

Foreword to Linklaters' analysis of draft US adequacy decision

EU-US trade is worth over €1 trillion and supports 16 million jobs on both sides of the Atlantic. The US is still by far the EU's largest trade and investment partner.¹ Beyond the economic value of our relationship, our partnership with the US is key to solving pressing global health and green transition challenges, and to protecting our shared democratic values in a world that increasingly threatens them.

Ever since the *Schrems II* ruling,² European industry has been needing more legal certainty about data flows to the US, without which no smooth trade can happen in what is now a fully digital economy. A survey we conducted two and a half years ago showed that almost all EU-based businesses across all sectors transfer data to the US, nearly eight out of ten being EU headquartered. The survey showed that the cost of reassessing companies' data transfers to comply with *Schrems II* was significant.³

In this context, we must now take stock of the negotiations that have led the European Commission and the US government to agree on a new EU-US Data Privacy Framework.⁴ To this end, we have commissioned an independent legal analysis to shed more light on some elements of the Commission's draft adequacy decision that are key in meeting the *Schrems II* ruling's requirements.

This analysis leaves us confident that considerable efforts have been made to correct the deficiencies of the previous EU-US framework relating to necessity, proportionality and redress, and that these efforts can meet the legal test established by the EU Court of Justice.

We hope that this analysis can contribute to a fruitful public discussion around the new framework, whose solidity and viability are so critical for European businesses and citizens alike.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

Markus J. Beyrer
Director General
BusinessEurope

¹ https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en.

² Case C-311/18.

³ *Schrems II impact survey report*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

⁴ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.

Mr. Alberto Di Felice
Director for Infrastructure, Privacy and Security
Policy
DIGITALEUROPE
Rue de la Science 14
B-1040 Brussels (Belgium)

16 February 2023

Dear Mr. Di Felice,

DigitalEurope – Draft US adequacy decision of the European Commission

On 13 December 2022, the European Commission (hereafter, the “**Commission**”) released its draft adequacy decision¹ recognising the United States of America (“**US**”) as ensuring an adequate level of protection for personal data transferred from the European Union (“**EU**”) to US organisations certified² under the new Transatlantic Data Privacy Framework (the “**DPF**”) (the draft adequacy decision of the Commission being hereafter referred to as the “**Adequacy Decision**”).

In this context, we have been asked to prepare a legal review of the Adequacy Decision focusing on its Section 3.2 (access and use of personal data by US public authorities for national security purposes) in order to shed more light on the reasoning of the Commission that underpins its conclusion that the US may be recognised as “adequate”³ within the meaning of Article 45(1) of the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”)⁴, with a particular attention to the ruling of the Court of Justice of the European Union (“**CJEU**”) in the *Schrems II* case⁵.

In doing so, we have focused on the following three topics, which are particularly relevant for the assessment of the consistency of the new US legal framework with the Schrems II findings:

- (i) The choice of an Executive Order as legal instrument in light of the legality principle (Section 3.1 below);

¹ Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Union and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, published on 13 December 2022 (available [here](#)).

² It should be recalled that certification under the DPF is open to organisations that are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the US Department of Transportation (DoT) (see Recital 9 of the Adequacy Decision).

³ For the avoidance of doubt, references to the adequacy of the US must be understood as being limited to the transfer of personal data from the EU to certified organisations under the DPF.

⁴ 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.

⁵ CJEU judgment of 16 July 2020, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (available [here](#)) (“**Schrems II**”).

This communication is confidential and may be privileged or otherwise protected by work product immunity.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an independent consultant or, outside of Belgium, an employee of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England, or on www.linklaters.com.

Please refer to www.linklaters.com/regulation for important information on Linklaters LLP’s regulatory position.

A49815438/6.0/16 Feb 2023

- (ii) The principles of proportionality and necessity applied to the restriction of the fundamental rights to privacy and personal data protection in the context of signals intelligence activities (Section 3.2 below); and
- (iii) The new redress mechanism available to EU individuals (possibly) subject to personal data processing by US public surveillance authorities (Section 3.3 below).

This review does not intend to carry out a comparative law study of the US vs EU legal systems, but rather looks into how the legal means set up by the US fit with the cluster of requirements drawn from the relevant case law of the CJEU and to some extent of the European Court of Human Rights (“**ECtHR**”)⁶.

1 Historical background

On 26 July 2000, the European Commission issued its first adequacy decision towards the US⁷, recognising the adequacy of the protection provided by the US safe harbour privacy principles to which certain organisations could adhere. In its *Schrems* judgment of 6 October 2015⁸, the CJEU however declared such decision invalid.

Following that judgment, the safe harbour privacy principles were replaced by the EU-US Privacy Shield (the “**Privacy Shield**”). On 12 July 2016, the Commission adopted a second decision⁹, which concluded that the protection provided by the Privacy Shield was adequate and allowed the free flow of personal data to companies certified in the US under the Privacy Shield.

However, in its ruling in *Schrems II*, the CJEU declared this decision invalid, holding that such decision was incompatible with Article 45(1) of the GDPR in light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the EU (the “**Charter**”). In particular, the CJEU considered that the US state surveillance powers were not properly circumscribed given the generic access to data by surveillance authorities in the US and that the oversight mechanism of the Privacy Shield did not ensure effective judicial protection for EU-based citizens.

The US and the Commission subsequently re-entered into negotiations with the aim of ensuring personal data transfers to the US afford a protection essentially equivalent to that provided in the EU in light of the requirements set forth by the CJEU in its *Schrems II* ruling. The Commission and the US reached an agreement in principle end of March 2022 for a new EU-US Data Privacy Framework, the so-called DPF. The DPF is an update of the framework applicable to certified commercial entities processing personal data transferred from the EU.

⁶ Although the CJEU has consistently held that the European Convention on Human Rights (“**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*” (see *Schrems II*, §98), the fundamental rights enshrined in the ECHR constitute general principles of EU law under Article 6(3) of the Treaty of the European Union (“**TEU**”) and Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that convention. The CJEU therefore recognises that “*account must [...] be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection*” (CJEU judgment of 6 October 2020, *La Quadrature du Net and others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791 (“**La Quadrature du Net and others**”), § 124 (available [here](#))).

⁷ Commission Implementing Decision (EU) 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

⁸ CJEU judgment of 6 October 2015, *Maximilian Schrems v. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650 (available [here](#)) (“**Schrems I**”).

⁹ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ L 207, 1.8.2016).

On 7 October 2022, President Biden signed Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities (“**EO 14086**”)¹⁰, which implements into US law the commitments made under the DPF. On the same date, the US Attorney General issued a Regulation (the “**AG Regulation**”)¹¹ establishing the Data Protection Review Court (the “**DPRC**”).

It is based on a thorough assessment of the DPF and the US legal framework applicable to personal data access by public authorities (including EO 14086 and the AG Regulation) that the Commission adopted its Adequacy Decision.

The draft is subject to the review of the European Data Protection Board (“**EDPB**”), which is expected to render its opinion in the first quarter of 2023. This opinion will not be binding but authoritative. It is likely to give rise to some adaptations of the Adequacy Decision further to which the draft will be submitted to the vote of the representatives of the EU Member States (the so-called comitology procedure) and may be subject to the scrutiny of the European Parliament. Following such process, the Commission should be able to adopt a final Adequacy Decision and EU companies should then be able to validly transfer personal data to US certified companies, without having to put in place any additional safeguards.

2 General considerations

The updated framework (EO 14086 and AG Regulation). EO 14086 and the AG regulation were prepared on the basis of extensive discussions with the Commission, which worked closely with the US government to address the concerns raised by the CJEU.

This new framework introduces additional safeguards and new redress mechanisms, which apply to all EU-US transfers (not only transfers to certified companies) and benefit to all individuals present in the EU, regardless of their nationality.

The progress achieved by this new data protection framework is substantial compared with the previous transfer mechanism in place and responds to the CJEU’s criticisms about the US legal landscape. The US has significantly moved a long way towards the EU in a field (national security) that is a highly sensitive topic of national sovereignty. This progress is part of a broader trend for more public scrutiny in this area¹².

Essential equivalence test. Article 45 of the GDPR is the basis for the adoption of adequacy decisions. Its second paragraph includes a series of elements to be taken into account by the Commission when assessing the level of protection of a third country (e.g. the rule of law, the respect of human rights and the enforcement mechanism for compliance with data protection rules), on the basis of which the CJEU’s and EDPB’s requirements have been developed.

¹⁰ US Executive Order 14086 ‘Enhancing Safeguards for United States Signals Intelligence Activities’, Federal Register Vol. 87, No 198(7 October 2022) (available [here](#)).

¹¹ Rule by the Justice Department published on 14 October 2022 amending the Department of Justice regulations to establish the DPRC (available [here](#)).

¹² At intergovernmental level, efforts are being made to better frame the powers of governments’ access to personal data held by private actors, including in the context of national security activities. For example, the Organisation for Economic Co-operation and Development (OECD), which the US is a member of, has recently issued a declaration to this effect. Although non-binding, it signals a move towards more restrictions to the rights of governments to access personal data held by private companies (see OECD Declaration on Government Access to Personal Data held by Private Sector Entities, 14 December 2022, available [here](#)). This declaration includes a commitment to comply with principles of proportionality and necessity, which are however to be interpreted on the basis of national law, unlike the principles imposed by EO 14086, which defines those principles directly in the text thereof (see Section 3.2).

The Adequacy Decision results from an assessment made by the Commission on the above basis to determine whether the US guarantees “*an adequate level of protection essentially equivalent to that ensured within the Union*”¹³. It should be recalled that essential equivalence, as interpreted by the CJEU¹⁴, does not require the US legal framework to replicate identically the same rules as those imposed in the EU. Instead, it must be determined whether the legal system of a sovereign State offers an adequate protection of the personal data, which effectively protects EU personal data within the boundaries of such third country legal system. The means used to offer such level of protection may therefore differ from those employed within the EU.

Final adequacy decision. The entry into force of the Adequacy Decision is made conditional upon the implementation of the safeguards and oversight and redress mechanisms set out under EO 14086 and the AG Regulation. Such implementation is expected to be completed by the adoption of the final Adequacy Decision¹⁵. It is assumed that the Commission will closely monitor the implementation of the Adequacy Decision in cooperation with the US to make sure it is completed in a satisfactory manner.

3 The collection and use of personal data by US public authorities for national security purposes

It should first be recalled that the interferences by US public authorities with EU citizens’ fundamental rights that were criticised by the CJEU in Schrems II and that are covered in Section 3.2 of the Adequacy Decision are focusing on the area of national security¹⁶. Within the EU, this area is the sole responsibility of each Member State, pursuant to Article 4(2) of the TEU. It is through the interaction of national security measures with areas governed by EU law, such as the protection of the fundamental rights enshrined within the Charter, that such measures fall within the realm of EU law and under the scrutiny of the CJEU.

Within the European context, the CJEU has recognised national security as being particularly specific and capable of justifying more serious limitations to EU individuals’ fundamental right to personal data protection under the Charter. Indeed, in *La Quadrature du Net* and others, the CJEU indicated that the importance of the objective of safeguarding national security goes beyond that of other objectives, such as combating (serious) crime and safeguarding public security¹⁷, due to the specific nature and particular seriousness of national security threats¹⁸. On that basis, the CJEU concluded that “*the objective of safeguarding national security is therefore capable of justifying*

¹³ Recital 104 of the GDPR.

¹⁴ See Schrems I, §§ 73-74 and CJEU Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI:EU:C:2017:592 (“**Opinion 1/15**”), § 134 (available [here](#)).

¹⁵ This implementation work is ongoing. See for instance the Intelligence Community Directive 126 entitled ‘Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086’, which was released to the public by the Office of the Director of National Intelligence (“**ODNI**”) on 14 December 2022 (available [here](#)).

¹⁶ In *La Quadrature du Net* and others (§ 135), the CJEU defines the responsibility of EU Member States in the field of national security as corresponding to “*the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities*”.

