TASK FORCE REPORT

RECONSTITUTIONALISING PRIVACY

EU-US data transfers and their impact on the rule of law, rights and trust

Rapporteurs

Franziska Boehm
Sergio Carrera
Valsamis Mitsilegas

This CEPS Task Force was co-organised by CEPS, FIZ and the University of Liverpool. The views and the overall content of the findings, as well as the policy recommendations presented in this final Task Force Report are exclusively attributable to the authors. It has duly considered and assessed the presentations, inputs and contributions of a group of Task Force experts coming from the private sector, academia and civil society, as well as EU and national officials. A list of participants is provided at the end of this report.

This final version of the Task Force Report does not represent the views of any of the Task Force participants and other invitees to the various Task Force meetings. A robust and clear set of principles has guided the design and drafting processes to preserve the authors' independence concerning the approach, methods and output. The Task Force complies with the CEPS Integrity Statement. All participants were given the opportunity to express their views and – if well-grounded – have been acknowledged in the final text of the Report. Wherever different views and positions arose, the most crucial have been reflected in the Report.

The Task Force consisted of three closed-door meetings that took place, under the Chatham House Rule, on 7 December 2023, 18 January and 8 April 2024 at CEPS in Brussels. This was complemented with a (by invitation only) session on 4 March 2024 as part of the 2024 edition of the CEPS Ideas Lab. The agendas for each meeting are included in Annex II of this Report.

The rapporteurs gratefully acknowledge the contributions provided by all participants and invitees during the Task Force. They would like to express their most sincere gratitude to Júlia Alexandra Pőcze (Research Assistant) and Miriam Mir (Project Officer) at CEPS; Clementina Salvi (University of Liverpool) and Thilo Gottschalk and Dr Oliver Vettermann (FIZ Karlsruhe) for their support and substantive input when implementing this Task Force, organising the various meetings, and their assistance in undertaking the necessary background research.

Franziska Boehm is a law Professor at FIZ Karlsruhe and Karlsruhe Institute of Technology, KIT; Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Unit at CEPS; Valsamis Mitsilegas is Professor of European and Global Law and Dean of the School of Law and Social Justice at the University of Liverpool.

Suggested citation: Boehm, F., Carrera, S. and Mitsilegas, V. (2024), *Reconstitutionalising Privacy: EU Data Transfers and their impact on the Rule of Law, Rights and Trust*, Task Force Report, Centre for European Policy Studies, Brussels.

ISBN: 978-94-6138-794-3

CEPS

Place du Congrès 1, B-1000 Brussels

Tel : 32 (0) 2 229 39 11

email : info@ceps.eu

www.ceps.eu

CONTENTS

Executive Summary i

1. Introduction 1

2. Background 3

2.1. *Schrems* I and Safe Harbor 3

2.2. Schrems *II* and the EU-US Privacy Shield 5

3. The Commission's Adequacy Decision and Executive Order 14086 9

3.1. EO 14086: Scope and safeguards 12

3.1.1. Signals intelligence and large-scale surveillance 12

3.1.2. Onward transfers 19

3.1.3. Redress mechanism 20

4. EU law and the Court of Justice's benchmarks 24

4.1. The Court of Justice's adequacy and essential equivalence standards 24

4.2. National security 26

4.3. Data retention and international data transfers 28

4.4. Effective remedies and judicial protection 33

5. Fitness check 37

5.1. Privacy, national security and law enforcement in light of the rule of law 37

5.2. Effective remedies and justice 40

6. Policy recommendations 42

Annex I - Interviews 46

Annex II – Task Force Meetings agendas 47

Annex III – Task Force participants 55

Principles and guidelines for the Task Force 57

Executive Summary

Does current US policy offer a level of privacy and rule of law protections that are essentially equivalent to those required in EU law so that transatlantic data transfers are lawful? And can the new EU-US Data Privacy Framework (DPF) be expected to comprehensively satisfy a legal test by the Court of Justice of the European Union in Luxembourg? This Report is the final output of a Task Force entitled '*EU-US Data Transfers and their impact on the rule of law, rights and trust*' which consisted of a series of closed-door meetings with experts and stakeholders representing authorities, companies, civil society organisations and academics from both Europe and the US.

The Report implements a legal evaluation or 'fitness check' of the DPF and the European Commission's 2023 Adequacy Decision, comparing them to the preceding 'Safe Harbor' (2000) and 'Privacy Shield' (2016) arrangements. Both were invalided by the Court of Justice as they ran contrary to EU Treaties principles and rights. In examining the new DPF, the assessment pays particular attention to its impacts on legal certainty, privacy, the rule of law, and trust between policymakers, regulators, companies and data citizens.

The Report's overall conclusion is that the current DPF framework still generates profound legal uncertainty. Despite noticeable and welcomed improvements under Executive Order (EO) 14086, US policy still does not fully satisfy the essential equivalence test and the Court of Justice's benchmarks.

Key findings

The European Commission's Adequacy Decision and EO 14086

- The Commission's Adequacy Decision presents a highly complex technical assessment, which includes some crucial gaps and often fails to consider the effectiveness of key safeguards and guarantees, as well as important challenges that could reasonably emerge during their practical implementation (please refer to *Section III* of the Report).
- Executive Order (EO) 14086 has been recognised as a visible and genuine effort by the Biden administration, particularly regarding the newly envisaged safeguards on US intelligence surveillance activities and the use of EU-imported legal concepts. While an EO is an enforceable law, its practical use, impacts, durability and longevity remain unclear.
- As for other legal instruments in the realm of US surveillance, FISA Section 702 and EO 12333 remain in place. Regarding the large-scale collection of bulk data under EO 12333, obtaining prior authorisation by an independent authority is still not an obligatory requirement, and no independent *ex-post* review is carried out by a court. The Report concludes that a key unresolved question is whether the

EO safeguards will actually lead to real changes in the daily administrative practices of all relevant US intelligence communities. As such, this will require further independent monitoring and evaluation at regular intervals.

- Some of the key terms used by the EO, such as 'bulk collection' or 'signal intelligence', remain largely unclear or not properly defined (*Section III.1.1.* of the Report). In the case of 'bulk collection', the EO opted to re-use the definition from PPD-28, which was criticised by the Court of Justice. Likewise, the EO's framing of 'legitimate objectives' for bulk collection purposes is formulated in potentially too far-reaching terms, thereby remaining able to encompass disproportionately large-scale volumes of data.
- Concerning the Court of Justice's proportionality requirements, profound differences remain in the understanding, interpretation and practical use of this term in both the EU and the US legal systems. Crucially, under EU law, *the very essence* of a fundamental right affected by any given policy, a balancing exercise or balance metaphor is prohibited. At the same time, as required by EO 14086, no foreign legal sources will be considered when assessing any complaints received, and the notion of proportionality will be examined exclusively considering US policies.
- When it comes to the justice dimension of data transfers, the EO establishes a two-level redress mechanism (*Section III.1.3* of the Report): first, the Civil Liberties Protection Officer (CLPO) based at the Office of the Director of National Security (ODNI) and second, a so-called Data Protection Review Court (DPRC). The Report concludes that the envisaged procedure is 'one-sided' and secret in nature, not allowing complainants to have meaningful insights into the procedures and whether the relevant data have been deleted or rectified. Moreover, the DPRC's final decisions cannot be appealed before US Courts.

EU law and the Court of Justice's benchmarks

- According to the adequacy and essential equivalence standards developed by the Court of Justice (*Section IV* of the Report), the Commission's Adequacy Decision must pass a three-step test. If an international data transfer interferes with the EU's fundamental rights, it must respect the 'essence or very substance' of the rights at stake; otherwise, it must be annulled. If the essence of the rights is not at stake, the transfer must pass a proportionality assessment. Finally, the extent to which the data transfers are justified by an objective of general interest recognised by the EU must also be assessed.
- The EU Charter of Fundamental Rights provides a higher level of protection than the standards of the Council of Europe and the European Convention of Human Rights (ECHR). This is the case for 'effective remedies' under Article 47 of the Charter, which focuses on access to justice by individuals as a core component of

EU rule of law – and effective legal/judicial protection – under Articles 2 and 19 TEU. Likewise, EU law offers higher protection for judicial independence and impartiality, as well as for delivering effective judicial protection and remedies.

