies of personal data in transit from the European Union is not, in the circumstances of the present case, subject to such prior authorisation.

129 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

130 It should be noted that the case that gave rise to the judgment in *Big Brother Watch* concerned, inter alia, the compatibility with Article 8 ECHR of the United Kingdom secret surveillance regime that allowed the intelligence agencies to carry out bulk interception of electronic communications and the related communications data, that is to say, the traffic data relating to the intercepted communications, which took place in principle outside the British Islands.

131 Furthermore, as is apparent from the case-law cited in paragraph 29 above, since Article 8 ECHR, in the same way as Article 7 of the Charter of Fundamental Rights, enshrines the right to respect for private and family life, the case-law of the ECtHR on Article 8 ECHR must be taken into account when interpreting the scope of Article 7 of the Charter of Fundamental Rights. It follows that, should the Court determine that the judgment in *Big Brother Watch* is relevant in the present case, the considerations put forward by the ECtHR in that judgment, as regards the scope of Article 8 ECHR, should be taken into account when interpreting the scope of Article 7 of that charter.

132 In that regard, it should be borne in mind that, in the judgment in *Big Brother Watch*, the ECtHR ruled on the legality of bulk interception by the United Kingdom intelligence services of electronic communications and related communications data that took place in principle outside the British Islands.

133 As the parties to the present case observed in their responses to the measure of organisation of procedure and at the hearing, the arguments put forward by the ECtHR in the judgment in *Big Brother Watch* are relevant in the present case, given that the mass interception of personal data at issue in the case that gave rise to that judgment may be considered to include the bulk collection that forms the subject matter of the contested decision.

134 First, it should be noted that, whereas the French-language version of the judgment in *Big Brother Watch* uses the expression 'interception en masse' of data, the English-language version uses the expression 'bulk interception', which corresponds more precisely to the French concept of 'interception en vrac'.

135 Second, in contrast to targeted interception, the interception of intelligence at issue in the judgment in *Big Brother Watch* was defined by the ECtHR as being that which was not targeted directly at specific individuals and was, consequently, capable of affecting a large number of persons and of related communications data and therefore of having a very wide reach, since it made it possible, inter alia, to collect information in the context of foreign intelligence and to identify new threats from both known and unknown actors. Furthermore, according to the ECtHR, because its aim concerns the protection of national security, bulk interception was generally conducted by the competent authorities in secret, which meant that very little, if any, information about the functioning of the system was made public (see, to that effect, the judgment in *Big Brother Watch*, § 322).

136 Third, in the judgment in *Big Brother Watch*, the ECtHR found that, although bulk interception regimes did not all follow the same model and the ways in which they were implemented might change without always following a strict chronological order, bulk interception was a gradual process which took place, in essence, in the following four stages ('the stages of interception'):

(a) the bulk interception and initial retention of electronic communications belonging to a large number of individuals and related communications data;

(b) the application of specific selectors to the retained communications and related communications data in order to identify the communications likely to be of interest to the intelligence services;

(c) the examination by analysts of the selected communications and related communications data;

(d) the subsequent retention of data and their use for inclusion in an intelligence report, communication to other intelligence services in the country or transmission to foreign intelligence services (see, to that effect, the judgment in *Big Brother Watch*, §§ 325 to 329).

137 It follows that an operation involving bulk collection of personal data, such as that forming the subject matter of the contested decision, falls under the first of the stages of interception identified by the ECtHR in the judgment in *Big Brother Watch*, since it consists in gathering the personal data in transit from the European Union of a large number of individuals for the purpose of protecting national security.

138 In that context, the appropriate inferences should be drawn from the judgment in *Big Brother Watch* for assessment of the legality of an adequacy decision adopted on the basis of Article 45(3) of the GDPR, such as the contested decision.

139 In that regard, in the first place, it should be noted that, in the judgment in *Big Brother Watch*, the ECtHR stated that Article 8 ECHR did not prohibit the use of bulk interception to protect national security or other essential national interests against serious external threats and that States enjoyed a wide margin of appreciation in deciding what type of interception regime was necessary (the judgment in *Big Brother Watch*, paragraph § 347).