¹⁷ The CJEU stresses that threats to national security (i.e. State security) “*can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise*” (*La Quadrature du Net* and others, § 136). See also CJEU judgment of 5 April 2022, *G.D. v. The Commissioner of the Garda Síochána and Others*, C-140/20, ECLI:EU:C:2022:258, § 52 (available [here](#)).

¹⁸ *La Quadrature du Net* and others, § 136.

*measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives*¹⁹.

In the same vein, the ECtHR has ruled in relation to state surveillance that national security is an area in which national authorities “*enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security*”²⁰.

Transposed in the context of an adequacy finding, the Article 29 Data Protection Working Party (“**WP29**”) Adequacy Referential also indicates that, while the “European Essential Guarantees”²¹ must be respected for personal data access by third country public authorities for such third country to be found adequate, such guarantees may be applied differently in the field of national security access to data²².

The above European Essential Guarantees cover the following four guarantees, which must be considered in the assessment of a third country adequacy under Article 45 of the GDPR²³:

- (i) The processing should be based on clear, precise and accessible rules (legal basis);
- (ii) The necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
- (iii) The processing must be subject to independent oversight; and
- (iv) Effective remedies must be available.

These guarantees were originally drafted by the WP29 in response to Schrems I in order to set minimum requirements to be respected in foreign public authorities’ interferences through surveillance measures with EU citizens’ fundamental rights to privacy and personal data protection²⁴.

Following the Schrems II judgment, the EDPB adopted its Recommendations 02/2020 to reflect in the European Essential Guarantees the recent developments of the CJEU and ECtHR case law in the field of surveillance, in particular the clarifications provided by the CJEU in Schrems II.

It is indeed in the field of national security (surveillance) that the CJEU found in Schrems II that the Commission’s US adequacy decision was invalid, essentially on the following two grounds:

¹⁹ *Ibidem*.

²⁰ ECtHR judgment of 25 May 2021, *Big Brother Watch and Others v. the United Kingdom*, No. 58170/13/13, 62322/14 and 24960/15, § 338 (available [here](#)) and case law cited therein (“**Big Brother Watch and Others**”). See also ECtHR judgment of 29 June 2006, *Gabriele Weber and Cesar Richard Saravia v. Germany*, No. 54934/00, § 106 (available [here](#)); ECtHR judgment of 4 December 2015, *Roman Zakharov v. Russia*, No. 47142/06, § 232 (available [here](#)), and the case law cited therein.

²¹ As set out in EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020 (available [here](#)) (the “**European Essential Guarantees**”).

²² See Chapter 4 of Opinion WP254 on the Adequacy Referential, adopted on 28 November 2017, as last revised on 6 February 2018 (available [here](#)).

²³ While the European Essential Guarantees are non-binding guidance issued by the EDPB, it remains an authoritative text which may inform the decisions of the EU Member States’ supervisory authorities, which are represented in the EDPB. They also constitute a useful basis for the assessment of a non-EEA country’s adequacy under the GDPR as they provide a structured consolidation of the relevant CJEU case law.

²⁴ Opinion WP237 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), adopted on 13 April 2016 (available [here](#)).

- (i) Applicable legislations in the field of surveillance did not provide the minimum safeguards resulting from the principle of proportionality so that US surveillance programmes could not be regarded as limited to what is strictly necessary²⁵; and
- (ii) The ombudsperson mechanism of the Privacy Shield did not offer guarantees to EU citizens that are essentially equivalent to those required by Article 47 of the Charter and hence did not remedy the deficiencies of the US legal system that deprived EU citizens from their right to an effective remedy (e.g. in relation to the collection of personal data outside the US under Executive Order 12333²⁶, such as personal data transiting between the EU and the US)²⁷.

In other words, the CJEU found that two European Essential Guarantees were not met in the adequacy assessment of the US: (i) the application of the necessity and proportionality principles and (ii) the availability of effective remedies.

With the adoption of EO 14086 and the AG Regulation, the US is addressing all four European Essential Guarantees, including the two main concerns of the CJEU, as expressed in Schrems II.

In the following sections, we look into how the US is addressing these guarantees in light of the CJEU's requirements in Schrems II, noting that the oversight mechanism will only be covered to the extent relevant in our review.

3.1 Acts of the Executive as legal instrument (legality principle)

The first European Essential Guarantee to be assessed in the framework of an adequacy decision is whether the processing of personal data is based on “*clear, precise and accessible rules*” governing the scope of application of the interfering measures and imposing minimum safeguards²⁸.

Such guarantee reflects the developments of the case law, which is built on the legality requirements of the Charter in relation to both the right to personal data protection and the restriction of such right. Pursuant to Article 8(2) of the Charter, personal data must be processed “*for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*”²⁹. Similarly, Article 52(1) of the Charter requires any limitation on the exercise of the rights and freedoms recognised by the Charter to be “*provided for by law*”.

In its interpretation of the Charter, the CJEU considers that, in order to fulfil this legality requirement, the foreign legal instrument must:

- (i) be “*legally binding under domestic law*”³⁰,
- (ii) “*itself define the scope of the limitation on the exercise of the right concerned*”³¹, and
- (iii) grant to EU individuals “*actionable rights before the courts against the US authorities*”³².

²⁵ Schrems II, § 184.

²⁶ US Executive Order 12333 'United States Intelligence Activities', Federal Register Vol. 40, No. 235 (8 December 1981 as amended 30 July 2018) (hereafter, “**EO 12333**”).

²⁷ Schrems II, §§ 192 and 197.

²⁸ EDPB Recommendations 02/2020, *op. cit.*, § 27.

²⁹ Such principle is recalled in the case law of the CJEU (see Schrems II, §173).

³⁰ CJEU judgment of 6 October 2020, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, C-623/17, ECLI:EU:C:2020:790 (“**Privacy International**”), § 68 (available [here](#)).

³¹ Schrems II, § 175 and the case law cited therein.

³² Schrems II, § 181.

It is clear that the CJEU does not take a formalistic approach and focuses on the content of the law as well as whether it can be invoked and relied on by individuals before a court, regardless of its form or source. The notion of “law” under the Charter, as interpreted by the CJEU is therefore broadly defined. Such notion can encompass rules that are not of a legislative nature (such as an act of the executive branch), provided that the above conditions (i) to (iii) are fulfilled.

- In the *Léger* case³³, the CJEU expressly recognised that a restriction on the principle of non-discrimination contained in a French ministerial decree met the condition of legality set out in Article 52(1) of the Charter: *“it is common ground that the permanent contraindication to blood donation for a man who has had sexual relations with another man, which constitutes a limitation on the exercise of the rights and freedoms recognised by the Charter, must be regarded as being provided for by law, within the meaning of Article 52(1), since it stems from the Decree of 12 January 2009”*³⁴ (we underline) that was adopted by the French Minister of Health and Sport³⁵.
- In *Schrems II*, while the CJEU considered that the US Presidential Policy Directive 28 (“**PPD-28**”)³⁶ did not fulfil the legality conditions as it could not be effectively relied on by EU individuals before a court, it did not question the bindingness of such a legal instrument on US public authorities³⁷.
- The French version of the CJEU decision in *Privacy International* uses the wording “*réglementation*”³⁸, which has a broader scope than legislative acts that would have been otherwise referred to as “*législation*”.

It stems from the above that nothing precludes a US Executive Order from being considered as a “law” within the meaning of the Charter.

The above legality conditions (i) to (iii) therefore appear to be met by the US, given that EO 14086:

- (i) is legally binding on US intelligence authorities pursuant to the authority vested in the President under Article II, Section 1 (the Executive Power) of the US Constitution,
- (ii) defines the scope of, and applicable safeguards to, the interferences of US intelligence activities with EU individuals’ rights to personal data protection (see notably Section 3.2), and
- (iii) offers EU citizens the right to enforce before an administrative court their right to personal data protection against such US intelligence authorities (see Section 3.3).

Most importantly, it should be noted that an Executive Order or other Presidential authorisation³⁹ (i.e. executive acts) is the sole US legal instrument to undertake or restrict intelligence surveillance

³³ CJEU judgment of 29 April 2015, *Geoffrey Léger v. Ministre des Affaires sociales, de la Santé et des Droits des femmes, Établissement français du sang*, C-528/13, ECLI:EU:C:2015:288 (available [here](#)).

³⁴ *Ibidem*, § 53.

³⁵ *Ibidem*, § 21.

³⁶ Please note that EO 14086 revokes and supersedes PPD-28, except for its Sections 3 (policy processes) and 6 (general provisions) and its classified annex. See Section 5(f) of EO 14086 and the National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, NSM-14, 7 October 2022 (available [here](#)).

³⁷ *Schrems II*, § 181.

³⁸ “*Cette réglementation doit être légalement contraignante en droit interne*” (*Privacy International*, § 68, we underline).

³⁹ Based on a combined reading of Recital 122 of the Adequacy Decision and Section 2(a)(i) of EO 14086 to which the Adequacy Decision refers, a Presidential authorisation should be construed as an “*Executive Order, proclamation or other Presidential directive*”.

of foreign powers or their agents when not conducted via US telecommunications infrastructure. While Congressional statutes (i.e. legislative acts) may authorise and place restrictions around signals intelligence activities to be carried out involving US persons or conducted via telecommunications infrastructure in the US (e.g. Section 702 of the Foreign Intelligence Surveillance Act, or “**FISA**”), the executive branch has the sole authority under Article II of the US Constitution to undertake or to restrict foreign intelligence activities conducted wholly outside the US, not involving US persons, and not taking place on US telecommunications infrastructure; in such instances, the established role of Congress since the 1970’s has been to provide oversight⁴⁰.

As a result, not only does EO 14086 meet the legality requirements of the CJEU, it is also the most appropriate means within the US legal system to ensure the effective implementation of the safeguards and mechanisms it introduces.

In any case, in the event EO 14086 would be repealed or changed in a way affecting the level of protection of EU personal data, the Commission may immediately suspend or repeal the Adequacy Decision, entirely or partially⁴¹.

Last, it is interesting to note that EO 14086 foresees that “*in the case of any conflict between this order and other applicable law, the more privacy-protective safeguards shall govern the conduct of signals intelligence activities, to the maximum extent allowed by law*”⁴².

We welcome this useful addition, noting that, in accordance with the US hierarchy of norms, an Executive Order may either (a) pertain to a topic exclusively reserved for presidential power, in which case there would be no possibility for conflict between an Executive Order and an act of Congress, or (b) pertain to a topic of concurrent authority between Congress and the executive branch, in which case the Executive Order will apply concurrently to the extent it does not contradict the express or implied will of Congress.

Given the above discussion about the executive branch maintaining exclusive authority to undertake or restrict certain foreign surveillance without a US nexus, we anticipate that much of the subject matter of EO 14086 would not be at risk for conflicting with US statute, and therefore there would be little risk of EO 14086 being subordinate to a less protective US statute.

3.2 Necessity and proportionality

It is settled case law that the fundamental right to the protection of personal data under Article 8 of the Charter is not absolute⁴³ and may thus be limited, provided such limitation complies with Article 52(1) of the Charter.

We have already looked into the first requirement of Article 52(1) of the Charter (see Section 3.1), i.e. limitations to the exercise of fundamental rights recognised by the Charter must be based on law (as broadly interpreted).

Article 52(1) further provides that “*subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union*

⁴⁰ See US Library of Congress, Congressional Research Service. *Cover Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, by Michael E. DeVine, CRS Report R45175, November 2022. See also Rosenbach, Eric and Aki Peritz. “Congressional Oversight of the Intelligence Community.” Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2009.

⁴¹ Article 3(5) of the Adequacy Decision.

⁴² Section 5(c) of EO 14086.

⁴³ Opinion 1/15, § 136 and the case law cited therein.

or the need to protect the rights and freedoms of others” (we underline). This double requirement that an interfering measure be proportionate and necessary is reflected in the European Essential Guarantees, which require the demonstration of such necessity and proportionality with regard to the legitimate objectives pursued⁴⁴.