- Article 4.2 TEU does not exempt the Court of Justice from presiding over cases concerning the legality of international data transfers in the name of 'national security' and from applying EU law. Through its case law, it has converted the concept of national security into an autonomous notion with a specific 'EU meaning' and scope, which (here too) provides a higher level of protection than the standards developed by the Council of Europe (*Section IV.2.* of the Report). The Court of Justice's case law has confirmed the applicability of EU law when evaluating the retention, access to and use of commercial data for national security purposes (*Section IV.3.*).
- Considering the benchmark of effective remedies (*Section IV.4.),* the Report concludes that the EO's envisaged two-level redress mechanism is not 'essentially equivalent' to the standards set down by the Court of Justice. While nominally called a 'court', the DPRC cannot be considered a true court, meaning an independent judicial tribunal in the constitutional sense of the word – namely separate from the executive and with the power of delivering effective remedies within the meaning of EU primary law.

Policy recommendations

Based on the above findings, the Report calls for a merited or deserved trust paradigm to be fully secured in EU international data transfers policy. It puts forward a set of policy recommendations for EU and US policymakers and relevant stakeholders:

- The Commission must retain its role as the guarantor of EU Treaties – this includes enforcement and the uniform of application of EU legal benchmarks, and Court of Justice benchmarks when conducting its own assessment on the adequacy of any third country arrangement.
- The Commission must ensure the full consistency of all foreign affairs policies with EU values as required by the Treaties.
- The Commission should strictly comply with the prescribed material scope when assessing Adequacy Decisions under the GDPR, which does not include geopolitical or foreign affairs, as well as wider international trade, considerations or interests.
- The forthcoming EU policy and evolving EU-US transatlantic relations on data transfers must be rooted and driven by an unequivocal compliance with EU Treaty principles as these are preconditions or act as a *sine qua non* for legal certainty and trust.

The United States recognises that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and … all persons have legitimate privacy interests in the handling of their personal information[1].

1. INTRODUCTION

This Task Force Report carries out a 'fitness check' or legal evaluation by examining the scope and key features of the 2023 EU-US Data Privacy Framework (DPF) and the European Commission's Adequacy Decision. The analysis compares the new DPF with two previous arrangements that enabled EU-US data transfers, the so-called Safe Harbor and the Privacy Shield arrangements. They were both invalidated by the Court of Justice of the European Union in Luxembourg (the 'CJEU', 'Court of Justice' or 'Luxembourg Court') through its *Schrems I* and *Schrems II* judgments. The Report examines whether the DPF would satisfy the legal benchmarks set by the Court of Justice for such transfers to be lawful and in compliance with EU Treaty values. It outlines the expected impact of the new framework on legal certainty, the rule of law, and trust between EU and national policymakers, regulators, companies and data citizens.

Can the newly authorised DPF foster a Court-proof and merited trust model and a principled level-playing field in transatlantic data transfers? And what are the outstanding issues and dilemmas characterising the newly adopted framework? The analysis and findings are based on three methods. The first is an assessment of the various discussions that were had, as well as presentations and contributions that were made during four Task Force meetings that took place between December 2023 and March 2024. The second is a set of semi-structured interviews with leading EU and US experts (see *Annex I* of this Report for a full list). Finally, the third is a legal analysis of the relevant EU law, the Court of Justice's case law, and key findings from desk research on the relevant primary and secondary sources. The Report then presents a set of policy recommendations for future EU-US data transfers.

In various Task Force meetings and interviews, the key role of geopolitics as a driver behind the negotiations and adoption of the new EU-US arrangement at the highest political levels at the European Commission was mentioned[2]. The arrangement began to

[1] This Report takes into account development up until 19 April 2024. US Executive Order (EO) 14086, 7 October 2022, Federal Register Vol. 87, No. 198, 62283.

[2] Some Task Force corporate participants expressed the opinion that the adequacy decision was not directly correlated with the political deal but rather hinges on a thorough evaluation of the legal safeguards and remedies provided by the new DPF framework. On the politics of international data transfers refer to C. Kuner (2017), Reality and Illusion in EU Data Transfer Regulation Post Schrems, *German Law Journal*, Vol. 18, No. 4, pp. 881-918.

take shape with the Joint Statement of 25 March 2022 between the Commission and the US, which announced an agreement 'in principle', with the Biden administration committing to implementing new safeguards and to address the concerns raised by the Luxembourg Court in the *Schrems II* judgment. The deal was reached as part of a larger effort to demonstrate renewed transatlantic unity in the wake of Russia's invasion of Ukraine[3]. US authorities have not yet adopted Executive Order (EO) 14086 which was intended to implement the EU's requests.

The Task Force meetings and most of the interviewees consistently underlined the genuine efforts made by the Biden administration behind the new policy and legal developments introduced by EO 14086, and the newly envisaged safeguards on US intelligence surveillance activities. They also emphasised the unprecedented use of EU-imported legal concepts such as 'proportionality', as well as the new redress mechanisms – including a new Data Protection Review Court (DPRC) – in US intelligence communities' activities and oversight. There was consensus that EO 14086 was probably 'the best solution' the US government could have offered at the time. But the Task Force discussions also left the question open as to whether the DPF would satisfactorily pass the Luxembourg Court's legality test, which this Report seeks to assess.

Section II of the Report will provide a background to the transatlantic data transfers controversy, including the main grounds upon which the Luxembourg Court invalidated the Commission's two previous decisions on adequacy. *Section III* moves to examine the most recent European Commission Adequacy Decision in 2023, and in particular its assessment of EO 14086's scope, and its safeguards in relation to signals intelligence and large-scale surveillance, onward transfers, and the newly established redress mechanism. *Section IV* provides an overview of the Court of Justice's landmark rulings and benchmarks which are crucial to assessing the adequacy of US policy in light of privacy/data protection and effective remedies/fair trials standards under the EU's Charter of Fundamental Rights (EU Charter). *Section V* carries out a 'fitness check' or legal evaluation of the latest US policy and legal developments relating to matters covering privacy and data protection, national security and law enforcement, as well as effective remedies and justice. *Section VI* concludes with a set of policy recommendations that aim to inform EU policy and EU-US transatlantic relations on data transfers.

[3] According to Politico, there was ongoing reluctance by some Brussels-based officials to sign off on a new transatlantic data arrangement, refer to Politico (2023), *Political pressure wins out as US secures preliminary EU data deal*, 25 March 2022, available at: https://www.politico.eu/article/privacy-shield-data-deal-joe-biden-ursula-von-der-leyen/

2. BACKGROUND

2.1. *SCHREMS* I AND SAFE HARBOR

The concept that a third country needs to have an 'adequate level of protection' to be able to lawfully transfer data to that country already existed under Directive 95/46[4], the General Data Protection Regulation's (GDPR) predecessor[5]. The Commission negotiated the first Adequacy Decision with the US based on the so-called Safe Harbor Principles[6] in 2000, and the US Department of Commerce established a sort of self-certification mechanism for US companies.

In 2013, Edward Snowden revealed the large-scale surveillance activities of the United States intelligence services, particularly those of the National Security Agency (NSA). Following this Max Schrems filed a complaint that his data had been illegally transferred from Facebook Ireland to the US. Against the background of the surveillance activities, he suspected that the US had not ensured 'an adequate level of protection' as required under the Safe Harbor Principles and that EU data protection authorities needed to intervene to stop such transfers.

Further to his complaint, in 2015 the Court of Justice provided its interpretation of Articles 25[7] and 28[8] of Directive 95/46 in light of the fundamental rights guaranteed by Articles 7, 8, and 47 of the Charter in detail. It concluded that not only are data protection authorities required to stop such data transfers, but also that the Commission´s Adequacy Decision was invalid as the US had not provided for an 'adequate level of protection[9]'.

In its *Schrems I* judgment, the Court of Justice further specified what an adequate level of protection meant under EU law. It recalled that adequacy is intended to ensure the protection of personal data rights as established under Article 8(1) of the EU Charter when data are transferred to a third country. It held that the term 'adequate' does not mean an *identical* level of protection but requires a level that is 'essentially equivalent' to that guaranteed within the European Union, that is, by virtue of Directive 95/46 read in the light of the Charter[10]. It elaborated that although the ways the third country chooses to

[4] Art. 25 of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

[5] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, of 27 April 2016, L 119/1, 4.5.2016 (GDPR).

[6] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

[7] Refer to principles under Article 25 Directive 95/46.

[8] Article 28 Directive 95/46 deals with the tasks and duties od supervisory authorities.

[9] Case C-362/14 *Schrems v. Data Protection Commissioner*, EU:C:2015:650. Schrems I, paras. 79-106.

[10] *Schrems I*, paras. 72 and 73.

ensure such a level of protection may differ from those used within the European Union', its 'means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union[11]'.

This 'essentially equivalent-test' established a solid standard for a third country to meet. And it also posed a clear legal benchmark for the Commission when assessing the level of protection under EU law. In fact, the Luxembourg Court insisted on reducing the amount of discretion the Commission had to determine the adequacy of the level of protection ensured by a third country in light of the right to data protection as a fundamental right when there is a 'large number of persons whose fundamental rights are liable to be infringed'. The result is that review of adequacy requirements should be strict[12].