140 In the second place, the ECtHR stated that bulk interception of personal data had to be subject to several end-to-end safeguards, which, taken together, constituted the cornerstone of any bulk interception system, namely:

– obtaining authorisation by an independent authority from the time when the object and scope of the surveillance operation in question are being defined (the judgment in *Big Brother Watch*, § 350);

– the establishment of a system of supervision and independent *ex post facto* judicial review (see, to that effect, the judgment in *Big Brother Watch*, §§ 336 and 347);

– the provision of legal rules making it possible to ensure, at each stage of the interception, the necessity and proportionality of the measures being taken (see, to that effect, the judgment in *Big Brother Watch*, § 350); in that regard, the ECtHR recalled that an interference with the rights guaranteed by Article 8 ECHR could be justified under paragraph 2 of that article only if it was in accordance with the law, pursued one or more of the legitimate aims to which that paragraph refers and was necessary in a democratic society in order to achieve those aims; in the context of secret surveillance, the foreseeability of the measures adopted implied that domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities were empowered to resort to any such measures (the judgment in *Big Brother Watch*, §§ 332 and 333).

141 In the third place, the ECtHR stated that, while Article 8 ECHR applied at each stage of the interception, the need to provide safeguards increased as the process moved through the different stages and, consequently, the degree of interference with the right to respect for private life became greater. Thus, according to the ECtHR, it is at the end of the process, where information about a particular

person will be analysed or the content of the communications is being examined by an analyst, that the need for safeguards is greatest (see, to that effect, the judgment in *Big Brother Watch*, §§ 330 and 331).

142 In the fourth place, the ECtHR held that, since it was not feasible in practice to include all the selectors used by the intelligence agencies to filter the communications collected within the perimeter of the prior authorisation, the scope of that authorisation should be limited in order to include at least the types or categories of selectors to be used (the judgment in *Big Brother Watch*, § 354).

143 In the present case, it should be borne in mind that, as the Court of Justice held in the judgments in *Schrems I* and *Schrems II*, the Commission is not required, in an adequacy decision, to satisfy itself that the relevant provisions of the third country are identical to those in force in the European Union, but that they are essentially equivalent (see paragraphs 19 and 20 above).

144 Furthermore, it must be found that, since the bulk collection of personal data by the United States intelligence agencies being challenged in the present proceedings may be treated as equivalent to the interception of data in the context of the first of the stages of interception identified by the ECtHR in the judgment in *Big Brother Watch*, there is a lesser need, for that specific stage of the bulk collection, to provide safeguards that limit the discretion of the intelligence agencies, in view of the context in which the interception is carried out. What is at issue in the present case is solely the initial bulk interception of personal data by intelligence agencies, excluding subsequent activities, which do not form the subject matter of this action, which might consist, where relevant, in the application of specific selectors, examination of the data collected and their subsequent use or disclosure.

145 It follows that a requirement for prior authorisation is not the only safeguard that must accompany bulk interception of personal data, but is one of the elements that, taken together, constitute the cornerstone of any bulk interception regime. In that regard, it should be borne in mind that the United States law in force has legal rules that govern in a sufficiently clear and precise manner the implementation, by the United States intelligence agencies, of bulk collection of personal data (see paragraphs 107 to 116 above) and afford the persons concerned by the transfer of their data the right to an effective judicial remedy before the DPRC (see paragraphs 33 to 63 above). In addition, recitals 162 to 169 of the contested decision state, and it is not disputed by the applicant, that the intelligence activities carried out by the intelligence agencies are overseen by the PCLOB, which, as is apparent from paragraph 54 above, was envisaged by its founding statute as an independent agency. Likewise, those activities are subject to oversight, in the first place, by the legal, oversight and compliance officials within each intelligence agency who are responsible for surveillance and for compliance with that law; in the second place, by the independent Inspector General responsible, for each intelligence agency, for supervising foreign intelligence activities carried out by the agency in question; in the third place, by the Intelligence Oversight Board (United States), created within the President's Intelligence Advisory Board (United States) and required to oversee compliance with the law by the United States authorities; and, in the fourth place, by special committees set up within the United States Congress which perform surveillance functions in relation to all that country's foreign intelligence activities.