In order to satisfy the above requirements, the CJEU considers that the foreign legislation which entails an interference with the fundamental rights guaranteed by the Charter “*must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse*”⁴⁵. In particular, such legislation must specify “*in what circumstances and under which conditions a measure providing for the processing of such data may be adopted*”⁴⁶.

The case law of the CJEU has developed a threefold test to determine whether a restriction on fundamental rights protected by the Charter is proportionate⁴⁷.

1. First, the measure must be **appropriate** for the achievement of the general interest objective such measure pursues⁴⁸. In other words, the measure must fulfil a recognised objective of general interest and be at least “*capable of contributing*”⁴⁹ to its achievement.
2. The measure must then be **necessary** for the achievement of the above objective, which can only be the case “*in the absence of any other measure which would be equally appropriate but less restrictive*”⁵⁰. This means that, among all suitable options, the measure providing for the lowest degree of interference must be preferred.

The necessity threshold is quite high in the CJEU case law, the CJEU having recalled on several occasions the “*strictly necessary*” nature of the interfering measure⁵¹. In particular in the field of data transmission and retention in the context of the collection of data by telecom operators for the fight against serious crime⁵², the CJEU has applied particularly high requirements of granularity and precision of the objectives pursued or other objective criteria with the aim of narrowing down the scope of data collection and retention to what is strictly necessary.

3. Finally, and assuming that it is appropriate and necessary in the above senses, the measure must still be **proportionate sensu stricto** to the achievement of the objective pursued. In an

⁴⁴ EDPB Recommendations 02/2020, *op. cit.*, §§ 32-38.

⁴⁵ Schrems II, § 176. See also Opinion 1/15, § 141.

⁴⁶ *Ibidem*.

⁴⁷ See for example, the test applied by the CJEU in Opinion 1/15, §§ 152 and following. See also CJEU judgment of 5 April 2022, G.D. v. The Commissioner of the Garda Síochána and Others, *op. cit.*, § 93; Opinion of Advocate General Kokott of 31 May 2016, Samira Achbita and Centrum voor gelijkheid van kansen en voor racismebestrijding v. G4S Secure Solutions NV, C-157/15, ECLI:EU:C:2016:382, § 97 (available [here](#)); Opinion of Advocate General Saugmandsgaardøe of 17 July 2016, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department, C-203/15 and C-698/15, 21 December 2016, ECLI:EU:C:2016:572, § 174 (available [here](#)).

⁴⁸ Opinion 1/15, §§ 152-153.

⁴⁹ Opinion of Advocate General Saugmandsgaardøe in Tele2 Sverige AB, *op. cit.*, § 176.

⁵⁰ *Ibidem*, § 185.

⁵¹ Schrems II, § 176. See also as another example, CJEU judgment of 5 April 2022, G.D. v. The Commissioner of the Garda Síochána and Others, *op. cit.*, § 52.

⁵² CJEU judgment of 8 April 2014, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, joined cases C- 293/12 and C-594/12, ECLI:EU:C:2014:238 (available [here](#)) (“**Digital Rights**”); CJEU judgment of 21 December 2016, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department, C-203/15 and C-698/15, ECLI:EU:C:2016:970 (available [here](#)) (“**Tele2 Sverige AB**”).

opinion of Advocate General Saugmandsgaardoe, the latter states that "*a measure which infringes fundamental rights can only be regarded as proportionate if the disadvantages caused are not disproportionate to the aims pursued*"⁵³. This is a value-based judgment, which requires balancing the benefits and harms resulting from the measure at stake.

To conduct the above assessment, the CJEU generally measures the seriousness of the interference entailed by the limitation on the rights to privacy and data protection and verifies whether the importance of the public interest objective pursued by such limitation is proportionate to its seriousness⁵⁴.

The CJEU has provided only few guidance on such assessment in data protection matters, as it has often ruled that restrictions were not necessary (thus not looking at the third criteria, all three being cumulative).

It is interesting to note that the ECtHR has consistently recognised that "*when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, (...) the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security*"⁵⁵. This State's margin of appreciation in the field of national security should therefore be taken into account in the proportionality test.

In Schrems II, the CJEU found that neither Section 702 of FISA, nor EO 12333, read in conjunction with PPD-28, correlated to the minimum safeguards resulting from the EU proportionality principle⁵⁶ and therefore concluded that the interferences of US public authorities with the protection of personal data were "*not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter*"⁵⁷.

Such conclusion was based on the following grounds:

- (i) Section 702 of FISA provided for neither any limitations on the power to implement foreign intelligence surveillance programmes nor any guarantees for non-US individuals potentially targeted by such programmes⁵⁸; and
- (ii) The scope of the "bulk" collection in the context of surveillance programmes under EO 12333, which was authorised by PPD-28, was not delimited in a sufficiently clear and precise manner⁵⁹.

While the CJEU in Schrems II did not go through the entire three-step proportionality assessment (focusing on necessity), such test provides a solid reference point to examine the limitations and

⁵³ Opinion of Advocate General Saugmandsgaardøe in *Tele2 Sverige AB*, *op. cit.*, § 247.

⁵⁴ *La Quadrature du Net and others*, § 131 and case law cited therein; CJEU judgment of 5 April 2022, *G.D. v. The Commissioner of the Garda Síochána and Others*, *op. cit.*, § 53. See also EDPB Recommendations 02/2020, *op. cit.*, § 33.

⁵⁵ ECtHR judgment of 29 June 2006, *Gabriele Weber and Cesar Richard Saravia v. Germany*, *op. cit.*, § 106 and the case law cited therein. See also inter alia ECtHR judgment of 30 January 2020, *Breyer v. Germany*, No. 50001/12, §§ 79 and 80 (available [here](#)) and case law cited therein.

⁵⁶ Schrems II, § 184.

⁵⁷ Schrems II, § 185. The second sentence of Article 52(1) of the Charter provides that: "*subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*".

⁵⁸ Schrems II, § 180.

⁵⁹ Schrems II, § 184.

safeguards introduced by EO 14086 and consider its essential equivalence with the above EU proportionality principle.

In the following sections, we examine how EO 14086 considers the proportionality principle, also reviewing the bulk related aspects.

3.2.1 Proportionality under EO 14086

In the Adequacy Decision, the Commission enumerates the overarching safeguards that intelligence agencies must apply to all their signals intelligence activities to ensure that privacy and civil liberties are taken into account in the organisation and implementation of such activities.

The scope of application of such safeguards is broadly defined, as they apply to all processing activities carried out for signals intelligence purposes, from the collection to the dissemination of personal data by the intelligence agencies⁶⁰, regardless of the legal basis relied on to conduct such activities. In other words, signals intelligence activities both under Section 702 of FISA and EO 12333 will be subject to such overarching principles, being more generally subject to EO 14086 in its entirety⁶¹. These safeguards also apply to any individuals subject to US signals intelligence measures, regardless of their nationality and place of residence.

Two of the above safeguards require the application of the following necessity and proportionality principles, which define *when* and *how* signals intelligence activities may be carried out:

- Prior to any signals intelligence activities being authorised, it must first be determined on the basis of a multi-factor assessment whether such activities are necessary to advance a “validated intelligence priority” (as further explained below)⁶². Such assessment must be documented and is subject to oversight⁶³.
- Once authorised, such activities may then only be conducted to the extent and in a manner that is proportionate to the above validated intelligence priority⁶⁴. EO 14086 thereby requires “*a proper balance*” to be struck between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of the individuals at stake, regardless of their nationality or where such individuals might reside.

Not only does EO 14086 refer to, and provide the means to comply with, the concepts of necessity and proportionality, as we know them in EU law, but it also further substantiates these principles into more granular limitations and conditions that circumscribe the collection of signals intelligence activities. In doing so, EO 14086 introduces a test that appears essentially equivalent to the above EU proportionality three-step assessment.

First, the collection of signals intelligence activities is limited by the application of a two-layer standard in terms of purpose limitation.

⁶⁰ Section 2(a) of EO 14086 and Recital 121 of the Adequacy Decision.

⁶¹ Recital 118 of the Adequacy Decision.

⁶² Section 2(a)(ii)(A) of EO 14086.

⁶³ Section 2(c)(iii)(E) of EO 14086.

⁶⁴ Section 2(a)(ii)(B) of EO 14086.

- (i) The collection of signals intelligence may only take place in the pursuit of legitimate objectives, which are defined both in positive and negative terms. On the one hand, EO 14086 exhaustively lists the sole legitimate objectives that may be pursued in the collection of signals intelligence (e.g. protection against foreign military capabilities and activities, terrorism, espionage, threats from the development, possession or proliferation of weapons of mass destruction)⁶⁵, and on the other hand, EO 14086 enumerates a series of prohibited objectives that must not be pursued through signals intelligence collection activities (e.g. suppression of the free expression of ideas, restriction of legitimate privacy interests, discrimination based on race, gender identity or religion)⁶⁶. This exhaustive listing draws the line between what can be included and what cannot be included under “national security”, which is the common basis for the conduct of intelligence activities.
- (ii) EO 14086 adds an extra layer of purpose limitation by requiring that the above theoretical objectives be concretised into operational priorities to be validated by the President. It is only on the basis of such validated priorities that the actual collection of signals intelligence may be carried out (after having assessed the necessity of the envisaged measure to advance a particular validated priority).

These priorities are established by the Director of National Intelligence under the scrutiny of the Civil Liberties and Protection Officer (“**CLPO**”)⁶⁷ through the so-called National Intelligence Priorities Framework (**NIPF**)⁶⁸. Before presenting the NIPF to the President, the CLPO must first assess whether each priority identified in the NIPF (a) advances one or more of the above legitimate objectives, (b) may/will not result in signals intelligence collection for a prohibited objective, and (c) takes due account of the privacy and civil liberties of individuals, regardless of their nationality or wherever they might reside⁶⁹.

By providing a “positive” list of authorised objectives (and, conversely, a “negative” list of prohibited objectives) combined with concrete priorities, EO 14086 requires intelligence agencies to carry out the first step of the above proportionality test, namely the appropriateness test (see point 1 above). Indeed, each signals intelligence measure will only be authorised if it fulfils a recognised general interest objective (exclusive of any prohibited objectives).

Second, once this initial stage has been completed and the purpose delimitations have been defined, intelligence agencies must apply the other two steps of the proportionality test in

⁶⁵ Section 2(b)(i)(A) of EO 14086. It should be noted that the President may extend the list of legitimate objectives “*in light of new national security imperatives*”, which would then be made publicly available by the Director of National Intelligence, unless such publication would pose a risk to the national security of the US (Section 2(b)(i)(B) of EO 14086).

⁶⁶ Section 2(b)(ii)(A) of EO 14086.

⁶⁷ Pursuant to 50 U.S.C. § 3029 (b), the CLPO is responsible for (among others) ensuring that the protection of civil liberties and privacy is appropriately incorporated in policies and procedures of the intelligence agencies. The CLPO is also responsible for exercising oversight functions towards ODNI to monitor its compliance with applicable civil liberties and privacy requirements.

⁶⁸ It is interesting to note that the definition of “validated intelligence priority” allows for the application of exceptions to the above validation process. The priority may indeed be set by the President or the head of an element of the intelligence community, in accordance with the criteria set out in the validation process (Section 2(b)(iii)(A) of EO 14086) “*to the extent feasible*” (Section 4(n) of EO 14086). References to “elements of the Intelligence Community” should be construed as referring to the similar concept defined in Section 3.5(h) of EO 12333.

⁶⁹ Section 2(b)(iii)(A)(1)-(3) of EO 14086.

the broad sense in order to limit signals intelligence collection, i.e. the necessity test (see point 2 above) and the proportionality test *sensu stricto* (see point 3 above).

To give effect to the overarching necessity principle under EO 14086⁷⁰, intelligence agencies must consider the “*availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority*” and, where available, must prioritise such less intrusive alternatives⁷¹.

This requirement is an application of the EU necessity principle, which requires the least intrusive measure to be preferred over and above other intrusive measures capable of achieving a same goal⁷² (see point 2 above).