The Court's main point of criticism in its decision to invalidate the Commission´s first adequacy decision concerned the generalised access that US national security agencies had to the data transferred to the US and the lack of safeguards in place[13]. US domestic law even expressly provided for far-reaching access to the transferred data for national security, public interest or law enforcement purposes. In addition, the adequacy decision itself allowed for restrictions to its principles 'to meet national security, public interest, or law enforcement requirements' giving priority to those over the Safe Harbor Principles[14].

In its reasoning the Court referred to its jurisprudence on data retention, in particular to the 2014 *Digital Rights Ireland* case[15], to establish the existence of an interference and to highlight the need for safeguards. Importantly, the Court also provided clarification regarding the relationship between the right to respect privacy under Article 7 of the Charter and the right to data protection under Article 8 of the Charter. It noted that the right to respect for privacy is fundamental, and 'it is this right which makes it necessary to have rules on data protection to safeguard privacy and, thus, to limit all interferences except in so far as it is strictly necessary[16]'.

The most prominent points of criticism referred to the lack of effective redress mechanisms for governmental data access[17], lack of proportionality and necessity requirements, as well as the lack of access, rectification or erasure possibilities for data citizens concerned or any restrictions or criteria to limit the access of public authorities

[11] Ibid., para. 74.

[12] Ibid. para. 78 in which the CJEU makes reference to the judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48.

[13] Ibid., paras. 79-98.

[14] Ibid., paras. 84-86.

[15] *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238.

[16] S. Carrera and E. Guild (2015), The End of Safe Harbor: What Future for EU-US Data Transfers, *Maastricht Journal of European and Comparative Law*, Vol. 22, Issue 5, pp. 651-655.

[17] *Schrems I,* para. 89.

to the data[18]. Further, access to the data 'on a generalised basis' – whether it was content or metadata – was regarded as violating the essence of Article 7 of the EU Charter. The Court stated that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data' infringes *the essence* of the right to effective judicial protection/effective remedy as enshrined in Article 47 of the Charter (emphasis added[19]). The possibility to challenge non-compliance with EU law and obtain an effective judicial review was considered to be *inherent to the rule of law*[20].

2.2. SCHREMS //AND THE EU-US PRIVACY SHIELD

After its first adequacy decision was invalidated, the Commission negotiated a new arrangement called the 'EU-US Privacy Shield'. This instrument came into effect in July 2016 and was accompanied by a second adequacy decision[21]. The new arrangement was intended to address the criticism of the former Safe Harbor Adequacy Decision, but also failed to pass the 'essentially equivalent-test' of the Court of Justice as set out in the *Schrems II* judgment of July 2020. Here, the reasons for invalidation were similar to those in the *Schrems I* case[22]. Reference was made to the extensive exceptions which were made for national security, public interest, and law enforcement reasons[23] in the framework of US surveillance programmes allowing for the bulk collection of data[24]. In the view of the Court, those reasons, and the lack of effective judicial review possibilities meant there was violation of Articles 7, 8 and 47 of the Charter.

In *Schrems II*, the Court felt the need to set out its arguments in detail and reminded the parties of the guarantees inherent in Articles 7 and 8 of the Charter. It reiterated that both communication of personal data to a third party and the retention of and access to personal data, are interferences with the fundamental rights enshrined in Articles 7 and 8 EU Charter. The Court of Justice recapped that such interference with rights can be justified, as per Article 52(1) EU Charter. However, any limitations on those rights must be provided for by law and respect *the essence* of those rights and, otherwise, need to be

[18] Ibid., paras. 91-94.

[19] Ibid., para. 95.

[20] Ibid., para. 95, referring to the judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, para. 23; *Johnston*, 222/84, EU:C:1986:206, paras. 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, para. 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, para. 80.

[21] 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 (notified under document C(2016) 4176).

[22] The *Schrems II* case also dealt to a great extent with questions relating to standard contractual clauses, these are not in the focus of this Report and therefore not discussed here.

[23] Ibid., paras. 168-184.

[24] Ibid., para. 183.

proportionate[25]. Article 8(2) of the Charter also requires that 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'. The latter must 'itself define the scope of the limitation on the exercise of the right concerned[26]'.

The Luxembourg Court emphasised that limitations must 'apply only in so far as is strictly necessary', and therefore that legislation restricting fundamental rights '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[27]'. Such legislation must clearly indicate the circumstances under which a measure providing for the processing of such data may be adopted. When data are subject to automated processing, it is even more important to have safeguards in place.

On more specific points of criticism, the Court of Justice found that the implementation of the US surveillance programmes codified in Section 702 of the Foreign Intelligence Surveillance Act (FISA[28]) and in EO 12333 were not proportional and did not ensure an essentially equivalent level of protection. Section 702 of the FISA did not lay down clear and precise rules governing the scope and application of the surveillance measure in question, nor did it impose minimum safeguards. Both the Presidential Policy Directive (PPD) 28, which was mentioned by the US and the Commission as including some safeguards, and EO 12333 failed to grant enforceable rights for EU data subjects before courts. Therefore, they were not equivalent[29].

The Court added that PPD-28 allowed for so-called bulk collection 'of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target… to focus the collection[30]'. This meant it was not compliant with the EU principle of proportionality. In clarifying the meaning of bulk collection, the Court of Justice referred to the definition in PPD-28. There it means 'the authorised collection of *large quantities*

[25] *Schrems II*, paras. 171, 173-174.

[26] Ibid., para. 175 by referring to Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case law cited.

[27] Ibid., para. 176.

[28] Ibid., para. 176: 'In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programmes (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)'. As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'.

[29] *Schrems II*, paras. 180-182.

[30] Ibid., para. 183.

of signals intelligence data which, due to technical or operational considerations, is acquired *without the use of discriminants* (e.g. specific identifiers, selection terms, etc.)' (emphasis added[31]).

As well as remarking on the violations of Articles 7 and 8 of the Charter, the Court of Justice dedicated several paragraphs to analysing Article 47 of the Charter. That provision grants *everyone* in the EU- irrespective of nationality- the right to an effective remedy before a tribunal if their rights and freedoms under the Charter are violated. They also have the right to a fair and public hearing by an independent and impartial tribunal previously established by law. The Court stressed that 'the very existence of *effective judicial review* designed to ensure compliance with provisions of EU law is inherent in *the existence of the rule of law*'. It continued by repeating the *Schrems I* statement that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect *the essence* of the fundamental right to *effective judicial protection'* (emphasis added[32]).

The Court of Justice also referred to Article 45(2)(a) of the GDPR. That provision obliges the Commission to pay particular attention to 'the effective administrative and judicial redress for the data subjects whose personal data are being transferred' when assessing the adequacy of a third country. It added that Recital 104 of the GDPR requires that the 'third country should ensure effective *independent data protection supervision* and should provide for cooperation mechanisms with the Member States' data protection authorities' (emphasis added). It also adds that the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress'. Considering the difficulties individuals might be faced with when trying to obtain effective redress in a third country, the Court considered such guarantees of particular importance in the context of the transfer of data[33].

As neither Section 702 of the FISA, EO 12333, nor PPD-28 provided for any redress, the Privacy Shield arrangement added an Ombudsperson-mechanism intended to address the lack of a remedy system. However, the Ombudsperson did not fulfil the criteria to qualify as an independent and impartial court. Its position was 'an integral part of the US State Department' and the appointment of the Ombudsperson was not accompanied by sufficient guarantees to ensure its independence from the Executive[34]'. Moreover, there was no indication that power was allocated to the Ombudsperson to adopt binding

[31] PPD-28, Fn. 5. This definition is also referred to in *Annex VI* to the Privacy Shield Decision.

[32] *Schrems II*, para. 187.

[33] Ibid., paras. 188 and 189.

[34] Ibid., para. 195 by referring to judgment of 21 January 2020, Banco de Santander, C-274/14, EU:C:2020:17, paras. 60 and 63 and the case law cited.

decisions on intelligence services or any 'legal safeguards that would accompany that political commitment on which data subjects could rely[35]'. Ultimately, the Court declared the Privacy Shield Decision to be incompatible with Article 45(1) of the GDPR read in the light of Articles 7, 8 and 47 of the Charter.

[35] *Schrems II*, para. 196 states.

