European Journal of Risk Regulation (2024), **15**, 191–200
doi:10.1017/err.2023.67

CAMBRIDGE UNIVERSITY PRESS

REPORTS

EU–US Data Privacy Framework: A First Legal Assessment

Sergi Batlle[1] and Arnaud van Waeyenberge[2]

[1]GEIE GECOTTI-PE, Lille, France and [2]HEC Paris, Jouy-en-Josas, France
Corresponding author: Arnaud van Waeyenberge; Email: van-waeyenberge@hec.fr

Abstract

The purpose of this contribution is to briefly present the content of the EU–US Data Privacy Framework recently adopted by the European Commission and then to assess whether it meets the expectations expressed by the Court of Justice of the European Union in its Schrems II judgment and related case law.

Keywords: Data Privacy Framework; data protection; Privacy Shield

European data protection law requires that the protections provided for in the European Union (EU) follow the personal data of citizens wherever those data go, and it is the responsibility of the data controller to ensure that this is the case in accordance with the mechanisms and modalities provided for this purpose in the General Data Protection Regulation (GDPR).[1] After a thorough examination of its legislation and international commitments, the European Commission may find by means of an "adequacy decision"[2] that a third country ensures an adequate level of protection for data subjects established in the Union; in particular, they must have enforceable rights and effective remedy, complemented by appropriate safeguards ensuring a level of protection that, if not identical, is at least substantially equivalent to that provided by EU law. In the absence of such an adequacy decision, the transfer of data to this third country can only take place if the "exporter" of these data established in the Union provides appropriate safeguards[3] or, failing that, under the other conditions provided for in the GDPR.[4]

[1] Art 24 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 – hereafter "GDPR") – OJ L 119 of 4.5.2016, p 1 " . . . the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation . . . ".

[2] Art 45 GDPR.

[3] According to Art 46 GDPR, these safeguards may be provided namely by binding corporate rules approved by a competent supervisory authority or by standard data protection clauses approved by a competent supervisory authority or by the Commission. Currently, the latest version of these standard data protection clauses are those approved by the Commission in its decision of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council – OJ L 199 07.06.2021, p 31.

[4] Art 49 GDPR.

Until 2020, transfers from the EU to the USA were covered by the Commission's 2016 partial adequacy decision, the so-called "Privacy Shield".[5] However, this adequacy decision was annulled by the Court of Justice of the European Union (CJEU)[6] following a complaint lodged by Maximilian Schrems with the Irish Supervisory Authority seeking to prohibit the transfers of his personal data from Facebook Ireland to servers belonging to Facebook, Inc., located in the USA.[7] The Irish authority initiated proceedings before the High Court to ask the latter to submit a preliminary ruling request to the CJEU on, among other things, the validity of the "Privacy Shield" decision. Following this reference for a preliminary ruling, the Commission's "Privacy Shield" adequacy decision was annulled by the CJEU on 16 July 2022 ("Schrems II judgment"). The Court found that, contrary to the Commission's assertion in its decision, the limitations on data protection arising from the US domestic regulations "are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law . . . ",[8] and that the judicial protection mechanism provided for in the "Privacy Shield", in this case a mediation mechanism, did not provide " . . . any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter".[9]

This decision goes against the European Data Strategy, in addition to putting at risk an economic relationship estimated to be valued at approximately 7 billion euros.[10] The Commission therefore launched a drive to address the criticisms levelled by the CJEU.

The first steps towards a new adequacy decision were taken in March 2022 with an agreement in principle between the European Commission and the USA.[11]

On 7 October 2022, the White House adopted Executive Order 14086 "Enhancing safeguards for United States signals intelligence activities" (hereinafter "EO 14086"),[12] which is intended to provide additional safeguards and guarantees regarding the

[5] Decision 2016/1250 on the adequacy of the protection provided by the EU–US Data Protection Shield – OJ L 207 pf 1.8.2016, pp 1–112.

[6] CJEU, "Schrems II" judgment of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559. For an analysis of the case, see, among many others, M Rotenberg, "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection" (2020) 26 European Law Journal 141; M Zalnieriute and G Churches, "Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance" (2021) 80(1) Cambridge Law Journal 8.