Provided that the envisaged signals intelligence collection is considered appropriate and necessary, such collection must be “*as tailored as feasible*” to advance the particular validated intelligence priority and “*may not disproportionately impact privacy and civil liberties*”⁷³.

To carry out this balancing exercise between the validated intelligence priority and the protection of privacy and civil liberties, EO 14086 requires intelligence agencies to take due account of all relevant factors depending on the circumstances. Such factors include for instance the nature of the objective pursued, the intrusiveness of the collection (including its duration), the reasonably foreseeable consequences on individuals as well as the nature and sensitivity of the data.

The factors listed in EO 14086 are recognisably based on certain criteria⁷⁴ taken into consideration by the CJEU in its proportionality assessment in data protection cases. In order to assess the seriousness of an interference, the CJEU generally looks first at the nature of the data and the sensitivity of the (derived) information⁷⁵. The reasonable consequences on individuals and in particular their other rights guaranteed by the Charter, such as the freedom of expression, is also relevant⁷⁶. In assessing the necessity of an interfering measure, the CJEU has also paid particular attention to the objectives pursued by the foreign public authority⁷⁷ and the duration of the retention of personal data⁷⁸. The inclusion of such factors in the proportionality assessment introduced by EO 14086 shows the US willingness to align with the EU concepts applied by the CJEU.

⁷⁰ According to which, signal intelligence may only be collected “*following a determination that, based on a reasonable assessment of all relevant factors, the collection is necessary to advance a specific intelligence priority*” (Section 2(a)(ii)(A) of EO 14086).

⁷¹ Section 2(c)(i)(A) of EO 14086.

⁷² CJEU judgment of 22 January 2013, *Sky Österreich GmbH v. Österreichischer Rundfunk*, C-283/11, ECLI:EU:C:2013:28, §§ 54-57 (available [here](#)); CJEU judgment of 13 November 2014, *Ute Reindl, representative of MPREIS Warenvertriebs GmbH v. Bezirkshauptmannschaft Innsbruck*, C-443/13, ECLI:EU:C:2014:2370, § 39 (available [here](#)); CJEU judgment of 16 July 2015, *CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia*, C-83/14, ECLI:EU:C:2015:480, §§ 120-122 (available [here](#)).

⁷³ Section 2(c)(i)(B) of EO 14086.

⁷⁴ It should be noted that the factors taken into account by the CJEU in its proportionality assessment as well as the extent of their review vary depending on the circumstances of the matter subject to its review. Other criteria may therefore be taken into account.

⁷⁵ In *Tele2 Sverige AB*, the CJEU made an entire analysis of the types of data that may be collected and the information that may be derived therefrom. It concluded on that basis that the interference in the fundamental rights of Articles 7 and 8 of the Charter “*is very far-reaching and must be considered to be particularly serious*” (§100). See also *La Quadrature du Net and others*, § 117.

⁷⁶ *Tele2 Sverige AB*, § 101. See also *La Quadrature du Net and others*, § 118.

⁷⁷ Opinion 1/15, §§ 175 and following.

⁷⁸ Opinion 1/15, §§ 190 and following.

These factors also largely reflect those considered by the European Data Protection Supervisor in its guidelines on proportionality assessment⁷⁹, inter alia the level of intrusiveness of the measure, the consequences of such measure (e.g. the number of people affected, whether it affects other person's privacy or other fundamental rights), the amount of data collected and whether it includes special categories of data.

Third, the overarching necessity and proportionality principles do not solely apply in relation to the collection of the data on the basis of the above safeguards but also its further use by intelligence agencies. Again, these principles are further substantiated in various conditions and limitations set out in EO 14086, such as the following⁸⁰:

- The retention and dissemination of personal data collected through signals intelligence must be minimised⁸¹.

To that effect, EO 14086 requires inter alia that dissemination of personal data within the US government is also subject to the confirmation of an authorised and specifically trained member of the personnel, who must reasonably believe that the information will be appropriately protected and that data will be accessed on a need-to-know basis⁸².

EO 14086 also introduces a dissemination and retention regime that replicates that applicable to US citizens⁸³. For instance, only signals intelligence that involves certain types of information comparable to those of US persons may be disseminated⁸⁴.

- In the handling of personal information, intelligence agencies must comply with a number of security requirements. For instance, (i) the processing and storing of personal data must be subject to appropriate protection so as to prevent the unauthorised access to such data⁸⁵ and (ii) personal data may only be accessed by trained and authorised personnel on a need-to-know basis⁸⁶. In that respect, intelligence agencies are required to provide and maintain appropriate training to their personnel who have access to signal intelligence⁸⁷.
- The personal data collected via signals intelligence activities may only be kept in accordance with the intelligence community standard for accuracy and objectivity, including the quality and reliability of such data⁸⁸.

The above requirements of EO 14086 participate in meeting the proportionality requirements described above, in particular the requirement of Article 8 of the Charter *“to ensure effective*

⁷⁹ EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, adopted on 19 December 2019, pp. 22-23 (available [here](#)).

⁸⁰ Section 2(c)(iii) of EO 14086.

⁸¹ Section 2(c)(iii)(A) of EO 14086.

⁸² Section 2(c)(iii)(A)(1)(c) of EO 14086.

⁸³ See, in relation to data retention, Section 2(c)(iii)(A)(2) of EO 14086.

⁸⁴ Section 2(c)(iii)(A)(1)(a) of EO 14086.

⁸⁵ Section 2(c)(iii)(B)(1) of EO 14086.

⁸⁶ Section 2(c)(iii)(B)(2) of EO 14086.

⁸⁷ Section 2(d)(ii) of EO 14086.

⁸⁸ Section 2(c)(iii)(C) of EO 14086.

*protection of the data retained against the risk of abuse and against any unlawful access and use of that data*⁸⁹.

It is apparent from the above developments that the US authorities took pains to address the CJEU's concerns in Schrems II by introducing limitations on the power of intelligence agencies to implement foreign intelligence surveillance programmes and by providing additional guarantees for non-US individuals potentially targeted by such programmes, beyond what was in place at the time of Schrems II and was not considered sufficient by the CJEU.

To do so, EO 14086 defines the scope of application of the signals intelligence activities and the conditions under which they may be carried out, thus meeting the general requirement that a third country law authorising interferences with the fundamental rights to privacy and data protection “*must itself defined the scope of the limitation on the exercise of the right concerned*”⁹⁰ and “*must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted*”⁹¹.

3.2.2 Bulk collection under EO 14086

The CJEU has a long history of rejecting EU Member States' so-called “mass surveillance”, i.e. the general and indiscriminate retention and transmission of personal data from electronic communications network for the purposes of combating serious crime and safeguarding national security⁹².

In such instances, the CJEU found that “*national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter*”⁹³.

As further explained below, this so-called mass surveillance must be distinguished from the data bulk collection under EO 14086, the collection of data in bulk being in principle allowed, subject to the application of limitations and safeguards designed to ensure that data is not accessed on an indiscriminate basis⁹⁴.

(i) Mass surveillance in EU Member States for the purpose of combating serious crime

The CJEU has indeed considered that the objective of general interest of fighting serious crime, including organised crime and terrorism, “*however fundamental it may be, cannot in itself justify that national legislation providing for the general and*

⁸⁹ Digital Rights, § 66.

⁹⁰ Schrems II, § 175 and Opinion 1/15, § 139.

⁹¹ Schrems II, § 176.

⁹² See inter alia Tele2 Sverige AB, § 107; La Quadrature du Net and others, § 141; Privacy International, § 81, on the transmission of traffic and location data to security and intelligence agencies for national security purposes; CJEU judgment of 5 April 2022, G.D. v. The Commissioner of the Garda Síochána and Others, *op. cit.*, § 101.

⁹³ Privacy International, § 81; see also Tele2 Sverige AB, § 107; La Quadrature du Net and others, § 141.

⁹⁴ See footnote 223 of the Adequacy Decision.

*indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight*⁹⁵.

Additional limitations and guarantees must apply to consider such serious interference as strictly necessary, among others the need to establish a connection between the personal data sought to be collected and the objectives pursued by the public authorities (as further explained below)⁹⁶.

(ii) Mass surveillance in EU Member States for the purpose of safeguarding national security

In relation to the general and indiscriminate retention of traffic and location data by telecommunication companies for the purpose of protecting national security, the CJEU seems to have adopted a more lenient position, taking into account the nature and particular seriousness of threats to national security⁹⁷. The CJEU has indeed held that in such context, the Charter “*does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat [...] to national security which is shown to be genuine and present or foreseeable*”⁹⁸ (we underline). In so doing, the CJEU has effectively admitted the general and indiscriminate retention of data without the need to establish a direct connection between the data sought and the objective pursued on the basis of objective criteria, considering that the existence of that threat is, in itself, capable of establishing such connection⁹⁹.

While allowing for some flexibility in the field of national security in the above context, the CJEU nevertheless requires that such data retention be subject to limitations and circumscribed by strict safeguards making it possible to protect the personal data of the persons concerned effectively against the risk of abuse¹⁰⁰.

(iii) Bulk collection in the US under EO 14086

Similarly, in Schrems II, the CJEU challenged the fact that US public authorities resort to the “bulk collection” of signals intelligence in the context of surveillance programmes under EO 12333. In particular, the CJEU found that such bulk collection was not delimited in a sufficiently clear and precise manner¹⁰¹, without however banning bulk collection as a matter of principle. Likewise, the ECtHR has expressly recognised that “*Article 8 of the Convention does not prohibit the use of bulk*

⁹⁵ Tele2 Sverige AB, § 103. See also Digital Rights, § 51; CJEU judgment of 5 April 2022, G.D. v. The Commissioner of the Garda Síochána and Others, *op. cit.*, § 94.

⁹⁶ Privacy International, § 80. See also Digital Rights Ireland and others, § 58; Tele2 Sverige AB, § 105; La Quadrature du Net and others, § 143.

⁹⁷ As defined in La Quadrature du Net and others, §§ 135-136.

⁹⁸ La Quadrature du Net and others, § 137.

⁹⁹ *Ibidem*.

¹⁰⁰ La Quadrature du Net and others, § 138. According to the CJEU, the instructions of public authorities in this context must also be subject to effective review, either by a court or by an independent administrative body with binding decision power in order to verify that a situation of serious threat to national security exists and that the conditions and safeguards which must be laid down are observed (La Quadrature du Net and others, § 139).

¹⁰¹ Schrems II, § 184.

*interception to protect national security and other essential national interests against serious external threats*¹⁰². The ECtHR has also underlined the usefulness of bulk interception, which it considers having a valuable technological capacity to identify new threats in the digital domain¹⁰³.

While the above decisions ended up with a negative assessment on the basis of the necessity test, the collection in bulk under EO 12333 combined with EO 14086 should be contrasted with the above collection of data on a generalised and indiscriminate basis sanctioned in the CJEU case law, which is tantamount to mass surveillance (Section 3.2.2(i)-(ii)).

Indeed, the so-called “mass surveillance” authorised under EU Member States national laws implementing Directive 2002/58¹⁰⁴ entailed the comprehensive collection of traffic and location data in a general and indiscriminate way so as to affect all persons using electronic communications services, outside the context of a serious threat to national security that is genuine, present or foreseeable. Such measures therefore applied to all such persons, including those *“for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with the objective of safeguarding national security and, in particular, without any relationship being established between the data which is to be transmitted and a threat to national security”*¹⁰⁵ (we underline).

Similarly, in assessing the necessity of the interferences caused by EU Directive 2006/24¹⁰⁶, the CJEU highlighted that such Directive *“covers in a generalised manner, all persons and all means of electronic communications as well as all traffic data without any differentiation, limitation or exception being made in light of the objective of fighting against serious crime”*¹⁰⁷ (we underline). The scope of the Directive was judged so broad that it entailed *“an interference with the fundamental rights of practically the entire European population”*¹⁰⁸.

In contrast, the bulk collection authorised under EO 12333, combined with EO 14086, may be defined as *“the collection of large quantities of signals intelligence*

¹⁰² ECtHR judgment of 25 May 2021, *Centrum för rättvisa v. Sweden*, No. 35252/08, § 261 (available [here](#)).