3. THE COMMISSION'S ADEQUACY DECISION AND EXECUTIVE ORDER 14086

In July 2023, 3 years after the invalidation of the Privacy Shield Decision and more negotiations with the US authorities, the Commission published the current Adequacy Decision based on the EU-US Data Privacy Framework (DPF)[36]. The DPF consists of an assessment of the Commission on adequacy which builds on the Principles and Supplemental Principles (collectively 'the Principles') issued by the US Department of Commerce (Annex I) and eight annexes. The annexes explain the US instruments intended to establish safeguards for data subjects and consist of documents of 'different legal value[37]'. They range from the DPF principles issued by the Department of Commerce, to letters providing an overview of applicable guidelines, practices, and US law.

The assessment and text of the Commission Adequacy Decision[38] is highly complex in terms of its technical nature and structure, which makes it difficult to understand and comprehend the text. The European Data Protection Board (EDPB) refers to 'an overall complex presentation' and a structure that 'makes information rather difficult to find and refer to' which 'may not favour a good understanding of the DFP Principles by data subjects, DFP Organisations and EU Data Protection Authorities[39]'.

The assessment frequently fails to consider all the key issues which can be expected to emerge during the implementation of the listed guarantees and safeguards, and their effectiveness in practice[40]. It also presents some crucial gaps. For instance, the DPF Principles are silent when it comes to 'decisions affecting individuals based solely on the automated processing of personal data[41]'. To justify not regulating this aspect, the Commission argues that such decision will 'typically be taken by the controller in the Union' which would then be subject to the GDPR[42]. References are also made to sector-

[36] European Commission Implementing Decision on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final, Brussels, 10.7.2023.

[37] European Data Protection Board (EDPB), Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28 February 2023, p. 3.

[38] European Commission Implementing Decision on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final, Brussels, 10.7.2023.

[39] EDPB Opinion 5/2023, p. 15.

[40] Some Task Force participants underlined that this may be resolved by the annual Privacy and Civil Liberties Oversight Board (PCLOB) review of the functioning of the new DPF redress system, or by upcoming DPF joint reviews.

[41] Commission implementing decision, recitals (33)-(35). The 2023 Commission Adequacy Decision concluded, based on an older 2018 Study, that, at that time, 'there was no evidence suggesting that automated decision-making was normally being carried out by Privacy Shield organisations on the basis of personal data transferred under the Privacy Shield'. Refer to paras 33 and 34, and footnote 52.

[42] Commission implementing decision, recital (33).

specific US law[43]. This is surprising given recent developments surrounding Artificial Intelligence (AI) and has been criticised by the EDPB[44].

Regarding data transfers for national security purposes, the US still maintains Section 702 of FISA and EO 12333. As they do not provide for safeguards and are not limited in scope or to certain offences or the extent to which data can be collected, retained or further disseminated[45], these instruments together with PPD-28[46] were some of the key reasons why the Court of Justice invalidated the Privacy Shield. This is problematic as they do not provide for sufficient legal safeguards, are not clearly limited in scope, or to certain offences, and do not offer legal certainty/guarantees on the extent to which data can be collected, retained or further disseminated by all relevant US intelligence communities. The EO 14086 should limit the use of these provisions, but it is not always successful in doing so.

Presentations given during the Task Force meetings and some interviewees highlighted the shortcomings in the practical implementation of these US surveillance policies. Affected individuals or legal persons face procedural hurdles to obtaining effective judicial redress for unlawful activities before the US Courts. This is mainly due to the 'standing[47] and state secrets[48]' doctrines where US tribunals can dismiss a case challenging the lawfulness of intelligence surveillance without deciding on the merits[49].

Section 702 of FISA is also heavily criticised in the US, as there are apparently serious compliance issues and privacy concerns within the US and abroad. The Privacy and Civil Liberties Oversight Board (PCLOB)[50] and the report of the House Intelligence (Permanent Select) Committee of Congress have recently published reports on the FISA Reform and

[43] Commission implementing decision, recitals (33)-(35).

[44] EDPB Opinion 5/2023, pp. 19-20.

[45] Ibid., p. 29, para. 114.

[46] Presidential Policy Directive- Signals Intelligence Activities, 17 January 2014, now mainly replaced by EO 14086.

[47] US law requires individuals to prove a 'concrete, particularised, and actual or imminent injury', Refer to *Clapper v. Amnesty International* USA, 568 U.S. 398 (2013) II. p. 10.

[48] Refer to Supreme Court in the 1953 case of *Reynolds v United* States, the 'state secrets privilege' (SSP) allows the government to withhold evidence and refuse to share information. The executive may refer to this privilege in court, leading to the dismissal of cases that challenge action taken by the administration in US courts. https://ccrjustice.org/files/factsheet_stateSecrets.pdf

[49] An example mentioned during our interviews relates to a case brought by the Wikimedia Foundation to challenge the NSA's 'Upstream surveillance'. Wikimedia, which operates the website Wikipedia, a webpage that generates 'trillions of communications' on an annual basis, claimed that some of its communications were subject to NSA seizure and surveillance. The case was dismissed on state secret grounds and not heard by the Supreme Court following lengthy litigation in the lower courts.

[50] US Privacy and Civil Liberties Oversight Board PCLOB), Report on the surveillance programme operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act, available at: https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf (accessed 13.02.2024)

Reauthorization Act of 2023[51]. These reports also highlight shortcomings in the current implementation of FISA Section 702 and recommend additional measures, such as a 'probable cause' standard similar to the context of law enforcement – albeit in this case with regard to US citizens.

During the lifespan of the Task Force a reform of Section 702 of FISA was ongoing in the US and Congress had to decide by 19 April 2024 whether to reauthorise it or not[52]. The Parliament had therefore asked the Commission whether the proposed reform and reauthorisation of Section 702 of FISA would cast doubts over the Commission's signature of the DPF. Our interviewees unanimously emphasised that it was unlikely that the US Congress would let it expire, and that experience shows that it had not allowed it to expire on multiple previous occasions. On 12 April 2024, the US House finally voted to approve a two-year extension[53].

Although issued by the US President and not Congress, EO 14086 is still considered law in the US legal system. It is legally binding, and therefore it can be enforced. During the various Task Force meetings and the interviews it was highlighted that an EO has inherent structural limits or shortcomings that can make it difficult to ensure its durability in the medium and long term. This is because the US President has complete discretion to modify any of its provisions, issue another EO that changes it substantially or fundamentally, and can even annul it altogether.

Some interviews have underlined that the US President could modify or issue a 'secret' EO in a classified manner without the public knowing about it or lay down certain exceptions where select provisions of the 'public' act shall not apply. Furthermore, some interventions during the Task Force meetings and several interviewees underlined that if a new US President is elected in the upcoming presidential elections, EO 14086 could potentially be overturned[54]. Other Task Force participants underlined that this would lead

[51] Report of the House Intelligence (Permanent Select) Committee of the Congress on the FISA Reform and Reauthorization Act of 2023, available at: https://www.congress.gov/congressional-report/118th-congress/house-report/302 (accessed 13.02.2024).

[52] https://www.brennancenter.org/our-work/research-reports/whats-next-reforming-section-702-foreign-intelligence-surveillance-act; see also question to the Commission Mathilde Androuët: https://www.europarl.europa.eu/doceo/document/E-9-2024-000166_EN.html

[53] This was instead of the five-year original extension, influenced by Donald Trump opposing the reauthorisation of the bill, and as reported by *The Guardian* 'An amendment that would have required authorities seek a warrant failed, in a tied 212-212 vote across party line'. Refer to https://www.theguardian.com/us-news/2024/apr/12/fisa-surveillance-act-reauthorized In any case, the FISA 702 'grandfather clause' would have still authorised the US intelligence communities to conduct surveillance for another 12 months.

[54] The Heritage Foundation (2023), *Mandate for Leadership: The Conservative Promise*, Project 2025 – Presidential Transition Project, Washington, which in page 226 states that: 'An incoming President should ask for an immediate study of the implementation of Executive Order 14086 and suspend any provisions that unduly burden intelligence collection.'

to a repeal or suspension of the Adequacy Decision by the Commission according to Article 45(5) of the GDPR[55].

The EO provisions are legally binding upon the entire US intelligence community and have been implemented through relevant agency policies and procedures transposing these principles into practice[56]. Despite this, a key question is whether these principles will actually lead to real changes in the daily administrative practices of all relevant US intelligence communities. It is also important to consider how the envisaged safeguards will be interpreted by each of the US intelligence community actors, including what will be considered as 'proportionate' in relation to a validated intelligence priority or objective[57]. This will require further independent monitoring and evaluation at regular intervals.