[7] This saga started with the Schrems I ruling (Case C-362/14 Maximillian Schrems v Data Protection Commissioner of 6 October 2015, ECLI:EU:C:2015:650) under the previous data protection Directive 95/46/EC of 24 October 1995. In the Schrems I ruling, the Court invalidated the so-called "Safe Harbour" EC Decision of 26 July 2000 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 (2000/520/EC). The Court found that – unlike Commission assertions – the Safe Harbour Scheme did not provide a level of protection for fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in light of the Charter. The Court pointed out that a "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded *as compromising the essence of the fundamental right* to respect for private life, as guaranteed by Article 7 of the Charter" (point 94, emphasis added), declared the Safe Harbour Decision invalid and required the Irish Data Protection Commissioner to examine Mr Schrems' complaint, and it eventually suspended the transfer of data of Facebook's European subscribers to Facebook servers located in the USA.

[8] See para 185, "Schrems II", supra, note 6.

[9] See para 197, "Schrems II", supra, note 6. For an analysis post-Schrems II, see G Voss, "Transatlantic Data Transfer Compliance" (2022) 28 Boston University Journal of Science and Technology Law 158.

[10] M Zalnieriute, "Data Transfers after Schrems II: The EU–US Disagreements Over Data Privacy and National Security" (2022) 55(1) Vanderbilt Journal of Transnational Law 1; D Hamilton and J Quinlan, *The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe* (Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network 2023) p II.

[11] Press release of 25 March 2022 <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087>.

[12] Executive Order (EO) 14086 of 7 October 2022, on Enhancing Safeguards for United States Signals Intelligence Activities, Sec. 2. Signals Intelligence Activities <https://www.state.gov/executive-order-14086-policy-and-procedures/#:~:text=14086%20of%20October%207%2C%202022,defined%20as%20countries%20and%20regional>.

limitations on the protection of European citizens' data arising from the intelligence activities of US intelligence agencies. In addition to this decision, on 14 October 2022, the US Department of Justice adopted the regulation creating the Data Protection Review Court (DPRC). Finally, the previous EU–US Data Privacy Framework (DPF) was updated.

On 13 December 2022, the European Commission launched the process of adopting a new adequacy decision for the DPF, which will promote transatlantic data flows and address the concerns raised by the CJEU in its 2020 Schrems II judgment.[13]

On 28 February 2023, the European Data Protection Board (EDPB) adopted Opinion 05/2023 on the draft implementing decision.[14] The EDPB's assessment raised some concerns regarding the rights of data subjects, the newly created DPRC's independence in practice and the lack of clarity surrounding some aspects of EO 14086. However, in contrast to the European Parliament, the EDPB's assessment does not seem to consider that the DPF "per se" fails to provide the essential safeguards to ensure that interference with the right to privacy and the protection of personal data by surveillance measures when personal data are transferred does not go beyond what is necessary and proportionate in a democratic society,[15] and thus it called on the Commission to closely monitor the implementation of the DPF in practice.

On 11 May 2023, the European Parliament adopted a resolution on the adequacy of the protection afforded by the DPF.[16] The European Parliament concluded that the "EU–US Data Privacy Framework fails to create essential equivalence in the level of protection",[17] and it called on the Commission not to adopt the adequacy decision in that state.

On 10 July 2023, the European Commission formally adopted the draft decision unchanged.[18]

The purpose of this contribution is to briefly present the content of the DPF recently adopted by the European Commission (Section I) and then to assess whether it meets the expectations expressed by the CJEU in its Schrems II judgment and related case law (Section II).[19] Section III concludes.

[13] European Commission, 13 December 2022, Questions & Answers: EU–US Data Privacy Framework, draft adequacy decision <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632>.

[14] EDPB 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" <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en>.

[15] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures adopted on 10 November 2020 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>. These recommendations were adopted following the CJEU Schrems II judgment and can be summarised as the provision of four essential guarantees: (1) processing should be based on clear, precise and accessible rules; (2) necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; (3) an independent oversight mechanism should exist; and (4) effective remedies need to be available to the individual.