¹⁰³ *Big Brother Watch and Others*, § 323.

¹⁰⁴ See Directive (EU) 2002/58 of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (available [here](#)). Article 15(1) of that Directive foresaw the possibility for EU Member States to adopt legislative measures regarding the retention of data from electronic communications networks for a limited period justified on certain limitative grounds, such as national security. A number of EU Member States made use of such possibility, which has been heavily challenged in courts. The above Directive has been modified, notably by Directive 2006/24/EC cited below, which has also been challenged and ultimately annulled.

¹⁰⁵ *Privacy International*, § 80. See also *Digital Rights Ireland and others*, § 58; *Tele2 Sverige AB*, § 105; *La Quadrature du Net and others*, § 143.

¹⁰⁶ See Directive (EU) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 (available [here](#)). This so-called Data Retention Directive provided that EU Member States had to store all EU citizens' telecommunications data for a limited period of time so as to make them available to police authorities upon request. In *Digital Rights*, the CJEU declared this Directive invalid on grounds that the interference caused by such Directive exceeded the limits imposed by the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter (§ 69).

¹⁰⁷ *Digital Rights*, § 57.

¹⁰⁸ *Ibidem*, § 56.

*that, due to technical or operational considerations, is acquired without the use of discriminants (e.g. without using specific identifiers or selection terms)*¹⁰⁹.

Contrary to the above findings made in the context of mass surveillance in the EU, EO 14086 introduces a number of limitations on the recourse to the bulk collection of signals intelligence, which come in addition to the restrictions and safeguards that already apply under the necessity and proportionality principles (see Section 3.2.1). Such limitations should address the finding of the CJEU in Schrems II that the bulk collection under EO 12333 was not circumscribed in a sufficiently clear and precise manner¹¹⁰.

We have examined the applicable limitations below.

- It should first be noted that EO 14086 now expressly requires that targeted collection of signals intelligence be the principle. Targeted collection must therefore be prioritised and the bulk collection of signals intelligence may only be authorised where it is determined that *“the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection”*¹¹¹.
- The Adequacy Decision highlights that cases of possible bulk collection should therefore be limited, given that data may only be collected in bulk if it is located outside the US, i.e. in transit, on the basis of EO 12333 and that, even in such a scenario, the targeted collection of data must be prioritised¹¹².
- When the bulk collection is necessary, the collection of non-pertinent information must be minimised and methods and technical measures must be applied to limit the data collected to only what is necessary to advance the particular validated intelligence priority¹¹³.
- The use of intelligence that is collected in bulk is also further limited by the obligation for intelligence agencies to pursue one or more of the legitimate objectives included in the more restrictive and limitative list of EO 14086¹¹⁴. Such list further narrows down the list of legitimate objectives referred to above (in Section 3.2.1(i)) to some more fundamental objectives, such as the protection against terrorism, the taking of hostages, espionage, intelligence activities of foreign governments, threats posed by the use of weapons of mass destruction, cybersecurity threats, threats to governmental and military personnel and transnational criminal threats¹¹⁵.

The application of a narrower scope of legitimate objectives that may be pursued in collecting information in bulk forces intelligence agencies to

¹⁰⁹ See the definition provided by the Commission in footnote 223 of the Adequacy Decision.

¹¹⁰ Schrems II, § 184.

¹¹¹ Section 2(c)(ii)(A) of EO 14086.

¹¹² Recital 134 of the Adequacy Decision and Section 2(c)(ii)(A) of EO 14086.

¹¹³ Section 2(c)(ii)(A) of EO 14086.

¹¹⁴ Section 2(c)(ii)(B) of EO 14086.

¹¹⁵ Section 2(c)(ii)(B)(1)-(6) of EO 14086. It should be noted that, again, the President may extend the list of legitimate objectives *“in light of new national security imperatives”*, which would then be made publicly available by the Director of National Intelligence, unless such publication would pose a risk to the national security of the US (Section 2(c)(ii)(C) of EO 14086).

reconsider all the above proportionality requirements (*lato sensu*) and to make sure such collection maintains a link (be it indirect or even remote) with the legitimate objective pursued. To apply this obligation, it can be anticipated that intelligence agencies will rely on objective criteria to identify a larger public whose data is likely to reveal a link, at least indirect, with one of these legitimate objectives and to contribute in one way or another to its achievement¹¹⁶.

Such limitation is therefore different from the mass surveillance measures adopted under Directive 2002/58 in a way that it cannot be considered a “general and indiscriminate” collection of data, as described above.

As a result of this new privacy driven regime introduced by EO 14086, the scope of application of bulk collection has been narrowed down in light of the necessity principle. First, where bulk collection may be considered under EO 12333, intelligence agencies are now required to prioritise targeted collection and only resort to bulk collection where necessary. Second, EO 14086 imposes additional limitations as to the volume and types of data that may be collected and the purposes that may be pursued in conducting such bulk collection.

3.2.3 Remarks on the proportionality of the (bulk) collection of signals intelligence

It stems from the above descriptions and analysis that the necessity and proportionality principles enshrined in EO 14086 reflect to a large extent the principles applied in EU law, as further settled in the CJEU evolving case law.

The fact that some limitations in EO 14086 are drafted in a relatively broad manner and therefore leave room for appreciation by the intelligence agencies in their implementation should not lead to the questioning of an adequacy finding. As recalled above, the ECtHR has consistently held that the determination of the means to achieve the protection of national security (e.g. the decision to resort to bulk interception to identify threats to national security or against essential national interests¹¹⁷) falls within the national authorities’ margin of appreciation¹¹⁸. It is therefore legitimate that intelligence agencies enjoy a certain degree of manoeuvre in the operation of their activities .

In addition, it is important to recall that the implementation of EO 14086 by intelligence agencies, including in the context of bulk collection, will be subject to both *ex ante* and *ex post* supervision by the Privacy and Civil Liberties Oversight Board (“PCLOB”). The PCLOB is indeed an independent body authorised to review policies of the executive branch and their implementation, with a view to protect privacy and civil liberties¹¹⁹. It is inter alia tasked

¹¹⁶ As mentioned above, the CJEU requires that “*the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*”. See *Tele2 Sverige AB*, § 111. In line with the above, the ECtHR has recognised that “*the requirement of ‘reasonable suspicion’, which can be found in the Court’s case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence*” (*Big Brother Watch and Others*, § 348).

¹¹⁷ *Big Brother Watch and Others*, § 340.

¹¹⁸ ECtHR judgment of 29 June 2006, *Gabriele Weber and Cesar Richard Saravia v. Germany*, *op. cit.*, § 106 and the case law cited therein. See also inter alia ECtHR judgment of 30 January 2020, *Breyer v. Germany*, No. 50001/12, §§ 79 and 80 (available [here](#)) and case law cited therein.

¹¹⁹ See Recital 120 of the Adequacy Decision. The PCLOB is an agency instituted within the executive branch, whose board members are appointed by the President and confirmed by the Senate. More information on the PCLOB can be found [here](#).

with the monitoring of the intelligence agencies activities¹²⁰ and the review of the EO 14086 implementation by the intelligence agencies¹²¹ to ensure compliance with the principles and safeguards enshrined in EO 14086.

The implementation of EO 14086 will also be periodically reviewed by the Commission, including within one year after the entry into force of the Adequacy Decision to verify the implementation of all requirements enshrined in EO 14086 and the effective functioning of all elements contained in EO 14086 in practice¹²². Such monitoring by the Commission associated with its power to suspend, repeal or amend the Adequacy Decision, should create the right incentive for a correct implementation of EO 14086 by US intelligence agencies.

In any case, the Adequacy Decision must pass an equivalence test. Such test does not require the US to put in place a completely congruent legal system for the protection of personal data, but a level that is essentially equivalent to that of the EU legal system. The proportionality threshold to be met by the US is therefore not identical to that applicable to EU Member States. While the case law referred to above in relation to intra-EU surveillance may provide a reference point for the ruling of the CJEU on the US adequacy, the CJEU may not apply the exact same assessment. To our knowledge, the CJEU decisions in the field of surveillance programmes have indeed been limited so far to the review of Member States legislation and/or EU Directives allowing 'mass surveillance' (see Section 3.2.2 above), with the exception of Opinion 1/15 on the (then draft) PNR agreement between the EU and Canada, which however focuses on a specific processing activity of personal data.

3.3 Effective remedies

Pursuant to Article 45(2)(a) of the GDPR, the Commission must take account (among others) of "*effective and enforceable rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred*"¹²³ to determine whether an adequacy may be recognised.

On the basis of the CJEU's case law, the EDPB has translated this criterion into one of the four above European Essential Guarantees. Effective remedies must be available to the individuals whose personal data is transferred to a non-EEA country. According to the interpretation of the CJEU¹²⁴, this means that US law should offer individuals the possibility to pursue legal remedies to have access to their personal data or to obtain the rectification or erasure of such data to ensure the US legal system respects the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

In Schrems II, the CJEU concluded that the US law and the ombudsperson mechanism organised by the Privacy Shield did not ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter. Such conclusion was based on the following issues raised by the CJEU:

- (i) Some of the intelligence activities of the US public authorities were not covered by any administrative or judicial redress (e.g. collection of personal data in transit under

¹²⁰ See Recital 159 of the Adequacy Decision.

¹²¹ Sections 2(c)(iv)-(v) of EO 14086.

¹²² Recital 203 of the Adequacy Decision.

¹²³ This is also addressed in Recital 104 of the GDPR.

¹²⁴ Schrems I, § 95 and Schrems II, § 187.

EO 12333)¹²⁵ and, regarding the surveillance programmes under Section 702 of FISA and EO 12333, neither PPD-28 nor EO 12333 granted non-US individuals rights actionable in courts against US authorities¹²⁶; and

- (ii) The ombudsperson mechanism did not provide “*guarantees essentially equivalent to those required by Article 47 of the Charter*”¹²⁷ on grounds that the ombudsperson was not sufficiently independent from the US executive branch¹²⁸ and had no binding enforcement power vis-à-vis the intelligence agencies, except on the basis of a political commitment from the US government, which did however not provide any legal safeguards¹²⁹.

In the following section, we will look into how the US has addressed the above concerns raised by the CJEU so as to enable the Commission to consider that the requirements of Article 47 of the Charter, as interpreted by the CJEU, are met. We will first provide an overview of the redress mechanism introduced by EO 14086 and the AG Regulation (Section 3.3.1). We will then deep dive into this mechanism in light of the above CJEU requirements (Sections 3.3.2 and 3.3.3) before concluding with the brief analysis of the minimum requirements of the ECtHR case law (Section 3.3.4).

3.3.1 US redress mechanisms

First, it is important to note the redress avenues that were already available to non-US citizens prior to EO 14086 to bring legal actions in relation to the processing of their personal data by the US intelligence authorities¹³⁰. Non-US individuals may also avail themselves of the Freedom of Information Act (or “**FOIA**”), which allows them to request access to existing federal agency records, without having to demonstrate any harm or injury¹³¹.

The Commission has considered the above in its Adequacy Decision and concludes that together with the EO 14086, which we examined hereafter, such mechanisms allow data subjects to obtain access to their personal data, to have the lawfulness of the US intelligence authorities reviewed and to obtain remedies in case a violation would be found, including through the rectification or erasure of their personal data¹³².

For the purpose of our review, we focused our attention on the new US redress mechanism introduced by EO 14086 supplemented by the AG Regulation, which constitutes an additional specific avenue for data subjects to seek redress through a two-level administrative mechanism. This new redress mechanism fills in the gaps of the US judicial system, as highlighted by the CJEU in Schrems II¹³³ and should therefore be in a position to pass the essential equivalence test in light of Article 47 of the Charter. In particular, the creation of the DPRC introduces three main improvements, as further described below: (a) the newly created DPRC will be an independent tribunal, (b) it will have investigatory,

¹²⁵ Schrems II, § 191.