3.1. EO 14086: SCOPE AND SAFEGUARDS

3.1.1. Signals intelligence and large-scale surveillance

The new EO 14086 aims to set limitations and safeguards in the framework of signals intelligence, including in the context of FISA and EO 12333. It is intended to satisfy the requirements established by the Court of Justice in *Schrems I* and *Schrems II*. It replaces the heavily criticised PPD-28 except for its Section 3 and a (secret) complementing annex which includes provisions on an annual review of the signals intelligence activities by intelligence agencies. Some of the key concepts and notions used by EO 14086 remain by and large undefined or formulated/used in rather unclear terms, which leads to profound

[55] Section 220 of the Commission's Adequacy Decision states that, 'for example if EO 14086 or the AG Regulation would be amended *in a way that undermines the level of protection* described in this Decision or if the Attorney General's designation of the Union as a qualifying organisation for the purpose of the redress' (emphasis added). Moreover, some Task Force participants expressed the opinion that while Executive Orders like EO 14086 can be modified or revoked by future administrations, there are significant factors that suggest their continuity. These factors include bipartisan support for facilitating EU-US data flows, including regarding previous frameworks.

[56] ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086, 3 July 2023. Refer to https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086

[57] The various intelligence communities procedures present some differences regarding the use of 'proportionality'. For instance, the Central Intelligence Agency (CIA) Procedures state in Point 2 that ,'Signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorised, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.' This compares to those envisaged by the NSA Procedures, Sections 10 and 11, which state that 'NSA/CSS will conduct targeted collection using selection terms whenever practicable. NSA shall only engage in bulk collection upon a determination that it is necessary to engage in bulk collection in order to advance a validated intelligence priority…and NSA employees are required to consider…methods to limit the types and aspects of the information collected to those necessary and proportionate to one or more of the legitimate objectives listed in Section 2 of EO 14086…[and] bulk collection shall, nevertheless, be as circumscribed as possible, proportionate to the intelligence objective'.

legal uncertainty. This includes nebulous terms such as 'signals intelligence', 'bulk collection' and 'temporary bulk collection[58]'.

The term 'signals intelligence' is often referred to in both EOs and involves, according to the National Security Agency (NSA), 'collecting foreign intelligence from communications and information systems and providing it to customers across the US government, such as senior civilian and military officials[59]'. These wide-ranging surveillance activities and techniques are referred to by the Court of Justice as bulk collection[60] in the *Schrems* cases and should be limited by EO 14086. The latter recognises 'legitimate privacy interest' and that 'all persons should be treated with dignity and respect[61]'.

The definition of 'bulk collection' in EO 14086 stems from the former PPD-28 which was criticised by the Court of Justice in *Schrems II*. Bulk collection is defined as 'the authorised collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants[62]'. This corresponds almost exactly to the definition of bulk collection used in the former PPD-28[63]. EO 14086 establishes that 'targeted retention shall be prioritised' and bulk collection carried out if 'the information necessary to advance a validated intelligence priority cannot reasonably obtained by targeted collection[64]'. The EO 14086 expressly acknowledges that 'bulk' (used as not 'targeted' by the EO) collection can take place when 'it is determined to be *necessary* [and in a manner that is *proportionate*] to advance a validated intelligence priority'.

Some interviews with US experts and authorities have revealed that such an analysis is limited to assessing the overall importance of the given 'intelligence priority' – and these priorities, contrary to the need for individual/targeted, concrete assessments, are defined

---

[58] According to the EO 14086, '"Bulk collection'' means "the authorised collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, *without the use of specific identifiers or selection terms*)"' (emphasis added).

[59] Compare definition on the Website of the NSA: https://www.nsa.gov/Signals-Intelligence/Overview/ (accessed 12.02.2024). The NSA collects signal intelligence: 'from various sources, including foreign communications, radar and other electronic systems. This information is frequently in foreign languages and dialects, is protected by codes and other security measures, and involves complex technical characteristics. NSA needs to collect and understand the information, interpret it, and get it to our customers in time for them to take action. Our workforce is deeply skilled in a wide range of highly technical fields that allow them to this work, and they develop and employ state-of-the-art tools and systems that are essential to success in today's fast-changing communications and information environment'.

[60] *Schrems II*, para. 183.

[61] Enhancing Safeguards for United States Signals Intelligence Activities – Executive Order 14086 [2022], section 1, available at: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf.

[62] EO 14086, Section 4 (b).

[63] PPD-28, Fn. 5, this definition is also referred to in Annex VI to the former Privacy Shield Decision and reads: 'References to signals intelligence collected in "bulk" mean the authorised collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)'.

[64] EO 14086, Section 2 (c) (ii) (A).

very generally, resulting in very little actual case-by-case analysis when it comes to greenlighting large-scale surveillance. The interviews also revealed that the question of whether the US intelligence communities engage in 'bulk collection[65]' or not depends on how one interprets what 'bulk collection' actually means and entails in practical terms. As one officer at a US national intelligence authority put it during an interview, 'intelligence is an art, not a science'.

Several interviewees particularly underlined that the definition relies on the exact legal interpretation used or preferred by the administration in power, and it is ultimately the intelligence community that defines its own terms so that they may very well end up redefining what 'bulk collection' means in practice[66]. According to one interviewee, 'the scanning component of upstream surveillance' has a 'bulk surveillance aspect', since the government is 'accessing and scanning through communications in bulk', even if it is only concerned with the communications to and from its targets. With respect to the collection under Section 702 of FISA – where Downstream and Upstream surveillance are used – the same interviewee said that while the collectors 'technically use discriminants', the surveillance conducted under that mandate is very large-scale because the targeting threshold is very low and the number of targets is consequently high.

In that respect, the US government can 'target any non-US person abroad to acquire foreign intelligence information'. However, crucially, the terms of 'foreign intelligence information' are very broadly defined. Therefore, as long as this targeting threshold remains low and the definitions are broad, any non-US person may be targeted for the acquisition of foreign intelligence information, which qualifies as large-scale surveillance despite Section 702 of FISA's targeting. Importantly, in the case of non-US persons, there is no specific independent, individual judicial review of the surveillance and collection request under Section 702 of FISA – whereas there is for US persons.

According to EO 14086, 'signals intelligence' should only be conducted based on 'a reasonable assessment of all relevant factors that the activities are necessary to advance

[65] The official position of the Office of the Director of National Intelligence (ODNI): in a Brief on Section 702, the ODNI explicitly states that 702 was '"not a bulk collection programme" but a "substantial and important targeted intelligence collection program"'. Refer to DNI Resource Library, see: https://www.dni.gov/files/FISA_Section_702/FISA_Section_702_FISA.pdf

[66] Moreover, as regards the collection under Section 702 FISA, the surveillance conducted under that mandate is large-scale because the targeting threshold is extremely low and the number of targets is consequently high. In that respect, interviews underlined that the US government can target any non-US person abroad to acquire foreign intelligence information, however, and crucially, the terms of 'foreign intelligence information' are very broadly defined. In addition, the EDPB Opinion 2023/5 expresses concerns in relation to the notion of 'temporary bulk collection' under EO 14086, which in its view 'still appears to mean that as long as the target has not been identified, bulk collection could continue'. In this regard, the EDPB recalls the necessity to have clear and precise rules and stresses here as well "the key safeguard that these rules constitute for data subjects… In conclusion, concerning the safeguards applicable to bulk collection, the EDPB remains concerned that, despite additional safeguards provided under EO 14086, the possibility to collect data in bulk, i.e. without discriminants, is still provided"' paras. 162 and 163.

a validated intelligence priority, although signal intelligence does not have to be the sole means available…[67]'. Further, signals intelligence 'shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority …[68]'. These principles should apply to all stages of the use of signals intelligence. Further, the 'availability, feasibility and appropriateness of other less intrusive sources and methods' shall be considered when determining whether to collect signals intelligence and the latter shall be 'as tailored as feasible to advance a validated intelligence priority[69]'.

Section 2 of EO 14086 lists 'legitimate objectives' that should be pursued when carrying out signals intelligence activities, five objectives for which signals intelligence is prohibited[70] and six objectives for which bulk collection is considered legitimised. The six objectives considered legitimate for bulk collection relate to specific goals such as foreign military capabilities, taking of hostages, or protection against the development, possession or proliferation of weapons of mass destruction. It also includes rather open-ended objectives and blurred notions such as to a potential threat to national security, understanding or assessing threats that impact global security, including climate or other ecological change, political instability or the protection against threats to US personal or its allies or the protection against transnational criminal threats, including illicit finance and sanctions evasion or the protection of the integrity or elections and political processes[71].