[16] European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU–US Data Privacy Framework (2023/2501(RSP)): <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html>.

[17] ibid, point 19 of the conclusions. The European Parliament considers EO 14086 not to be sufficiently robust for providing a level of protection substantially equivalent to that guaranteed in the EU.

[18] Commission implementing decision of 10.7.2023 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, C(2023) 4745 final <https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf>.

[19] For a critical assessment, see L Drechsler, A Elbi, E Kindt et al, "Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States" CiTiP Working Paper 2023 <https://ssrn.com/abstract=4477120>; M Tzanou and P Vogiatzoglou, "In Search of Legal Certainty Regarding 'Effective Redress' in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements" (2023) 16 Review of European Administrative Law 11.

I. Essential elements of the DPF

The DPF adequacy decision takes the form of a Commission implementing act. As mentioned previously, it has been subject to a non-binding opinion of the European Data Protection Supervisor (EDPS)/EDPB, before then being adopted according to the principles and rules of the "comitology" review procedure.[20]

At least three key elements of the DPF merit analysis, which will be discussed in the following subsections.

1. Mechanism for certification and adherence to the principles of the DPF

It should be made clear from the outset that this is a partial adequacy decision, in the sense that it is not intended to cover the processing of personal data by all US organisations and operators, but only those that voluntarily adhere to the DPF principles as issued by the US Department of Commerce (DoC) and complete the self-certification process.[21] This certification attests to compliance with seven core principles and sixteen additional principles. This is essentially a correlation of the principles listed in Chapter II of the GDPR and related articles, from which the rights of data subjects and the obligations of operators flow. These basic principles are those of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, data access and recourse, liability and effective enforcement of regulation. The additional principles deal with specific subjects, such as data relating to human resources or exceptions relating to journalism.[22]

To be eligible for certification, operators must also be subject to the investigative and remedial powers of the US Federal Trade Commission (FTC) or Department of Transportation (DoT). Oversight of the certification scheme is provided by the US DoC, which may require certified operators to re-certify on an annual basis. The FTC or the DoT, as the case may be, performs the functions of the Control Authority[23] with regard to the handling of complaints by data subjects, the powers of investigation and the imposition of remedies or sanctions in cases where the amiable dispute resolution or arbitration mechanisms provided for in the DPF would not have sufficed.[24]

2. Additional safeguards and guarantees regarding the limitations on the data protection of European citizens arising from the intelligence activities of US intelligence agencies

This second element of the DPF is the US government's response to the first requirement of the Schrems II judgment,[25] in particular the criticism that had been expressed by the CJEU regarding Presidential Policy Directive 28 (PPD-28) adopted under the Obama

[20] See Arts 45.2 and 93.2 of the GDPR and Art 5 of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers – OJ L 55 of 28.2.2011, pp 13–18.

[21] Interested organisations initiate the self-certification process, although the DoC will only place an organisation on the DPF list after having determined that the initial self-certification submission is complete. The DoC shall remove an organisation from the list if it fails to complete its annual re-certification or if it persistently fails to comply with the DPF principles.

[22] See Annex I of Commission implementing decision of 10.7.2023, supra, note 18.

[23] This is a simplification for the purposes of the report, as the competences, tasks and powers attributed in Chapter VI of the GDPR to the Supervisory Authorities in the EU are here divided between the DoC, the FTC and the DoT, among others.

[24] For more details, see paras 64–85 of the decision mentioned supra, note 18.

[25] See para 185, "Schrems II", supra, note 6.

administration[26] that it did not sufficiently regulate the limitations on data protection for Europeans. President Biden's EO 14086 replaces PPD-28, which is partially revoked.[27] It should be noted that, like the previous order, the current one does not contain a definition of the intelligence activities that fall within its scope.