¹²⁶ Schrems II, § 192.

¹²⁷ Schrems II, § 197.

¹²⁸ Schrems II, § 195.

¹²⁹ Schrems II, § 196.

¹³⁰ See Recitals 187 and following of the Adequacy Decision.

¹³¹ See Recital 191 of the Adequacy Decision and 5 U.S.C. § 552. It should be noted that the exercise of this right is subject to limitations, e.g. in relation to classified information.

¹³² Recital 167 of the Adequacy Decision.

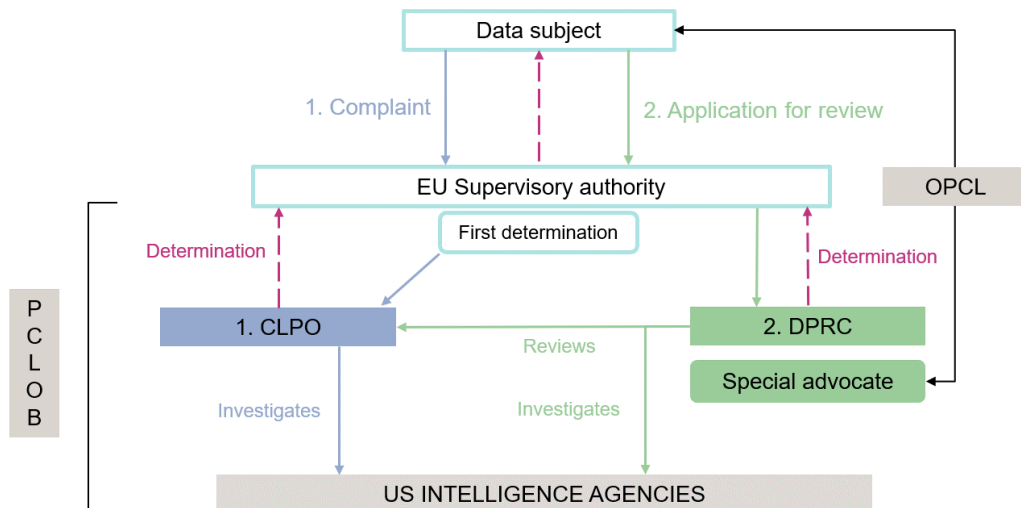
¹³³ Schrems II, § 190 and following.

adjudicative and remedial powers and (c) it will adopt decisions binding on intelligence agencies.

(i) The new two-layer redress mechanism

The redress mechanism established by EO 14086 and the AG Regulation allows individuals to lodge a complaint about an alleged violation of US law governing US intelligence activities that adversely affects their privacy and civil liberties interest, by submitting it to the supervisory authority of one of the EU Member States. The seized EU supervisory authority will in turn communicate directly with the US authorities in charge, after verification of the complainant's identity and an initial qualification determination of his/her complaint¹³⁴.

As shown in the diagram below, the submission of the individual's complaint to the EU supervisory authority triggers a two-layer mechanism with (a) a review of the complaint being carried out by the CLPO, which renders a decision on whether a violation has been found and on the appropriate remediations; and (b) upon request by the individual or any element of the intelligence community, a review of the CLPO's decision by the DPRC.



This diagram can be further explained as follows:

1 At the level of the CLPO:

- Upon receipt of a complaint, the relevant EU-based supervisory authority will verify the identity of the complainant and conduct an initial qualification determination, upon which it will transmit it to the CLPO.
- The CLPO must then carry out the initial investigation of the complaint. For that purpose, the CLPO has access to all relevant information and can require the assistance of the privacy and civil liberties officials

¹³⁴ Section 4(k)(v) of EO 14086. Recital 198 of the Adequacy Decision recalls that the Commission's adequacy decisions are binding on all organs of EU Member States to which such decisions are addressed, including their independent supervisory authorities. EU Member States and their supervisory authorities must therefore take the necessary measures to implement the above mechanism.

within the elements of the intelligence community¹³⁵. During the entire process, the CLPO is required to document its review¹³⁶.

- As part of its review, the CLPO must confirm whether a violation of US law has been found and, in such case, what remediation actions must be undertaken. These so-called “determinations” are binding on the intelligence agencies concerned¹³⁷. The CLPO is also required to issue a classified decision that explains the basis for its findings and determinations in each particular case¹³⁸.
- Upon completion of its review, the CLPO informs the complainant (via the EU-based supervisory authority concerned) (i) either that “the review did not identify any covered violations” or “the CLPO issued a determination requiring appropriate remediation”, and (ii) in both cases, of the possibility of appeal of such determination before the DPRC¹³⁹.

2 At the level of the DPRC:

- Within 60 days after receiving the above information, the complainant (as well as any element of the intelligence community) may file an application for appeal before the DPRC, again through the supervisory authority of his/her Member State¹⁴⁰.
- The DPRC is then seized and a special advocate is selected¹⁴¹ to represent the complainant’s interests and make sure the panel is adequately informed about all relevant issues of law and fact¹⁴². To that end, the special advocate has access to the record of the CLPO’s review and any information provided to the DPRC panel by any element of the intelligence community (even classified one)¹⁴³ and can exchange in writing with the complainant to seek/receive further information¹⁴⁴.

¹³⁵ Section 3(c)(iii) of EO 14086.

¹³⁶ Section 3(c)(i)(F)-(G) of EO 14086.

¹³⁷ Section 3(c)(ii) of EO 14086.

¹³⁸ Section 3(c)(i)(F) of EO 14086.

¹³⁹ Section 3(c)(i)(E) of EO 14086.

¹⁴⁰ Section 201.6(a) of the AG Regulation. Given the low level admissibility threshold to appeal CLPO’s determinations, it is likely that claimants will exercise their right of appeal to enable further investigation as to the protection afforded to their data. In doing so, individuals may be represented by a legal counsel in the context of their appeal application (see Section 201.6(b) of the AG Regulation).

¹⁴¹ To be appointed, special advocates (i) may not have been employees of the executive branch within the two years preceding their appointment, (ii) must have appropriate experience in the fields of data privacy and national security law, and (iii) must be experienced attorneys, active members in good standing of the bar and duly licensed to practice law (See Section 201.4 of the AG Regulation).

¹⁴² Recital 180 of the Adequacy Decision, Section 3(d)(i)(C) of EO 14086 and Section 201.8(e) of the AG Regulation. While representing the interests of the claimant, the special advocate will however not act as the agent of such complainant and they will not entertain any attorney-client relationship (Section 201.8(b) of the AG Regulation).

¹⁴³ Sections 201.8(c) and 201.11 of the AG Regulation.

¹⁴⁴ Questions from the special advocate to the complainant or his/her counsel will be first submitted to the Office of Privacy and Civil Liberties (“OPCL”), which will review such questions in consultation with relevant elements of intelligence community to ensure no classified/privileged/protected information is disclosed to the complainant (Section 201.8(d)(2) of the AG Regulation).

- The DPRC reviews the determinations of the CLPO and may either (i) find that there has been no intelligence activities involving the personal data of the complainant, (ii) confirm the determinations of the CLPO based on substantial evidence, or (iii) issue its own determinations (i.e. determine whether a violation of US law occur and the appropriate remediation), in case it disagrees with those of the CLPO¹⁴⁵. Again, such decision is binding on the intelligence agencies concerned¹⁴⁶.
- The DPRC's determination is communicated to the CLPO in all cases¹⁴⁷. Where the appeal is triggered by the complainant, he/she is informed that "the review did not identify any covered violations" or "the DPRC issued a determination requiring appropriate remediation"¹⁴⁸, through the relevant EU-based supervisory authority¹⁴⁹.
- A record of the DPRC determinations, including all information reviewed by the DPRC is maintained by the OPCL¹⁵⁰. The US Secretary of Commerce is also required to maintain a record for each complainant and verify at least every five years whether the information that has been subject to the review of the DPRC has been declassified, in which case it must notify the relevant individual thereof so that he/she can exercise his/her right of access to such record under FOIA (see beginning of Section 3.3.1 above)¹⁵¹.

(ii) Additional guarantees through oversight

It is commonly understood and accepted that, due to its particularly sensitive nature, the field of national security is highly protected and characterised by less transparency on intelligence activities being conducted¹⁵².

As mentioned above¹⁵³, to counterbalance such opacity and to offer safeguards that the law will be complied with, EO 14086 introduces an independent and regular oversight mechanism by the PCLOB, which is inter alia tasked with the monitoring

¹⁴⁵ Section 3(d)(i)(E) of EO 14086 and Section 201.9(c)-(e) of the AG Regulation.

¹⁴⁶ Section 3(d)(ii) of EO 14086 and Section 201.9(g) of the AG Regulation.

¹⁴⁷ Section 3(d)(i)(G) of EO 14086 and Section 201.9(h) of the AG Regulation.

¹⁴⁸ See Section 4(a) of EO 14086 for the definition of "appropriate determination".

¹⁴⁹ Section 3(d)(i)(H) of EO 14086 and Section 201.9(h) of the AG Regulation.

¹⁵⁰ Section 201.9(J) of the AG Regulation. The OPCL is the office instituted within the Department of Justice (DoJ) to provide legal advice and guidance to the DoJ, to ensure the DoJ's privacy compliance and to assist the Chief Privacy and Civil Liberties Officer (CPCLO) who is the main advisor of the Attorney General on privacy and civil liberties matters. More on the OPCL can be found [here](#).

¹⁵¹ Section 3(d)(v) of EO 14086.

¹⁵² This has notably been recognised by the ECtHR, which ruled that "*having regard to the imperative need for secrecy, in particular at the stages of initial authorisation and conducting signals intelligence, the arrangement described above contains relevant safeguards against arbitrariness and must be accepted as an inevitable limitation on the authorisation procedure's transparency*" (See ECtHR judgment of 25 May 2021, *Centrum för rättvisa v. Sweden*, No. 35252/08, §297 (available [here](#))). Advocate General Pitruzzella also highlighted the peculiar nature of intelligence activities, recognising that the modus operandi of intelligence services "*is typically non-transparent*" (see the Opinion of Advocate General Pitruzzella of 27 January 2022, *Ligue des droits humains v. Conseil des ministres*, C-817/19, ECLI:EU:C:2022:65, § 262 (available [here](#))).

¹⁵³ See Section 3.2.3.

of the intelligence agencies activities and the review of EO 14086 implementation by the intelligence agencies¹⁵⁴.

The PCLOB is also responsible to review the CLPO's and DPRC's activities and, in particular, to assess whether (a) complaints were processed in a timely manner, (b) the CLPO and the DPRC were granted full access to the necessary information, (c) whether the safeguards of EO 14086 have been properly considered by the CLPO and the DPRC (including those described in Section 3.2 above), and (d) whether the intelligence agencies have fully complied with the decisions of the CLPO and DPRC¹⁵⁵. Following such assessment, the PCLOB may issue recommendations to the relevant stakeholders of the intelligence community, which have to be implemented or otherwise addressed¹⁵⁶.

The outcome of this review is also consolidated in a declassified report that is made publicly available, in addition to the PCLOB's annual public certification confirming that the redress mechanism complies with the requirements of EO 14086¹⁵⁷.

For the purpose of carrying its tasks, the PCLOB has access to all relevant information and data from the federal government, including classified information and may even conduct interviews and hear testimony from representatives of the intelligence agencies¹⁵⁸.

3.3.2 Scope and availability of the redress mechanism

As mentioned above¹⁵⁹, one of the criticisms of the CJEU in Schrems II was that no administrative or judicial redress was made available to non-US citizens, in particular with regard to the US intelligence activities under EO 12 333 (in transit) and Section 702 of FISA.

With the new redress mechanism described in Section 3.3.1, such criticism has now been thoroughly addressed by EO 14086 and the AG Regulation as explained below.

First, as was already the case with the ombudsperson mechanism, the new redress mechanism of EO 14086 and the AG Regulation is open to any individual that is located in the EU¹⁶⁰, regardless of his/her nationality. Indeed, the alleged violation must simply pertain to *“personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state”*¹⁶¹. Based on the information available at this stage, it is our understanding that access to this redress mechanism will be free of charge for the complainant. The fact that individuals may lodge their complaint locally, via their national supervisory authority also participates to a broad access to such redress mechanism.