146 In the light of those considerations, it cannot be concluded that the fact there is no requirement for prior authorisation applying to initial bulk collection, by the United States intelligence agencies, of personal data in transit from the European Union is sufficient to support a finding that, in the light of the lessons to be drawn from the judgment in *Big Brother Watch*, United States law does not provide safeguards essentially equivalent to those provided for by EU law.

147 The present argument must therefore be rejected.

(4) *The fourth argument, based on Opinion 5/2023 of the European Data Protection Controller*

148 By his fourth argument, the applicant claims that, in its Opinion 5/2023 of 28 February 2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework ('Opinion 5/2023'), the European Data Protection Board ('the EDPB') emphasised the importance of making bulk collection of personal data subject to prior authorisation. According to the applicant, bulk collection by the United States intelligence agencies of personal data in transit from the European Union is not, in the present case, subject to prior authorisation.

149 The Commission, supported by Ireland and the United States of America, disputes the applicant's argument.

150 It should be noted that Opinion 5/2023 was issued by the EDPB on the basis of Article 70(1)(s) of the GDPR. Pursuant to that provision, the EDPB may, on its own initiative or at the Commission's request, provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country.

151 Where it acts on the basis of Article 70(1) of the GDPR, the EDPB acts merely in an advisory capacity by writing opinions, guidelines, recommendations and best practice recommendations which do not have binding legal effect (see, to that effect, order of the President of the Court of Justice of 29 November 2023, *EDPS* v *SRB*, C-413/23 P, not published, EU:C:2023:1036, paragraph 11). Accordingly, that opinion is not binding on the Commission, which remains free to assess whether the law of that country provides, overall, a level of protection essentially equivalent to that guaranteed by EU law as regards bulk collection of personal data. In any event, it should be noted that, in that opinion, the EDPB did not state that the failure to put in place a prior review concerning bulk collection of personal data necessarily undermined the positive assessment, by the Commission, of the adequacy of the level of protection of personal data afforded by the DPF. On the contrary, it observed, in paragraph 165 of its opinion, that that assessment depended on all the circumstances of the case, in particular on the establishment by the United States of America of an *ex post facto* judicial review and a mechanism for redress.

152 In that context, Opinion 5/2023 does not support a finding that bulk collection by the United States intelligence agencies of personal data in transit from the European Union must be subject to prior authorisation and that the protection afforded by the United States is not essentially equivalent to that guaranteed by EU law.

153 The present argument and, accordingly, the second complaint in the second plea in law in its entirety, must therefore be rejected.

(d) ***The third complaint in the second plea in law, that Executive Order 14086 gives the President of the United States power to authorise a secret update of the specific obligations relating to bulk collection***

154 By the third complaint in his second plea in law, the applicant claims that the Commission infringed Articles 7 and 8 of the Charter of Fundamental Rights when it found, in the contested decision, that the United States of America offered a level of protection essentially equivalent to that guaranteed by EU law by virtue of the GDPR, read in the light of that Charter, notwithstanding that Executive Order 14086 gives the President of the United States power, on grounds of national security, to authorise a secret update of the specific objectives of bulk collection. Specifically, he maintains that, contrary to what was held in the judgment of the ECtHR of 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, 'the judgment in *Zakharov*'), the attribution to the President of the United States of power to update those specific objectives does not enable persons concerned by a transfer of personal data to identify precisely the legal framework within which those data are processed in the United States.

155 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

156 It should be noted that, in the judgment in *Zakharov*, the ECtHR held that any interference with the fundamental right to respect for private and family life could be justified under Article 8(2) ECHR only if it was in accordance with the law (the judgment in *Zakharov*, § 227). According to the ECtHR, the expression 'in accordance with the law' meant that the measure at issue had to be accessible to the person concerned and foreseeable as to its effects (the judgment in *Zakharov*, § 228). In the context of the interception of communications, 'foreseeability' did not mean that an individual should be able to foresee when the authorities were likely to intercept his or her communications, but that, in essence, the limitations on that person's right to respect for private and family life had to result from clear rules (the judgment in *Zakharov*, § 229).

157 It should also be borne in mind that, in accordance with the case-law cited in paragraph 29 above, since Article 8 ECHR, in the same way as Article 7 of the Charter of Fundamental Rights, enshrines the right to respect for private and family life, the case-law of the ECtHR on Article 8 ECHR, including, therefore, the judgment in *Zakharov*, must be taken into account when interpreting, as in the present case, Article 7 of that charter.