Section 2 of the order lists twelve legitimate objectives that intelligence activities may pursue and four prohibited objectives, the latter relating to the protection of freedom of expression, of the press and of legitimate privacy interests, the right of access to legal counsel or ethnic, racial, gender, sex or religious discrimination. It should also be noted that a status distinct from these prohibited objectives is granted to the collection of information or business secrets of foreign companies to provide a competitive advantage to US companies. Indeed, while it is expressly characterised as a "non-legitimate objective", it is not defined as a prohibited one. The order even states that it can be a legitimate objective when it is "to protect the national security of the United States or of its allies and partners", a generic term if ever there was one.[28]

The order introduces the principles of "necessity", "proportionality" and the "oversight" of intelligence activities, assessed against pre-approved intelligence priorities (which represent classified information, yet much of which can be deduced from publicly available reports). The factors for assessing these principles are not exhaustively defined, but the order particularly mentions the nature of the pursued objective, the impacts of the measures on third parties, their duration, the sensitivity of the data to be collected and the safeguards afforded to the information collected. The order also reinforces the application of these principles in the case of mass surveillance, which is subject to additional safeguards.[29]

It should be noted, however, that while this order establishes guidelines and principles to be respected in intelligence activities, it in no way modifies existing intelligence legislation, in particular the Foreign Intelligence Surveillance Act (FISA) and its Section 702, which allows, under certain conditions, targeted surveillance of non-US citizens abroad.[30]

3. *Creation of a two-layer redress mechanism*

The aim here is to meet the second requirement of the Schrems II judgment, which affirmed the need for "... cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter".[31] This third element of the DPF therefore establishes a dual administrative body, but a priori without the possibility of a judicial remedy as such.

The complaint is first reviewed by the Civil Liberties Protection Officer (CLPO), who is appointed by and reports to the Director of National Intelligence. This decision may subsequently be appealed administratively and reviewed by the newly created Data Protection Review Court, which is composed of judges from outside the administration appointed by the US Attorney General.[32]

[26] Presidential Policy Directive 28 – Signals Intelligence Activities, 17 January 2004 <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[27] National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, 7 October 2022 <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>.

[28] EO 14086, supra, note 12.

[29] EO 14086, sub-section c "Privacy and civil liberties safeguards", point ii "Bulk collection of signals intelligence", supra, note 12.

[30] Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.).

[31] See para 197, "Schrems II", supra, note 6.

[32] The Data Protection Review Court (DPRC) is established by the Department of Justice Regulation of 14 October 202, 87 FR 62303, pp 62303–08 <https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court>.

The system is limited to "qualifying complaints" transmitted by public authorities of a "qualifying state". With regard to the latter term, the order provides that, in addition to a state, it may correspond to "a regional economic integration organization" (the EU comes to mind, of course), and that this designation is awarded by the US Attorney General, taking into account several criteria, including the fact that this designation "advances the national interests of the United States".[33] In addition, the CLPO's response neither confirms nor denies that the complainant has been subjected to US intelligence activities, and it will be limited to stating (1) that no violation has been found or, conversely, that the CLPO has requested the implementation of appropriate measures (without specifying which violation), (2) that the complainant may appeal to the Data Protection Review Court and (3) that, if necessary, a special attorney will be chosen by the court to represent the complainant's interests. The grounds for the CLPO's decision remain classified in any event.[34]

II. Towards a Schrems III?

While the self-certification mechanism does not pose any particular problem, as it is a simple update of the pre-existing system from the previous Privacy Shield, which had not raised any major criticisms from the CJEU in the Schrems II judgment, this is not the case with points (2) and (3) that we mentioned. Although these represent real steps from the USA towards our system of fundamental rights, legal questions nevertheless remain.

1. Are the additional safeguards provided by EO 14086 sufficient?

With respect to the second key element of the DPF, regarding the additional safeguards provided by EO 14086, the first issue that arises is the choice of instrument: it is an administrative act with binding effect for the various departments of the federal administration, which therefore includes the intelligence services. While it can be amended by the President without Congressional intervention, logically it cannot amend other laws concerning intelligence activities, such as FISA and its Article 702, which authorises the targeted surveillance of non-US citizens abroad.

The compatibility of the text with the EU Charter of Fundamental Rights is questionable in two respects. First is whether the interpretation of the principles of "necessity" and "proportionality" set out in EO 14086 is in a manner compatible with Articles 7 and 52 of the Charter (and Article 8 of the European Convention on Human Rights; ECHR). Furthermore, the Charter provides that any limitation on the exercise of fundamental rights must be provided for by law[35] (ie "the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned"[36]). Here, the legal basis (eg FISA) remains unchanged.