¹⁵⁴ Recital 159 of the Adequacy Decision.

¹⁵⁵ Section 3(e) of EO 14086.

¹⁵⁶ Section 3(e)(iv) of EO 14086.

¹⁵⁷ Section 3(e)(iii)(B)-(C) of EO 14086.

¹⁵⁸ 42 U.S.C. § 2000ee (g).

¹⁵⁹ See Section 3.3(i) above.

¹⁶⁰ As part of the implementation of the redress mechanism, the US Attorney General is due to designate the European Economic Area (i.e. the EU, Iceland, the Lichtenstein and Norway) as “qualifying states” pursuant to Section 3(f) of EO 14086.

¹⁶¹ Section 4(k)(i) of EO 14086.

Second, the redress mechanism covers the processing of complaints “concerning United States signals intelligence activities for any covered violation of United States law”¹⁶², including Section 702 of FISA and EO 12333. Indeed, a “covered violation” is broadly defined by EO 14086 as¹⁶³:

- (i) any violation of (a) the US Constitution, (b) the applicable sections of FISA, EO 12333 and EO 14086, (c) any applicable agency procedures and policies pursuant to such rules, (d) any successor statute, order, policies or procedures, or (e) any other statute, order, policies or procedures providing privacy and civil liberties safeguards with respect to US signals intelligence activities, as identified in a list published and updated by the US Attorney General,
- (ii) that arises from signals intelligence activities, i.e. covering the collection of electronic communications and data from information systems both within and outside the US¹⁶⁴,
- (iii) regarding data transferred to the US from a qualifying state (i.e. the EEA), which adversely affects the complainant’s individual privacy and civil liberties interests.

Third, EO 14086 and the AG Regulation apply low admissibility requirements, as:

- Individuals are not required to evidence that their personal data has actually been subject to US signals intelligence activities (which would have otherwise proven impossible in practice, given the lack of information provided to individuals in the field of national security)¹⁶⁵.
- Only a few information must be provided in a general manner, i.e. (a) the personal data and means by which such personal data were “reasonably believed” to be transferred to the US, (b) only if known, the US government entities “believed to be involved”, (c) information that forms the basis for alleging that a violation of US law occurred, (d) the relief sought and (e) any other measures that may have been pursued by the complainant to obtain such relief and the response received¹⁶⁶.
- The only grounds for dismissing a complaint being in case the complaint is frivolous, vexatious or made in bad faith¹⁶⁷.

This low level of admissibility of the complaint, especially the fact that data subjects are not required to evidence any harm or that their data has in fact been subject to intelligence activities, should help compensate the lack of notification that individuals are subject to surveillance measures, as it should enable individuals to effectively exercise their rights to remedies in the protected field of national security.

It is important to note in that respect that the CJEU has accepted that individuals may benefit from effective legal remedies without being notified of the surveillance measure they have been subject to, to the extent that and as soon as such notification is liable to jeopardise the

¹⁶² Section 3(a) of EO 14086.

¹⁶³ Section 4(d)(i) of EO 14086.

¹⁶⁴ Recital 118 of the Adequacy Decision.

¹⁶⁵ Section 5(k)(ii) of the AG Regulation.

¹⁶⁶ *Ibidem*.

¹⁶⁷ Section 4(k)(iii) of EO 14086.

tasks for which the surveillance authorities are responsible¹⁶⁸. Similarly, the ECtHR found that *“there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications”*.

Given the broad possibility for individuals to bring a claim in case they suspect their rights to privacy have been violated, the lack of notification should be adequately remedied and the data subjects’ exercise of their rights not impeded.

3.3.3 The redress mechanism in light of Article 47 of the Charter

The CJEU has long held that the principle of effective judicial protection is a general principle of EU law *“which has been enshrined in Articles 6 and 13 of the ECHR and which has also been reaffirmed by Article 47 of the Charter of fundamental rights of the European Union”*¹⁶⁹.

The notion of effective judicial protection is closely linked to that of “tribunal” under Article 47 of the Charter. The first paragraph of that article requires individuals whose fundamental rights are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article¹⁷⁰.

As mentioned above¹⁷¹, another set of the CJEU’s criticisms in Schrems II was that the specific ombudsperson mechanism of the Privacy Shield did not remedy the deficiencies highlighted in Section 3.3(i) so that the US did not offer guarantees essentially equivalent to those provided by Article 47 of the Charter. In particular, the CJEU found that such mechanism was not meeting the criterion of independence imposed by the second paragraph of Article 47 of the Charter and that the ombudsperson did not have binding decision power on intelligence agencies.

In the following sections, we review how EO 14086 and the AG Regulation have addressed the concerns raised by the CJEU in Schrems II, by assessing whether the DPRC (i) can be considered as a tribunal within the meaning of Article 47 of the Charter, (ii) meets the requirement of independence, and (iii) adopts decisions that are binding on the intelligence services.

We have intentionally carved-out the analysis of the CLPO from our review in the sections below to focus on the DPRC. While the CLPO offers certain guarantees of independence

¹⁶⁸ The CJEU has indeed admitted that the notification of individuals that they are subject to surveillance measures may be subject to exceptions in certain circumstances (La Quadrature du Net and others, §§ 190-191. See also Opinion 1/15, §§ 219-220 and Tele2 Sverige AB, § 121 and the case law cited therein).

¹⁶⁹ CJEU judgment of 17 July 2009, Mono Car Styling SA v. Dervis Odemis and Others, C-12/08, ECLI:EU:C:2009:466, §47 (available [here](#)); CJEU judgment of 28 July 2011, Samba Diouf v. Ministre du Travail, de l’Emploi et de l’Immigration, C-69/10, ECLI:EU:C:2011:524, § 49 (available [here](#)).

¹⁷⁰ Schrems I, § 95 (available [here](#)); CJEU judgment of 23 April 1986, Les Verts v. Parliament, C-294/83, ECLI:EU:C:1986:166, § 23 (available [here](#)); CJEU judgment of 15 May 1986, Marguerite Johnston v. Chief Constable of the Royal Ulster Constabulary, C-222/84, ECLI:EU:C:1986:206, §§ 18 and 19 (available [here](#)); CJEU judgment of 15 October 1987, Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v. Georges Heylens and others, C-222/86, ECLI:EU:C:1987:442, §14 (available [here](#)).

¹⁷¹ See Section 3.3(i)(ii) above.

and impartiality¹⁷², it is not subject to the requirements of Article 47 of the Charter. Indeed, it must rather be seen as the first step of lodging a complaint with a State authority, which is the closest to the stakeholders and thus in a better position to investigate a complaint and respond to it.

In that respect, the fact that the CLPO qualifies or not as a “tribunal” within the meaning of Article 47 of the Charter should not affect the essential equivalence of the new US redress mechanism. Having two levels of jurisdiction is indeed not a criterion for the provision of effective legal remedies under the Charter. Neither Article 47(1) of the Charter nor Article 6(1) of the ECHR require States to offer possibilities for appeal, cassation or constitutional jurisdiction. This is confirmed by the CJEU, which held that “*the principle of effective judicial protection affords an individual a right of access to a court or tribunal but not to a number of levels of jurisdiction*”¹⁷³.

(i) The DPRC as a “tribunal”

The preliminary question that must be answered as part of this assessment is whether a body like the DPRC may be considered as a “tribunal” within the meaning of Article 47 of the Charter.

While Article 47 of the Charter uses the concept of a “tribunal” (or “court” in some language versions of the Charter¹⁷⁴), the CJEU generally refers to “a body” that must meet certain criteria¹⁷⁵. This notion has a broader scope than that of “tribunal” or “court”, which have a judicial connotation.

Also in Schrems II, the CJEU considered that an effective judicial protection can be ensured not only by a tribunal or court, but also by “a body” (i.e. not necessarily a judicial authority), provided such body offers guarantees that are essentially equivalent to those provided by Article 47 of the Charter¹⁷⁶. This interpretation is supported by the wording of Article 45(2)(a) of the GDPR, as recalled by CJEU in Schrems II¹⁷⁷, which requires the Commission to take into account “*any effective administrative and judicial redress*” in its adequacy assessment.

In addition, the administrative (versus judicial) nature of the DPRC is actually rendering the protection afforded by EO 14086 and the AG Regulation effective in the field of national security. Indeed, privacy cases face legal hurdles before the ordinary US courts, due to the so-called “standing” barrier. Specifically, to bring suit before US federal courts, plaintiffs must demonstrate (i) an actual injury-in-fact

¹⁷² Although the CLPO is an integral part of the ODNI, this function is protected by certain safeguards of independence and impartiality. For instance, the CLPO can only be dismissed by the Director of National Intelligence for cause, intelligence agencies and the Director are prohibited from impeding or improperly influencing the CLPO’s review and the CLPO must apply the law impartially (see Recitals 171 and 172 of the Adequacy Decision).

¹⁷³ CJEU judgment of 28 July 2011, *Samba Diouf v. Ministre du Travail, de l’Emploi et de l’Immigration*, *op. cit.*, § 69 read in combination with § 48-49 (available [here](#)).

¹⁷⁴ The Dutch version of Article 47 of the Charter refers to “Gerecht” and the German version to “Gericht”.

¹⁷⁵ In an Opinion delivered in March 2022, Advocate General Bobek recalled the jurisprudence of the CJEU on the notion of tribunal, confirming that “*such a body must be established by law; be permanent; have compulsory jurisdiction; feature a proceeding that is inter partes; apply rules of law; and be independent (internally and externally)*” (we underline). See Opinion of Advocate General Bobek of 18 March 2022, *FN and Others v. Übernahmekommission*, C-546/18, ECLI:EU:C:2021:219, § 47 and the case-law cited therein (available [here](#)), including CJEU judgment of 27 February 2018, *Associação Sindical dos Juizes Portugueses*, C-64/16, ECLI:EU:C:2018:117, § 38 (available [here](#)).

¹⁷⁶ Schrems II, § 197.

¹⁷⁷ Schrems II, § 188.

having been suffered (not merely a heightened risk of a future injury), (ii) a reasonable likelihood of a causal link between such injury and the conduct challenged before the court, and (iii) a likelihood that a favourable decision by the court will address or remediate such injury¹⁷⁸.

Given the opacity that characterises the field of national surveillance, it would *de facto* prove impossible for individuals to evidence that they have been subject to surveillance measures in the US that have resulted in concrete harm or injury, thus making it challenging for individuals to bring a privacy lawsuit in an ordinary US court.

Conversely, as explained in Section 3.3.2, the submission of application for review to the DPRC is subject to low admissibility thresholds and does not require to prove any of the above elements.

(ii) Independent

As mentioned above, Article 47 of the Charter enshrines the right to a fair hearing by an independent and impartial tribunal. When assessing the compliance of national systems with this provision, the CJEU refers to both internal independence (i.e. from the parties subject to its authority) and external independence (i.e. from the legal system itself and its management bodies)¹⁷⁹.

The requirement for internal independence is closely linked to impartiality and imposes “*objectivity and the absence of any interest in the outcome of the proceedings apart from the strict interpretation of the rule of law*”¹⁸⁰.

According to settled case law, the criterion of external independence must be understood as requiring that the body concerned “*exercises 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*”¹⁸¹.

In addition, the CJEU recalls that the principle of the separation of powers must be ensured so that the “tribunal” remains independent in relation to the legislative and the executive powers¹⁸².

¹⁷⁸ See footnote 364 of the Adequacy Decision and the relevant US case law (*Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 472 (1982); *Gladstone, Realtors v. Village of Bellwood*, 441 U.S. 91, 99 (1979); *Simon v. Eastern Kentucky Welfare Rights Organization*, 426 U.S. 26, 37 (1976)).

¹⁷⁹ CJEU judgment of 19 November 2019, A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court), C-585/18, C-624/18 and C-625/18, ECLI:EU:C:2019:982, §§ 121-122 and the case law cited therein (available [here](#)).