The list foresees both specific and general objectives and may also be extended by the US President – secretly – if publication constitutes 'a risk to national security[72]'. The EDPB considers the scale of bulk collection possibilities as 'potentially broad, i.e. encompassing large volumes of data[73]'. Next to the six objectives, there is a further possibility to collect data in bulk 'temporarily' without discriminants (specific identifiers or selection terms) when data are used 'only to support the initial technical phase' of the signals intelligence collection activity[74]. Furthermore, the EDPB assessed these rules in detail and criticised

[67] EO 14086, Section 2 (a) (ii) (A).

[68] EO 14086, Section 2 (a) (ii) (B).

[69] EO 14086, Section 2 (c) (i) (A) and (B).

[70] EO 14086, Section 2 (b) (ii) (A) and (B). The five objectives for which signal intelligence is prohibited include, among others, suppressing or restricting legitimate privacy interests, disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation or religion or the collection of foreign private commercial information or trade secrets (...).

[71] EO 14086, Section 2 (b) (i) (A) (1)-(12).

[72] EO 14086, Section 2 (c) (ii) (C).

[73] EDPB Opinion 5/2023, p. 33, para. 140.

[74] EO 14086, Section 2 (c) (ii) (D). As the EDPB states, the wording used to describe this exception is similar to the now replaced PPD-28 (section 2, fn. 5), which was criticised by the EDPB in the last joint review of the Privacy Shield as contradicting the *Schrems II* judgment by not delimiting 'in a sufficiently clear and precise manner the scope of such bulk collection of personal data'. Particularly concerning is the reference to 'support of the initial technical phase', which

for instance the unspecific retention period, the missing limits on dissemination or the lack of prior authorisation for bulk collection[75].

Although the six objectives for which bulk collection is considered legitimate are listed under 12 points, the objectives often summarise more than one objective under one paragraph[76]. Updates to this list by the US President are possible (also in secret) if new national security imperatives emerge[77]. Some interviewees have underlined that the framing of 'legitimate objectives' in EO 14086 remains very broad, particularly those related to general objectives. This has been considered as potentially very broad and capable of encompassing large-scale volumes of data. The 12 objectives need to be substantiated for operation in practice[78], which should follow the procedure and objectives under Section 2 (b) (iii) of the EO 14086. In most cases the opinion of the CLPO (Civil Liberties Protection Officer of the Office of the Director of National Intelligence) should be heard[79]. However, in 'narrow circumstances' a priority can be set by the President or the head of an element of the Intelligence Community[80]. This exception should be in accordance with the criteria described in Section 2 (b)(iii) 'to the extent feasible[81].'

Furthermore, EO 14086 expressly envisages that the US President may authorise updates to this list of objectives in light of 'new national security imperatives'. The list of prohibited grounds is comprehensive and welcomed. However, it lacks careful consideration of any potential negative impacts or linkages between these and the objectives deemed 'legitimate'. Additionally, it fails to consider the potential negative impacts of the latter over the former. Following PPD-28, EO 14086 envisages an additional possibility to collect data in bulk 'temporarily' without any discriminants (specific identifiers or selection terms) when the data are used 'only to support the initial technical phase' of the signals intelligence collection activity. Therefore, the extent to which the guarantees of EO 14086 limit the scope of US surveillance in a sufficiently clear and precise manner remains questionable.

---

is not sufficiently clear. See EDPB Opinion 5/2023, p. 36, para. 156 with reference to *Schrems II* and the last Joint Review of the Privacy Shield.

[75] EDPB Opinion 5/2023, pp. 33-36, paras. 142-155.

[76] Taking, for instance, EO 14086, section 2 (b) (i) (A) (3), which covers six offences that might impact global security. EO 14086, section 2 (b) (i) (A) (3) 'understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry'.

[77] EO 14086, Section 2 (b) (i) (B).

[78] EO 14086, Section 2 (b) (iii) and also EDPB Opinion 5/2023, p. 30, para. 116.

[79] EO 14086, Section 2 (b) (iii) and also EDPB Opinion 5/2023, p. 30, para. 116.

[80] EO 14086, Section 4 (n) and also EDPB Opinion 5/2023, p. 30, para. 117.

[81] EO 14086, Section 4 (n) and also EDPB Opinion 5/2023, p. 30, para. 117.

Furthermore, as underlined by the EDPB, the collection of bulk data under EO 12333 still fails to meet the requirement of prior authorisation by an independent authority. It also does not 'provide for a systematic independent review *ex post* by a court or an equivalently independent body[82]'. Additionally, presentations by some US companies during the Task Force underlined that while 'bulk collection' can take place within the scope of EO 12333, there is no legal obligation under EO 12333 for a company to participate in any 'bulk' efforts, or to disclose any data at all[83]. Some US companies underlined that 'hyperscale cloud providers have legal, contractual, and principled obligations to protect their customers' data from any government's direct access attempts[84]'.

Some interviews underlined a 'major effort' by the US government to accommodate the EU-imported concept of proportionality. Contrary to the conclusion reached by the EDPB Opinion 5/2023[85], our research shows that the use by EO 14086 of 'proportionality' is not fully aligned with that established in EU law and the Court of Justice's-case law. This is confirmed, for instance, by the EO 14086 itself when requiring the DPRC 'judges' not to use any foreign sources of law when assessing and interpreting the complaints at hand.

Furthermore, our interviews have unanimously concluded that the US authorities will only examine these notions in the context of US policies. These policies primarily consider issues such as the extent to which the 'validated intelligence priority' is necessary, relevant, lawful, and an assessment of all available means to select 'the least intrusive option' for data collection and use. Some interviewees underlined that US policy is limited to assessing the overall importance of a given or validated intelligence priority. And these priorities, contrary to the need for individual, concrete assessments, are defined rather loosely, resulting in very little actual case-by-case analysis when it comes to greenlighting surveillance. In addition, the US interpretation fails to consider the *essence* of the rights

[82] EDPB Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28 February 2023. The same Opinion underlines that 'the EDPB regrets that the FISA Court ('FISC') does not review a programme application for compliance with the EO 14086 when certifying the programme authorising the targeting of non-US persons, even though the intelligence authorities carrying out the programme are bound by it.' It remains legally uncertain the extent to which the EO14086 additional safeguards are also applicable in EO 12333 surveillance programmes.

[83] *See* USG White Paper at 17 ('[U]nder EO 12333, there can be no "requirement" for a company to disclose any data to the US government. And the government certainly may not legally require US companies to disclose data transferred under SCCs "in bulk."').

[84] Specifically, according to a written contribution by a US company of this Task Force 'EO 12333 authorises elements of the US Intelligence Community to collect foreign intelligence information and places restrictions on collection techniques. However, unlike Section 702, EO 12333 does not permit the US government to compel private parties to disclose information. EO 12333 does authorise the US government to employ technical collection, or so-called direct access, when private party assistance is not needed. This authority is primarily used to obtain 'communications by foreign persons that occur wholly outside of the United States', and the collection occurs 'largely from outside the United States.'

[85] Para. 126.

and rule of law guarantees in question, which is why a balancing approach should be prohibited (see *Section IV.1.* below for more details).

Essential equivalence does not require other governments to literally incorporate EU law into their own. Instead, as shown in *Box 1*, it calls for a level of protection that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. The EU's essentially equivalent-test applies irrespective of whether a data transfers arrangement comes in the form of an international treaty or not.

Despite the wording such as that included in the opening of this Task Force Report when quoting EO 14086 regarding the need to treat *all* persons – irrespective of nationality and residence - with dignity and respect, or the express references to the EU notions of proportionality and necessity in the EO and implementing procedures, one can expect far-reaching differences in the actual understanding and practical applicability of these terms in the EU and the US legal systems. These differences question a similar approach to examining the compatibility and impacts of surveillance measures on civil liberties, fundamental rights and the rule of law.

Box 1: The EU's essentially equivalent-test

The *essentially equivalent-test* under EU law corresponds to a fundamental rights check according to Article 52(1) of the EU Charter and consists of the following components:

- Is an interference established? Is the interference **provided for by law?**
- Is the interference justified by an **objective of general interest** recognised by EU law?
- Does the interference respect ***the essence*** **of the fundamental right at stake?**
- In the positive, is the interference a **necessary** measure to achieve the public policy objective?
- Is the interreference **proportionate to achieve a balance between the objective and the intended aim?**

Source: Authors' own elaboration.

3.1.2. Onward transfers

The onward transfer of the obtained data by law enforcement authorities is also mentioned[86]. Several procedures and safeguards in different agencies are mentioned. However, the Adequacy Decision does not describe the conditions under which data can be handed over to other authorities. Instead, reference is made to principles that apply to all agencies, such as privacy programmes, the handling of data breaches or the establishment of retention periods (recitals (101)-(106)). The Federal Bureau of Investigation (FBI) is an exception mentioned in recital (101) of the Adequacy Decision, and this is not further discussed.