To fully and unambiguously comply with this requirement, it would most likely have been necessary to amend the problematic sections of FISA by law to add a definition of the "scope of the limitation on the exercise of the right concerned" with respect to, for example, the targeted surveillance of non-US citizens abroad.[37]

[33] "Qualifying complaint" and "qualifying state" are defined in sections 4(k) and 3(f), respectively, of EO 14086, supra, note 12.

[34] EO 14086, section 3, supra, note 12.

[35] Art 52 of the Charter of Fundamental Rights.

[36] See para 175 of the Schrems II judgment, supra, note 6, and the case law cited there.

[37] This is still the position of the European Parliament. See, eg, European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), Case C-311/18 (2020/2789(RSP)), and, more recently, the draft motion for a resolution of the Committee on Civil Liberties, Justice and Home Affairs on the adequacy of the protection afforded by the EU/US Data Privacy Framework of 14 February 2023 (2023/2501(RSP)).

However, the term "law" should not be interpreted in its formal sense; it could include, for example, regulatory measures,[38] provided that the rule is "legally binding under domestic law".[39]

The Court in Schrems II found that Article 702 of FISA did not, on its own, satisfy the proportionality requirement of Article 52(1) of the Charter because it did not set "any limits on the powers it granted"[40] and because the previous PPD-28 did not set out "clear and precise rules on the scope of the measure and minimum safeguards".[41] In addition, the previous PPD-28 did not provide data subjects with "actionable" rights before the courts against the US authorities.[42]

The remedies that the DPF implements and the consequences of non-compliance by intelligence agencies with the guidelines it sets should be made clearer. The Commission's decision mentions the existence of the Foreign Intelligence Surveillance Court (FISC), whose decisions can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR). These courts deal with requests for surveillance warrants from US intelligence services. However, the guarantees offered by this system are questionable: historically, the FISC has refused only twelve warrant applications out of the 33,942 it has received since its creation in 1978, and the first appeal to the FISCR of such a rejection only occurred in 2002, twenty-four years later. In view of the lack of enthusiasm displayed by the FISC, but also of its case law,[43] the CJEU is unlikely to be convinced by this system. Moreover, the extreme lack of transparency of these courts and their procedures makes it almost impossible to independently assess their effectiveness today.[44]

2. *Between the issues of the independence of the DPRC and the lack of judicial review, how robust is the DPF's two-layer redress mechanism?*

The third key element of the new DPF is the creation of a two-layer redress mechanism.[45] The question here is whether the absence of a *judicial* remedy can be regarded as prohibitive by the CJEU, or whether an administrative remedy can be regarded by the CJEU as offering guarantees "substantially equivalent" to those of the EU under Article 47 of the Charter. In other words, the question is whether the DPRC fulfils the criteria of independence and impartiality required by Article 47 of the Charter.

As to whether the right to an effective remedy – as defined in Article 47 of the Charter (and Articles 6 and 13 of the ECHR) – can be satisfied by an administrative body, the CJEU in Schrems II first stated that "... data subjects must have the possibility of bringing legal action before an *independent and impartial court* ...".[46] Later, however, in recital 197, the Court recognises that effective judicial protection can also be ensured by a "body" offering guarantees substantially equivalent to those of the EU under Article 47 of the Charter. In

[38] As long as the norm is "adequately accessible and formulated with sufficient precision"; see ECtHR, Sunday Times v UK (No 1), 26 April 1979.

[39] C-623/17, Privacy International, ECLI:EU:C:2020:790, point 68.

[40] For a detailed review of the relationship between proportionality and the "respect for the essence test" in light of the CJEU case law, see K Lenaerts, "Limits on Limitations: The Essence of Fundamental Rights in the EU" (2019) 20 German Law Journal 779–93.

[41] Para 180 of "Schrems II", supra, note 6.

[42] Para 181 of "Schrems II", supra, note 6.