158 In that regard, it is apparent from Section 2(c)(ii)(C) of Executive Order 14086 that the power conferred on the President of the United States to update the list of specific objectives of bulk collection is not unlimited, but is confined solely to situations in which such an update is necessary due to the emergence of new national security imperatives, such as new or heightened threats to national security, for which bulk collection of personal data might be used. In addition, it is clear from that provision, and was confirmed by the United States of America at the hearing, that the updating of those specific objectives by the President is not secret, but is made public by the Director of National Intelligence, unless the President considers that such publication in itself constitutes a risk for the national security of the United States. Furthermore, even in that situation, bulk collection is subject to all the safeguards and all the limitations provided for in Executive Order 14086 and, if a data subject files a complaint concerning personal data, that complaint will undergo oversight by the CLPO and, where appropriate, review by the DPRC.

159 In that context, it cannot be found that the power conferred on the President of the United States to update the list of specific objectives of bulk collection is contrary to the requirements identified by the ECtHR in the judgment in *Zakharov*.

160 The third complaint in the second plea in law and, accordingly, the second plea in law in its entirety, must therefore be rejected.

4. ***The fourth plea in law, alleging infringement of Article 22 of the GDPR***

161 By his fourth plea, the applicant maintains that the Commission infringed Article 22 of the GDPR since, in the contested decision, it failed to include a provision establishing the right of data subjects not to be subject to decisions based solely on the automated processing of personal data, including profiling, which produce legal effects concerning them or significantly affect them ('wholly automated decisions').

162 As a preliminary point, it should be observed that Article 22 of the GDPR is worded as follows:

'1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by [EU] or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

…'

163 It should also be noted that the term 'profiling', in Article 22(1) of the GDPR, is defined in Article 4(4) of that regulation as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

164 It follows that, according to Article 22 of the GDPR, any data subject is to have the right not to be subject to a decision based solely on automated processing of personal data, including where that measure consists of analysing or predicting certain aspects of his or her behaviour.

165 However, it is apparent from the contested decision that that decision does not specifically address the question of wholly automated decisions.

166 Accordingly, it is necessary to decide whether that omission is capable of affecting the legality of the contested decision, in so far as it might call into question the conclusion set out in Article 1 of that decision that the United States of America ensures an adequate level of protection for personal data.

167 It is in that context that the three complaints put forward by the applicant in support of his fourth plea in law must be analysed, beginning with the first and third complaints, which it is appropriate to examine together.

(a) ***The first and third complaints in the fourth plea in law, according to which (i) the fact that wholly automated decisions are generally adopted by controllers that, since they are established in the European Union, are subject to the GDPR does not provide a guarantee as regards other situations; and (ii) the establishment, by United States law, of sectoral protections in cases where the adoption of wholly automated decisions does not fall within the scope of that regulation is irrelevant in the present case***

168 By the first and third complaints in his fourth plea in law, the applicant maintains, first, that the fact that wholly automated decisions are generally adopted by controllers that, since they are established in the European Union, are subject to the GDPR does not provide a guarantee as regards other situations. Second, he states that the fact that United States law affords sectoral protections in cases where the adoption of such decisions does not fall within the scope of that regulation is irrelevant in the present case, because that circumstance does not permit the conclusion that, in general terms, the protection which the United States provides in relation to all wholly automated decisions is equivalent to that guaranteed by Article 22 of the GDPR.

169 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

170 It should be noted that it is apparent from recital 33 of the contested decision that, in the event of a transfer of personal data from the European Union to the United States, three situations must be distinguished as regards the adoption of wholly automated decisions.

171 First, wholly automated decisions may be adopted by a controller established in the European Union which has collected, in the Union, the personal data of the data subjects. In that regard, it should be noted that Article 4(7) of the GDPR defines 'controller' as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In that situation, since, in accordance with Article 3(1) of the GDPR, the controller is subject to that regulation, that person must comply with the requirements laid down in Article 22 of that regulation as regards such decisions.