Regarding the sharing of data among governmental agencies within the US, there is one example mentioned in recital (106) which relates to some basic sharing conditions and the imposing of conditions 'where relevant' that govern the processing of information through written agreements. The Adequacy Decision provides limited information on the sharing with other/foreign non-US agencies. Only one example is given in recital (106) which relates to the AGG-DOM and the FBI Domestic Investigations and Operations Guide. This allows for sharing when the information to be shared relates to the responsibilities of the foreign agency and the sharing is 'in the interest of the US; the dissemination is notably necessary to protect the safety and security of person or property or to protect against or prevent a crime of threat to national security and the disclosure is compatible with the purpose for which the information was collected[87]'.

Given the fact that sharing within and outside the US is only explained on the basis of one example, the EDPB has asked the Commission to further clarify the principles and safeguards on the further use of data within and outside of the US[88].

[86] Commission implementing decision, recitals (101) et ss.

[87] Commission implementing decision, recital (106).

[88] EDPB Opinion 5/2023, p. 26, para. 99.

3.1.3. Redress mechanism

EO 14086 envisages a two-level redress mechanism: First, an initial internal investigation of qualifying complaints by a Civil Liberties Protection Officer (CLPO) which is under the Office of the Director of National Intelligence. Second, a so-called Data Protection Review Court (DPRC) to review/appeal CLPO determinations, within the Executive branch of the US administration (US Department of Justice) composed by no less than six so-called judges appointed directly by the Attorney General[89].

This redress mechanism is only available to natural persons from qualifying states, who submit qualifying complaints. Qualifying states include all EEA Member States[90]. Complaints must be submitted to the (local) data protection authority by the data subject[91]. The qualifying complaint must be based on a 'covered violation', which is a violation that 'adversely affects the complainant's individual privacy and civil liberties interests[92]'. The exact meaning of this requirement is not further explained[93]. Standing is not required[94] meaning that individuals do not need to demonstrate that their data has been subject to US signals intelligence, as long as they reasonably believe their data has been transferred.

A complaint is then lodged with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO[95]). If the complainant is not satisfied with the answer, which is always the same, namely that 'the review either did not identify any covered violations' or the CLPO 'issued a determination requiring appropriate remediation', it is possible to appeal the decision before the DPRC.

At the time of their initial appointment, the 'judges' should not have been employees of the Executive branch in the previous two years[96]. They are appointed by the Attorney General in consultation with the PCLOB, the Secretary of Commerce and the Director of National Intelligence[97]. The Inspector General of the Department of Justice supervises compliance with the criteria and procedure for appointment and dismissal of DPRC judges[98]. Judges can only be dismissed in cases of 'misconduct, malfeasance, breach of

[89] There are currently 8 judges. Applications to the DPRC will be reviewed by a 3-judge panel (Section 3(d)(B) of the EO). Refer to https://www.justice.gov/opcl/redress-data-protection-review-court

[90] EO 14086, Section 3 (b).

[91] Commission implementing decision, recitals (176) and (177).

[92] EO 14086, Section 4 (k) (i) and 4 d (ii).

[93] EDPB Opinion 5/2023, p. 51, para. 235.

[94] EO 14086, Section 4 (k) (i) and (ii).

[95] EO 14086, Section 3.

[96] Code of Federal Regulations- Title 28 – Part 201, Data Protection Review Court, § 201.3.

[97] Commission implementing decision, recital (185).

[98] Commission implementing decision, recital (185), fn. 366.

security, neglect of duty or incapacity[99]'. Although the 'judges' may not have other official duties, they can 'participate in extrajudicial activities, including business activities, financial activities, non-profit fundraising activities, fiduciary activities, and the practice of law, where such extrajudicial activities do not interfere with the impartial performance of the judge's duties or the DPRC's effectiveness or independence[100]'.

The complainant, therefore, has no insights into the entire redress procedure. There is a special advocate, selected by the DPRC panel, which 'assists the panel in its consideration of the application for review, including by advocating regarding the complainant's interest in the matter (…)[101]', but which will not communicate the details of the procedure or the reasons for decision to the complainant.

The Task Force meetings have highlighted the 'one-sided' nature and secrecy/classified nature of the procedure, including the actual outcome, as key issues of concern from the perspective of effective remedies under EU law. The complainant will only receive a standardised official response[102] and will have no meaningful insight into the procedures, including whether the complaint has been remedied and whether the relevant data have been deleted or rectified. It does not provide the possibility to claim damages. This makes the monitoring of the envisaged remediation model of EO 14086 unfeasible and unrealistic in practice.

The DPRC's final decision cannot be appealed before US Courts[103]. In light of these structural deficits, it is surprising that the EDPB Opinion 5/2023 concludes by calling on the Commission 'to closely monitor the practical functioning of this mechanism'. The EDPB has rightly noted that the Foreign Intelligence Surveillance Court (FISC) 'does not provide effective judicial oversight on the targeting of non-U.S. persons which appears not to be resolved by the new EO 14086[104]'.

The Task Force meetings and most of the interviewees discussed and questioned the extent to which the DPRC actually constitutes a 'real court' under EU law and the extent to which it can be expected to provide effective remedies to EU citizens and residents. While nominally called a 'court' by the EO 14086, the DPRC cannot be considered a 'traditional court' or an independent judicial tribunal in the constitutional sense of the

[99] EO 14086, Section 3 (d) (vi).

[100] Code of Federal Regulations – Title 28 – Part 201, Data Protection Review Court, § 201.7 (c).

[101] EO 14086, Section 3 (d) (i) (C).

[102] According to the EO 14086, the DPRC shall inform the complainant, 'without confirming or denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."'

[103] Similarly, the concept of 'appropriate remediation' enshrined in the EO 14086 Sec.4.a envisages that it 'shall be *narrowly tailored to* redress the covered violation and to minimise adverse impacts on the operations of the Intelligence Community and *the national security of the United States*' (emphasis added).

[104] Para. 211 EDPB Opinion 5/2023.

word under US law. Under the US Constitution, the judicial branch is regulated in Article III, which is linked to the Court's status as a separate and equal branch to the Executive[105].

In the opinion of some interviewees, the DPRC seems to have been established under Article II[106]. At the same time, other interviewees noted that the DPRC is not a 'classic' Article II body either because EO 14086 foresees some additional safeguards to ensure more independence for the DPRC than any other tribunal established under Article II[107]. Crucially, a court under Article 3 is 'the final arbiter of what the law is', while the DPRC does not have that kind of autonomy. Some interviewees also underlined that those working for the Executive branch under Article II jurisdiction – unlike Article III judges – must be accountable to the President and may be removed by him, her, or them at will.

The independence of the so-called judges remains an outstanding issue. The DPRC remains part of the US Executive branch (US Department of Justice)[108]. Although EO 14086 includes some meaningful provisions primarily aimed at ensuring the 'judges' independence/impartiality[109], they are directly selected by the Attorney General without any input/accountability from the US Congress. Some interviewees expressed concerns about the excessive secrecy characterising the entire redress process. They were worried that the US President could make secret decisions[110], that would override the decisions made by the DPRC. This raises questions about whether the DPRC is truly independent

[105] The Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR) are examples of Article III Courts under US constitutional law.

[106] However, if that were the case, the DPRC would instead be a *sui generis* Article II Court because this constitutional category is based on the Executive's authority to establish them in accordance with an international treaty, supported by the US Congress, which is not the case in this instance.

[107] According to EO 14086 Section 3.d.iv, the Attorney General [shall not] remove any of the appointed judges except for instances of 'misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act.'

[108] According to Donohue and McCabe 'Separation of powers demands that the exercise of authorities that go to the core of the court acting in its judicial capacity are beyond the reach of either Congress or the Executive Branch'. This is a condition to 'ensure fairness and justice in the course of adjudication' L. K. Donohue and J. McCabe (2022), Federal Courts: Article I, II, III and IV Adjudication, *Catholic University Law Review*, Vol. 71, Issue 3, pp. 542-620.

[109] According to Section 3.(iv) of EO 14086, which deals with DPRC's independence, 'The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act'

Furthermore, representatives from some US companies participating in the Task Force were of the opinion that the DPRC remains part of the US executive branch (US Department of Justice), so that the US government can provide a court for EU data subjects which is not burdened by the US Supreme Court's high bar for standing in privacy matters in US Art. III courts.