[43] *Mutatis mutandis*, see also Privacy International, C-623/17, supra, note 39, para 44: "... according to the settled case-law of the Court, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law".

[44] For more details, see points 135 et seq. of the abovementioned Commission decision, supra, note 18.

[45] This two-layer redress mechanism is described in sections c) and d) of EO 14086, supra, note 12.

[46] "Schrems II", supra, note 6, point 194 (emphasis added).

addition, the European Court of Human Rights (ECtHR)[47] has often accepted that various specialised, non-judicial bodies can be regarded as courts in the European sense of the term.[48] Moreover, what seem to be important for the ECtHR in relation to Article 13 ECHR[49] are "the powers and procedural guarantees an authority possesses" rather than the judicial nature of the authority.[50]

On the issue of independence, the CJEU had pointed out in Schrems II, with regard to the mediation system proposed in the Privacy Shield, that there was "nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman's independence from the executive …".[51] EO 14086 mentions that the newly created DPRC acts independently and also lists the conditions for the dismissal of judges; the latter do not report to the Attorney General and are not subject to their supervision or hierarchical relationship.[52] As for their impartiality, EO 14086 specifies that "judges" may not combine the function of DPRC judge with other duties, including within the state administration, among other guarantees. This was also noted by the EDPB in his opinion, which emphasised and approved this strong reinforcement of the DPRC's independence guarantees, albeit with some reservations.[53] Finally, there is the question of the effective powers of the DPRC as recalled by the ECtHR in the aforementioned Klass judgment.[54] EO 14086 indicates that the decisions taken by the CLPO and the DPRC have "binding effect" and are intended to "fully redress" any identified violation; moreover, the decisions of the DPRC must be reasoned.[55] The new mechanism thus displays several important improvements and considers the ruling of the CJEU. Nevertheless, we believe that these guarantees will not be sufficient to meet the expectation of paragraph 195 of the Schrems II case. One of the reasons for this is that the appointment procedure remains exclusively in the hands of the executive, since the "judge" is appointed by "the Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB [US Privacy and Civil Liberties Oversight Board]",[56] and this can legitimately cast doubt on its true independence from the executive.[57] In the EU, the protection of personal data is a fundamental right, and the guarantees surrounding this issue (including Article 47 of the Charter, among others) must be in line with the importance given to it in law. If we add to this the fact that EO 14086 does not define the intelligence activities that fall within its

[47] According to Art 52(3) of the Charter, the meaning and scope of the rights guaranteed in the Charter are the same as in the ECHR. However, the Charter may provide more extensive protection.

[48] Eg ECtHR, 28 June 1984, Campbell and Fell v. UK, no. 7819/77.

[49] Art 13 ECHR stipulates that "[e]veryone whose rights and freedoms as set forth in the Convention are violated shall have an effective remedy before a national authority".

[50] See ECtHR, judgment of 6 September 1978, Klass and others v. Germany, n°5029/71. In para 67, *in fine* the ECtHR stated that "[i]n the Court's opinion, the authority referred to in Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective."

[51] Para 195 *in fine* of "Schrems II", supra, note 6.

[52] The two main criteria of independence from the executive have been clarified by the Strasbourg Court: on the one hand, independence is preserved when judges are appointed to sit in an individual capacity and cannot receive instructions from public authorities; what are important are the guarantees offered to judges during their term of office, in particular security of tenure. On the other hand, the second criterion concerns the existence of safeguards against external pressure and the appearance of independence (for more details, see ECHR, 22 October 1984 Sramek v. Austria, n°8790/79 and ECHR, 18 June 1971, De Wilde, Ooms and Versyp v. Belgium, no. 2832/66; 2835/66; 2899/66).

[53] See point 3.2.4 of the EDPB opinion 5/2023, supra, note 14.

[54] Supra, note 50.

[55] For more details, see EO 14086, sections 3.C (ii) and 3.D (ii), supra, note 12, and Attorney General regulation of 7 October 2022 establishing the DPRC.

[56] EO 14086 section 3.D (i)(A), supra, note 12.