172 Second, wholly automated decisions may be adopted either by a processor established in a third country, acting on behalf of the controller established in the European Union that has transferred to that processor the personal data which the controller has collected in the European Union, or by a sub-processor, acting on behalf of the processor established in the European Union which has transferred to that sub-processor the data which the processor has collected in the European Union. In that regard, it should be made clear that Article 4(8) of the GDPR defines 'processor' as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. In those situations, since the foreign processors act on behalf of the controller or processor in the European Union, they are subject to the GDPR pursuant to Article 3(1) of that regulation. Accordingly, in the case of such decisions, the controller and the processor must comply with the requirements laid down in Article 22 of that regulation.

173 Third, wholly automated decisions may be adopted by a controller or a processor not established in the European Union but that contacts data subjects who are in the European Union by offering them goods

or services or by monitoring their behaviour. In that situation, Article 3(2) of the GDPR provides that the foreign controller and processor are to be subject to that regulation. Accordingly, in the case of wholly automated decisions, the controller and processor must comply with the requirements laid down in Article 22 of that regulation.

174 Accordingly, it is apparent from the contested decision that the situations in which wholly automated decisions do not come within the scope of Article 22 of the GDPR are residual and are limited to the case where DPF organisations collect personal data directly, in the European Union, without offering goods or services to EU individuals and without monitoring their behaviour, within the meaning of Article 3(2) of that regulation.

175 It is apparent from recitals 35 and 36 of the contested decision, and is not disputed by the applicant, that, in those situations, United States law offers sectoral protections similar to those provided for by the GDPR in areas such as credit lending, mortgage offers and decisions on recruitment, employment, housing and insurance, in which it is more likely that the DPF organisations will adopt wholly automated decisions.

176 Accordingly, as regards consumer credit, the Fair Credit Reporting Act and the Equal Credit Opportunity Act include guarantees that offer consumers some form of a right to an explanation and a right to contest wholly automated decisions. Those laws apply to a large number of fields such as credit, employment, housing and insurance. In addition, Title VII of the Civil Rights Act and the Fair Housing Act protect natural persons against the models used in wholly automated decisions that might lead to discrimination on the basis of certain characteristics and grant them the right to challenge such decisions. In addition, as regards information relating to health, the rules adopted by the United States authorities pursuant to the Health Insurance Portability and Accountability Act require that medical service providers receive information allowing them to inform individuals of the systems of wholly automated decision-making used in the medical sector.

177 In that context, contrary to the applicant's assertion, it cannot be found that the sectoral protections provided for by United States law are irrelevant in the present case because they do not have the same general scope as Article 22 of the GDPR.

178 In that regard, it should be borne in mind that, in the judgments in *Schrems I* and *Schrems II*, the Court of Justice held that, although not requiring the third country concerned to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' in Article 45(1) of the GDPR had to be understood as requiring that 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 was essentially equivalent to that guaranteed within the European Union by virtue of that regulation, read in the light of the Charter of Fundamental Rights (see paragraphs 19 and 20 above).

179 Furthermore, in the judgment in *Schrems I*, the Court of Justice held that, even though the means to which the third country had recourse for the purpose of ensuring an adequate level of protection of personal data might differ from those employed within the European Union, those means nevertheless had to prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union (see paragraph 20 above).

180 In the light of all those considerations, the first and third complaints in the fourth plea in law must be rejected.

(b) ***The second complaint in the fourth plea in law, that the study commissioned by the Commission in 2018, which showed the residual nature of the situations in which organisations established in the United States that had adhered to the Privacy Shield adopted wholly automated decisions, is irrelevant in the present case***

181 By the second complaint in his fourth plea in law, the applicant maintains that the fact that the study concerning wholly automated decisions, cited in recital 34 of the contested decision, which the Commission had commissioned in 2018 and the results of which appear in section 4.1.5 of the COM(2018) 860 final report from the Commission to the European Parliament and to the Council [of 19 December 2018] on the second annual review of the functioning of the [EU-U.S.] Privacy Shield

('the 2018 study'), concluded that there was no evidence of the existence of wholly automated decisions adopted by organisations established in the United States that had acceded to the Privacy Shield is irrelevant in the present case. Specifically, he claims that that study relates to the Privacy Shield adequacy decision that was annulled by the Court of Justice in the judgment in *Schrems II* and that it does not take account of the current situation, which is characterised by the extremely rapid development of wholly automated services based on artificial intelligence.