¹⁸⁰ CJEU judgment of 25 July 2018, Minister for Justice and Equality, C-216/18 PPU, ECLI:EU:C:2018:586, § 65 (available [here](#)) and CJEU judgment of 19 September 2006, *Graham J. Wilson v. Ordre des avocats du barreau de Luxembourg*, C-506/04, ECLI:EU:C:2006:587, § 52 and the case-law cited (available [here](#)).

¹⁸¹ CJEU judgment of 25 July 2018, Minister for Justice and Equality, C-216/18 PPU, ECLI:EU:C:2018:586, § 63 and the case-law cited (available [here](#)).

¹⁸² CJEU judgment of 19 November 2019, A. K. and Others, *op. cit.*, § 124; CJEU judgment of 10 November 2016, *Openbaar Ministerie v. Krzysztof Marek Poltorak*, C-452/16 PPU, ECLI:EU:C:2016:858, § 35 (available [here](#)).

In that respect, the CJEU considers that the above requirements must be supported by rules that safeguard such independence, including as regards the appointment of the members of the body and the grounds for their dismissal¹⁸³.

It is on the basis of settled case law, as outlined above that the CJEU questioned the independence of the ombudsman in Schrems II. In particular, the CJEU found that the ombudsperson was not sufficiently independent, on grounds that (i) he had to report to the executive (i.e. the Secretary of the State) and was an integral part of the US State Department and that (ii) there were no guarantees with regards to the dismissal or revocation of his appointment¹⁸⁴.

The new US redress mechanism embodied by the DPRC addresses the above concerns.

- (i) While the DPRC is established by the Attorney General¹⁸⁵, which forms an integral part of the US Department of Justice, the Attorney General is barred from interfering with the activities of the DPRC¹⁸⁶. In particular, the AG Regulation expressly provides that the DPRC shall not be subject to the day-to-day supervision of the Attorney General¹⁸⁷.
- (ii) The Attorney General may also not remove judges from a DPRC panel, revoke DPRC judges' appointment prior to the end of their mandate or take any other adverse action against judges arising from their service on the DPRC, except for cause¹⁸⁸ and after taking due account of the standards applicable to federal judges¹⁸⁹.

Regarding point (i) above, it should be noted that the fact that the DPRC's judges are appointed by the US Attorney General that is a member of the executive should not undermine their independence. Indeed, the case law of the CJEU has ruled that *"the mere fact that those judges were appointed by the President of the Republic does not give rise to a relationship of subordination of the former to the latter or to doubts as to the former's impartiality, if, once appointed, they are free from influence or pressure when carrying out their role"*¹⁹⁰.

Hence, a body will not be directly considered as not respecting the independence criterion just on grounds that the executive decides on the appointment (and correlatively, the dismissal) of such body, to the extent such decision does not *"give rise to reasonable doubts, in the minds of individuals, as to the imperviousness of*

¹⁸³ CJEU judgment of 19 November 2019, A. K. and Others, *op. cit.*, § 123 and the case-law cited (available [here](#)).

¹⁸⁴ Schrems II, § 195.

¹⁸⁵ Such appointment being made in consultation with the PCLOB, the Secretary of Commerce and the Director of National Intelligence (Recital 177 of the Adequacy Decision).

¹⁸⁶ Section 3(d)(iv) of EO 14086.

¹⁸⁷ Section 201.7(d) of the AG Regulation.

¹⁸⁸ I.e. for instances of misconduct, malfeasance, breach of security, neglect of duty or incapacity.

¹⁸⁹ Section 201.7(d) of the AG Regulation.

¹⁹⁰ CJEU judgment of 31 January 2013, H. I. D. and B. A. v. Refugee Applications Commissioner and Others, C-175/11, ECLI:EU:C:2013:45, §133 (available [here](#)). See also CJEU judgment of 24 June 2019, European Commission v. Republic of Poland, C-619/18, ECLI:EU:C:2019:531, § 111 (available [here](#)).

*the judges concerned to external factors and as to their neutrality with respect to the interests before them*¹⁹¹.

In that regard, the new US law imposes additional requirements, which have the effects of safeguarding the internal and external independence of the DPRC, including the following:

- Despite the administrative nature of the DPRC, judges sitting on the DPRC are appointed on the basis of the criteria used to assess federal judge candidates¹⁹².
- The judges must be active members in good standing of the Bar and duly licensed to practice law (with appropriate experience in privacy and national security law)¹⁹³.
- The DPRC judges may not be employees of, or have official duties for, the executive power within the two years preceding their appointment and during the term of their appointment¹⁹⁴.
- The judges on a DPRC panel must behave in accordance with the Code of Conduct for US Judges that sets out ethical principles and guidelines among others in relation to judicial integrity, independence and impartiality¹⁹⁵. In particular, they must consider complainants' applications for review in a manner that is *inter alia* impartial¹⁹⁶.
- The DPRC must adopt its own rules of procedures, which must be consistent with EO 14086¹⁹⁷.

(iii) With legally binding enforcement powers

As recalled above¹⁹⁸, the CJEU also criticised the fact that the ombudsperson was deprived from any power to adopt decisions binding upon intelligence agencies.

This criticism has been taken into account in the new redress mechanism, as the DPRC has been granted expressly binding enforcement powers so that its decisions are final and binding on the intelligence agencies concerned by its decision¹⁹⁹, with the PCLOB being tasked with reviewing whether intelligence agencies have fully and correctly complied with the DPRC's determinations²⁰⁰.

¹⁹¹ CJEU judgment of 24 June 2019, A. K. and Others v. Sąd Najwyższy, CP v. Sąd Najwyższy and DO v. Sąd Najwyższy, C-585/18, C-624/18 and C-625/18, ECLI:EU:C:2019:982, § 134 (available [here](#)).

¹⁹² Section 201.3(b) of the AG Regulation.

¹⁹³ *Ibidem*.

¹⁹⁴ Section 3(d)(i)(A) of EO 14086 and Section 201.3(a) and (c) of the AG Regulation. Judges are nevertheless allowed to take part in extrajudicial activities (e.g. business, financial, non-profit fundraising, fiduciary activities and the practice of law) to the extent it does not interfere with the impartiality of the judge or the effectiveness and independence of the DPRC (Section 201.7(c) of the AG Regulation).

¹⁹⁵ Section 201.7(c) of the AG Regulation.

¹⁹⁶ Section 201.9(a) of the AG Regulation.

¹⁹⁷ Section 201.3(d) of the AG Regulation.

¹⁹⁸ See beginning of Section 3.3 above.

¹⁹⁹ Section 3(d)(ii) of EO 14086 and Section 201.9(g) of the AG Regulation.

²⁰⁰ Section 3(e)(i) and (iv) of EO 14086.

3.3.4 Effective legal protection in light of the ECtHR case-law

While the Schrems II decision provides the roadmap for the surveillance aspects of EO 14086, in the course of our review, we noted that other criteria stemming from the ECtHR case law have also been addressed.

As mentioned above²⁰¹, this is relevant since, pursuant to Article 52(3) of the Charter, the meaning and scope of the rights protected by the Charter are to be the same as those corresponding rights guaranteed by the ECHR. The CJEU therefore recognises that “*account must [...] be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection*”²⁰².

In particular, in relation to the right to effective legal protection, the CJEU considered that its interpretation of Article 47 of the Charter must safeguard a level of protection which does not fall below the level of protection established in the corresponding Articles 6(1) and 13 of the ECHR, as interpreted by the ECtHR²⁰³.

As recalled by the EDPB in its Recommendations 02/2020²⁰⁴, the ECtHR has developed a series of criteria to assess whether a court offers sufficient redress possibilities in light of the ECHR. In particular, the court must be “*an independent and impartial body, which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers and that there is no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the court should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance*”²⁰⁵.

Based on the above descriptions and analysis, it can be confirmed that the minimum level of protection set out by the ECtHR is essentially met by the DPRC:

- the DPRC must act in an independent and impartial manner (see Section 3.3.3(ii) above);
- the DPRC must adopt its own rules of procedure (see Section 3.3.3(ii) above);
- the judges sitting on the DPRC must at least be experienced lawyers (see Section 3.3.3(ii) above), with half of the panel who must have prior judicial experience²⁰⁶;
- EU individuals who wish to lodge an application for review of the CLPO’s decision before the DPRC may do so without justification²⁰⁷. There are only low admissibility criteria that apply for the lodging of the initial complaint, which do not constitute an evidential burden individuals must overcome (see Section 3.3.2);

²⁰¹ See footnote 6.

²⁰² La Quadrature du Net and others, § 124.

²⁰³ CJEU judgment of 24 June 2019, A. K. and Others v. Sąd Najwyższy, CP v. Sąd Najwyższy and DO v. Sąd Najwyższy, C-585/18, C-624/18 and C-625/18, ECLI:EU:C:2019:982, §§ 117-118 (available [here](#)).

²⁰⁴ EDPB Recommendations 02/2020, *op. cit.*, § 45.

²⁰⁵ *Ibidem*. See also the case-law referred therein (ECtHR judgment of 18 May 2010, Kennedy v. the United Kingdom, No. 26839/05, §§ 167 and 190 (available [here](#))).

²⁰⁶ Recital 177 of the Adequacy Decision.

²⁰⁷ Recital 176 of the Adequacy Decision.

- in its review process, the DPRC has access to any information it requires, including classified information²⁰⁸; and
- The DPRC has binding enforcement powers to require intelligence agencies to implement any remediation actions deemed appropriate by the DPRC (see Section 3.3.3(iii)).

These elements again demonstrate the improvement which EO 14086 is bringing in terms of protection afforded to citizens based in the EU whose personal data could be accessed and processed by intelligence agencies.

* *
*

With the adoption of EO 14086 (and the AG Regulation), the US have made a significant step towards the EU and its legal protection (and exceptions to) the individuals' fundamental rights to data protection. These efforts must be reviewed in consideration of the sovereignty of the US. Together, EO 14086 and the AG Regulation respond to the concerns raised by the CJEU in its Schrems II judgment. It stems from our analysis that it can be argued that the essential equivalence as identified by the Commission is met in relation to the points discussed in our legal review.

The final adoption of the Adequacy Decision is made conditional upon the proper implementation of EO 14086 and the AG Regulation by the US government and its intelligence agencies. It will be essential to consider such implementation when it will be public.

Upon its adoption, the Adequacy Decision will produce legal effects and be binding on all EU Member States and their organs, until it is withdrawn, annulled or declared invalid²⁰⁹. Given the history of US adequacy, it is likely that the Adequacy Decision will be challenged before the CJEU. While the CJEU case law is quite evolutive and the threshold for essential equivalence is not entirely circumscribed, we are confident that the progress achieved by the boundaries and other protections granted by the US will be recognised.

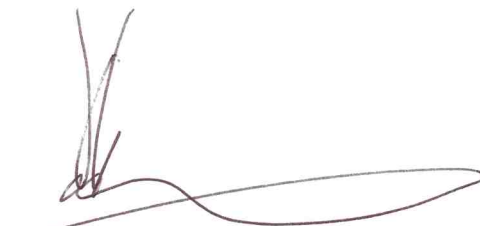
*

The above legal analysis is strictly limited to the matters stated herein as at the date it was prepared and is not to be read as extending by implication to any other matters not specifically referred to herein or changes or developments related to the matters herein after the above date. It is addressed to and has been prepared solely for the benefit of DigitalEurope in connection with its request to be provided with a legal analysis on certain aspects of the Adequacy Decision (as described above). This legal analysis is not to be relied upon by anyone else than DigitalEurope and we accept no responsibility or legal liability, whether in contract, statutory duty, tort or otherwise, to any person other than DigitalEurope in relation to the content of this legal analysis.

Yours sincerely,



Manon Habets
Associate



Tanguy Van Overstraeten
Partner

²⁰⁸ Recital 181 of the Adequacy Decision.

²⁰⁹ Recital 197 of the Adequacy Decision.