[57] For an analysis of this point, see A Savin, "The New Framework for Transatlantic Data Transfers", CBS LAW Research Paper No. 23-01, p 12 <https://ssrn.com/abstract=4494289>.

scope and that the "decree" instrument does not offer a sufficient level of legal certainty due to its non-legislative nature, it is reasonable to suggest that the new system will not pass through the review that the CJEU will likely be carrying out unscathed. However, additional limits and safeguards, as described above, have been agreed upon, and it is not entirely out of the question that these could be considered sufficiently clear and precise so as to meet the "substantially equivalent" requirements ensuring, at least formally, an adequate level of protection within the meaning of Article 45 of the GDPR. In this case, the redress mechanism needs to demonstrate *in practice* that it offers EU data subjects guarantees essentially equivalent to those required by Article 47 of the Charter. It is therefore essential for the Commission to monitor these developments on an ongoing basis and – if necessary – repeal, amend or suspend the decision in accordance with Article 45(4) and (5) of the GDPR.

III. Conclusion

It is always difficult to predict the rulings of the CJEU. However, in our view, the new mechanism only partially complies with the case law of the Court of Justice. Progress has clearly been made, although several "stumbling blocks" – identified in Section II of this article – remain, and it seems unlikely that European judges will validate a system that does not guarantee the high standards of protection for fundamental rights.[58]

In parallel with this legal analysis of the situation, one must bear in mind two other dimensions: the political and economic dimensions of the question. Irrespective of the CJEU's understanding of this legal debate, the underlying political question remains: is it realistic to ask for more effort from the USA? There is a fundamental conceptual difference between the two systems, with, on the one hand, the American "privacy" system, stemming from the Fourth Amendment, with a highly sectorialised data protection legislation based on consumer protection,[59] and, on the other hand, the European fundamental rights system, with specific norms in primary and secondary law and a right to personal data protection that is distinct and autonomous from the protection of privacy, even though it is often used jointly.[60] Moreover, the economic stakes are high for European companies because, in the absence of an adequacy decision, the GDPR places the responsibility for ensuring that the legal system and practices of the third country in question effectively meet the level of protection required in the EU from the data exporter.[61] This promotes real legal uncertainty and very significant additional costs, especially for medium-sized companies, for example, to put in place standard contractual clauses or other measures[62] to organise such a transfer in order to meet EU requirements in the absence of an agreement.

[58] For a proposal of a hybrid solution that could satisfy both parties, see I Rubinstein and P Margulies, "Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground" (2022) 54 Connecticut Law Review 391, spec. 447.

[59] In this sense, the European Parliament Committee on Civil Liberties, Justice and Home Affairs pointed out that, unlike all other third countries that have received an adequacy decision under the GDPR, the USA still does not have a federal data protection law (see European Parliament resolution of 14 February 2023, supra, note 37).

[60] For an in-depth analysis of the difference between the two systems, see P Schwartz and K Peifer, "Transatlantic Data Privacy" (2017) 106 Georgetown Law Journal 115.

[61] It should be remembered that almost half of the world's data storage capacity is located in the USA. Thus, on 17 May 2021, France presented its new "National Strategy for the Cloud", which develops a new doctrine based on French digital sovereignty in order to respond to, among other things, the "extraterritorial" American laws on intelligence and the risks linked to cybersecurity <https://www.economie.gouv.fr/files/files/Thematiques/numerique/Transcript_presentation_strategie_nationale_cloud.pdf>.

[62] See Art 46 of the GDPR regarding transfers to a third country with "appropriate safeguards" in the absence of an adequacy decision.

The EU is a Union based on the rule of law and on shared values, yet it is also a pragmatic construction. Nevertheless, this agreement clearly presents it with a dilemma: which of the economic, legal or political dimensions will be privileged?

Acknowledgments. We are very grateful to Pablo Baquero and Maxime Célérier-Davril, who provided useful comments on previous versions of this article. All remaining errors, mistakes and controversial points of view remain our own.

Competing interests. The authors declare none.

Cite this article: S Batlle and A van Waeyenberge (2024). "EU–US Data Privacy Framework: A First Legal Assessment". *European Journal of Risk Regulation* **15**, 191–200. https://doi.org/10.1017/err.2023.67