182 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

183 It is apparent, inter alia, from the 2018 study, first, that no information supported a finding, at that time, that the undertakings established in the United States that had adhered to the Privacy Shield had adopted wholly automated decisions and, second, that the United States of America had implemented sectoral legislation in areas such as consumer credit, employment, housing, insurance and health, in which there was a greater likelihood that wholly automated decisions would be adopted.

184 In that regard, in the first place, it should be noted that the 2018 study is not cited in the Privacy Shield adequacy decision and was commissioned by the Commission after that decision had entered into force. The fact that that decision was annulled by the Court of Justice in the judgment in *Schrems II* is therefore irrelevant in the present case. Furthermore, in the judgment in *Schrems II*, the Court of Justice did not annul that decision on the basis of the elements set out in that study.

185 In the second place, the 2018 study admittedly did not take into account the factual and legal situation existing in the United States in 2023, on the date of adoption of the contested decision, but the situation existing in 2018, when the study was carried out. However, the residual nature of the situations in which organisations established in the United States which had adhered to the Privacy Shield had adopted wholly automated decisions was confirmed by the COM(2019) 495 final report from the Commission to the European Parliament and the Council [of 23 October 2019] on the third annual review of the functioning of the [EU-U.S.] Privacy Shield. In that report, it was stated, inter alia, that the number of organisations established in the United States participating in the Privacy Shield that had adopted wholly automated decisions was limited and that the decisions taken by those organisations generally did not have legal effects and did not have other effects on data subjects.

186 In the third place, it should be noted that, in his written submissions, the applicant has adduced no evidence to support a finding that, after the 2018 study had been carried out, organisations established in the United States have adopted wholly automated decisions, and has not set out to the requisite legal standard the reason why the development of artificial intelligence purportedly renders that study irrelevant.

187 In that context, the second complaint in the fourth plea in law and, accordingly, the fourth plea in law in its entirety, must be rejected.

5. *The fifth plea in law, alleging infringement of Article 32 of the GDPR, read in conjunction with Article 45(2) of that regulation*

188 By his fifth plea in law, the applicant claims that the Commission infringed Article 32 of the GDPR, read in conjunction with Article 45(2) of that regulation, since, in the contested decision, it considered that the United States of America afforded a level of protection essentially equivalent to that guaranteed in the European Union as regards the implementation, by controllers and processors established in the United States, of adequate technical and organisational measures aimed at ensuring the security of the processing of personal data transferred from the European Union to the United States.

189 In that regard, in the first place, the applicant claims that Section II.4.(a) of Annex I to the contested decision provides merely that DPF organisations must take reasonable and appropriate security measures only when creating, maintaining, using or disseminating personal data. Accordingly, no security measure is required when those organisations consult personal data from the European Union. The applicant maintains that consultation is nevertheless among the operations included in the concept of the 'processing' of personal data set out in Article 4(2) of the GDPR.

190 In the second place, the applicant maintains that Section III.6(f) of Annex I to the contested decision provides that organisations established in the United States which leave the DPF are required to continue to comply with the principles set out in that decision, including those relating to the security of processing, for as long as they store, use or disclose personal data transferred from the European Union to the United States, but does not establish such an obligation where those organisations consult personal data.

191 The Commission, supported by Ireland and by the United States of America, disputes the applicant's arguments.

192 As a preliminary point, first of all, it should be borne in mind that Article 32 of the GDPR is worded as follows:

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability [of] and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

…'

193 Next, the term 'processing', contained in Article 32 of the GDPR, is defined in Article 4(2) of that regulation as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

194 According to the case-law, it is apparent in particular from the expression 'any operation', in Article 4(2) of the GDPR, that the EU legislature intended to give the concept of 'processing' a broad scope, which is corroborated by the non-exhaustive nature, expressed by the phrase 'such as', of the operations listed in that provision (see judgment of 7 March 2024, *Endemol Shine Finland*, C-740/22, EU:C:2024:216, paragraph 29 and the case-law cited).

195 Last, it should be noted that, the elements which the Commission must take into account when it assesses, under Article 45(2)(a) of the GDPR, the level of protection afforded by a third country, include the security measures relating to personal data implemented by that country.

196 That is the context in which it is appropriate to examine, together, the two arguments raised by the applicant in support of the present plea in law.

197 In that regard, it should be borne in mind that Section II.4(a) of Annex 1 to the contested decision is worded as follows:

‘Organisations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.’

198 Furthermore, Section III.6(f) of Annex I to the contested decision is worded as follows:

‘An organisation must subject to the Principles all personal data received from the EU in reliance on the [DPF]. The undertaking to adhere to the Principles is not time limited in respect of personal data received during the period in which the organisation enjoys the benefits of the [DPF]; its undertaking means that it will continue to apply the Principles to such data for as long as the organisation stores, uses or discloses them, even if it subsequently leaves the [DPF] for any reason. …’

199 It follows that Sections II.4(a) and III.6(f) of Annex I to the contested decision do not concern the processing in any form of personal data, within the meaning of Article 4(2) of the GDPR. On the contrary, Section II.4(a) limits the obligation of the DPF organisations to adopt security measures solely to situations in which they create, manage, use or disseminate personal data. Furthermore, Section III.6(f) provides that organisations that leave the DPF must continue to apply the principles set out in the contested decision as long as they store, use or disclose personal data transferred from the European Union to the United States.

200 First, it should be borne in mind that, in the judgments in *Schrems I* and *Schrems II*, the Court of Justice held that it was not necessary for the third country to ensure legal protection identical to that guaranteed in the EU legal order (see paragraphs 19 and 20 above). It follows that while, in the contested decision, the Commission finds that the United States law in force at the time when that decision was adopted ensures a level of protection essentially equivalent to that established in EU law, it is not necessary that that decision should contain exactly the same terms as those that appear in the GDPR.

201 Second, the principles set out in Section II.4(a) of Annex I to the contested decision must be interpreted in the light of the elements set out in recital 23 of that decision, which, in a similar manner to Article 32 of the GDPR, provides as follows:

‘Personal data should also be processed in a manner that ensures [their] security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. To that end, controllers and processors should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art, related costs and the nature, scope, context and purposes of processing, as well as the risks for the rights of individuals.’

202 Third, it should be observed that the terms ‘create’, ‘maintain’, ‘use’ and ‘disseminate’ in Section II.4(a) of Annex I to the contested decision, and the terms ‘store’, ‘use’ and ‘disclose’ in Section III.6(f) of that annex are specific manifestations of the operation consisting in the ‘processing’ of personal data within the meaning of Article 32 of the GDPR, and that, in the same way as that term, they are intended to cover a wide range of operations relating to personal data.

203 Fourth, the term ‘use’, which occurs in both Section II.4(a) of Annex I to the contested decision and in Section III.6(f) of that annex, is defined as having recourse to something with a specific aim or for a specific use. From that perspective, the use of personal data includes consultation of those data since, in order to be able to have recourse to data, it is necessary first to have access to them and therefore to consult them. It follows that the applicant’s argument that no security measure is required in the contested decision when DPF organisations consult personal data originating in the European Union is unfounded.

204 In the light of all those elements, the fifth plea in law must be rejected and, accordingly, the action must be dismissed in its entirety.

IV. **Costs**

205 Under Article 134(1) of the Rules of Procedure, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings.

206 As the Commission has applied for costs and the applicant has been unsuccessful, he must be ordered, in addition to bearing his own costs, to pay those incurred by the Commission, including in the interlocutory proceedings.

207 Furthermore, under Article 138(1) of the Rules of Procedure, the Member States and institutions which have intervened in the proceedings are to bear their own costs. Consequently, Ireland shall bear its own costs.

208 In addition, under Article 138(3) of the Rules of Procedure, the General Court may order an intervener other than those referred to in paragraphs 1 and 2 of that article to bear its own costs. In the present case, the United States of America must be ordered to bear its own costs.

On those grounds,

THE GENERAL COURT (Tenth Chamber, Extended Composition)

hereby:

1. **Dismisses the action;**

2. **Orders Mr Philippe Latombe to bear his own costs and to pay those incurred by the European Commission, including in the interlocutory proceedings;**

3. **Orders Ireland to bear its own costs;**

4. **Orders the United States of America to bear its own costs.**

Porchia Jaeger Madise

Nihoul Verschuur

Delivered in open court in Luxembourg on 3 September 2025.

[Signatures]

---

* Language of the case: French.