[110] According to Gorski 'the court's decisions can be overruled by the President. Indeed, the President could presumably overrule these decisions in secret, since the court's opinions are not issued publicly'. A. Gorski (2022), The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, JUST SECURITY.

and whether it is able to make decisions without being overruled in secret as well as its durable autonomy from the US Government[111]. On this point, other Task Force participants and speakers questioned the likelihood and legality of a secretive overruling. The Office of the Director of National Intelligence (ODNI) is responsible for the 'fact-finding'. As it is part of the Executive branch, this is another point of contention that showcases the close ties between the ODNI and the US government. Moreover, the DPRC members are only allowed to assess EU law/policy and cannot include other sources of international/regional law.

[111] Acknowledging this lack of durability over time, it has been recommended that 'An adequacy finding by the EU Commission could be conditioned on these legal limits remaining in place' T. Christakis, K. Propp and P. Swire (2022), The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC, International Association of Privacy Professionals.

4. EU LAW AND THE COURT OF JUSTICE'S BENCHMARKS

Compliance with Articles 7, 8 and 47 of the EU Charter of Fundamental Rights, which bring to the fore the rights to privacy, data protection, an effective remedy, and a fair trial, including the guarantees or benchmarks established in related case law of the Court of Justice, are a *precondition* or *sine qua non* for trust in international data transfers and the adoption of an adequacy decision pursuant to Article 45(1) of the GDPR. This is confirmed by EU law and the benchmarks set by the Luxembourg Court.

4.1. THE COURT OF JUSTICE'S ADEQUACY AND ESSENTIAL EQUIVALENCE STANDARDS

When assessing the adequacy of the level of protection of personal data in a third country according to Article 45(2) of the GDPR, the Commission must particularly take into account issues which relate to the rule of law, respect for human rights, relevant (general and sectoral) legislation and its implementation, the existence of independent supervisory authorities and the third country's international commitments.

Crucially, Article 45(2) of the GDPR does not envisage any role for the Commission to consider foreign affairs or geopolitics in the decisions. And while recital 101 of the GDPR states that data transfers to third countries are 'necessary for the expansion of international trade and international cooperation', this must be subject and in compliance with the conditions laid down in the Regulation, including an adequacy decision-legal check by the Commission that is in line with the EU Charter[112].

These requirements are to be read in the light of fundamental rights, in particular Articles 7, 8 and 47 of the Charter, and result in a far-reaching indirect horizontal effect of such articles[113]. Compliance with Articles 7, 8 and 47 of the Charter, including the guarantees established in related case law, is therefore a precondition for the adoption of an adequacy decision pursuant to Article 45(1) of the GDPR. Also, the fact 'that data are liable to be processed by the authorities of the third country in question for the purposes of

[112] Recital 101 GDRP states that 'Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of *international trade and international cooperation*. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, *subject to the other provisions of this Regulation*, *the conditions laid down in the provisions of this Regulation* relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.' (emphasis added).

[113] *Schrems II*, para. 168.

public security, defence and State security', does not remove the transfer from the scope of the GDPR[114].

Articles 7 and 8 of the Charter constitute the basis for the rights to private life and data protection. Article 7 of the Charter codifies the right to private life and corresponds to Article 8 of the European Convention on Human Rights (ECHR) and must be interpreted, in accordance with Article 52(3) of the Charter, in conformity with such Article[115]. Furthermore, since the adoption of the Treaty of Lisbon, the Court of Justice has considerably contributed to the development of case law regarding Articles 7 and 8 of the Charter, whereby the relationship between these two rights is not always perfectly clear[116]. Still, in data protection-related cases of the Court of Justice, such as in the *Schrems* judgments, both provisions are of equal importance and are often examined together. Moreover, it has been argued that 'any exception in a data protection regime can be considered as valid only if it is consistent with the individual's right to respect for privacy. The two – privacy and data protection – cannot be separated and there is a hierarchical relation between them with privacy being the superior right and for which data protection enables fulfilment of the right[117]'.

Already in *Schrems I*, and by analogy to the data retention case-law including *Digital Rights Ireland*, the Court clarified that the concept of adequacy aims to ensure that the rights of Article 8(1) of the Charter are protected when data are transferred to a third country[118] and that the standard for an adequate level of protection read in the light of the Charter is strict[119]. According to the Court, 'adequate' does not mean an identical level of protection. It requires a level 'that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter[120]'.

The standard of essentially equivalent thereby relates to the carrying out of a fundamental rights check according to Article 52(1) of the Charter in the framework of data transfers and results in a 'quasi-constitutional role' of this test[121]. In practice, this close link to fundamental rights translates into a far-reaching indirect horizontal effect of Articles 7, 8

[114] *Schrems II*, paras. 86 and 89.

[115] Lock, Art. 7, para. 1.

[116] Lock, Art. 8 para. 3.

[117] S. Carrera and E. Guild (2015), The End of Safe Harbor: What Future for EU-US Data Transfers, *Maastricht Journal of European and Comparative Law*, Vol. 22, Issue 5, pp. 651-655.

[118] Schrems I para. 72.

[119] Ibid., para. 78.

[120] Ibid., para. 73.

[121] Compare L. Drechsler and I. Kamara (2021), Essential equivalence as a benchmark for international data transfers after Schrems II, in E. Kosta and R. Leenes (eds), *Research Handbook on EU data protection*, Elgar Publishing, Chapter 13, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881875, p. 14, and C. Kuner (2017), Reality and illusion in EU data transfer regulation post Schrems, *German Law Journal*, 18(4), pp. 881-919, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346

and 47 of the Charter[122], including the guarantees of its related case-law when transferring data into third countries. In *Schrems II* and in *Opinion 1/15* on the EU-Canada PNR Agreement the Court of Justice detailed the elements of this test and described how to assess this standard[123].

The adequacy and essential equivalence test apply horizontally in the context of the Commission's Adequacy Decisions, contractual arrangements such as Standards Contractual Clauses (SCCs) and international agreements. The three-step test pays attention:

Firstly, if an international data transfer interferes with EU fundamental rights to an extent that it affects *the essence* or very substance of the rights at stake; the measure is automatically disproportionate and it must be annulled or declared invalid as running contrary to EU law (*respect for the essence test*), without there being a need to apply a 'balancing exercise' between competing interests. It cannot be justified on any ground, including 'national security'. The concept of the essence of a fundamental right 'operates as a constant reminder that our core values as Europeans are absolute and, as such, are not up for balancing[124]'. While there have been few cases in which the respect of the essence of rights has been violated[125], the Court of Justice found such violations in *Schrems I* and partly in *Schrems II*[126].

Secondly, in cases where the essence of the rights at issue is not at stake, the test continues or moves towards a proportionality assessment and a balancing exercise (Article 52(1) of the Charter). And t*hirdly*, the assessment focuses on the extent to which the data transfers are justified by an objective of general interest recognised by the EU, which pursues an incremental approach: the higher the interference the higher the general interest justifying it must be.

4.2. NATIONAL SECURITY

In the specific context of national security and access to commercial data, governments argue sometimes that Article 4(2) of the TEU exempts the Court of Justice from deciding cases involving the transfer of data to national security agencies[127]. However, the Court

[122] *Schrems II*, para. 168 and Lock, Art. 8 para. 5 with regard to Article 8 of the Charter.

[123] Compare L. Drechsler and I. Kamara (2021), p. 14.

[124] K. Lenaerts (2019), Limits on Limitations: The essence of fundamental rights in the EU, *German Law Journal*, Vol. 20, pp. 779-793.

[125] G. González Fuster (2022), Study on the essence of the fundamental rights to privacy and to protection of personal data, EDPS 2021/0932 of December 2022, available at: https://www.edps.europa.eu/system/files/2023-11/study_en.pdf, p. 5.

[126] *Schrems I* paras. 94 and 95 and *Schrems II* para. 107.

[127] Schrems II, para. 81; Case C-623/17 Privacy International ECLI:EU:C:2020:790, para. 44 and joined Cases C-793/19 and C-794/19 Spacenet/Telekom, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 48.

of Justice has confirmed that 'the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law[128]'. This has also been highlighted by the FRA, which has concluded that 'some aspects of the intelligence services' work, namely surveillance of communications data, cannot be completely excluded from the scope of EU law, including the Charter[129]'.

Therefore, Article 4(2) of the TEU does not exempt the Luxembourg Court from adjudicating over the legality of international data transfers for 'national security' reasons. Data transferred between two economic partners for commercial purposes which might take place during or after the transfer processing for national security purposes in a third country, cannot remove that transfer from the scope of the GDPR and the Charter. What matters for EU law to apply is the actual activity performed by the private sector[130].

The Court of Justice has converted the concept of national security into an autonomous notion with specific EU-meaning and scope, whereby a 'threat to national security' is distinguishable from a serious criminal offences affecting public security[131]. States are therefore forced to clearly indicate which objectives they are pursuing and which (restrictive) measures they apply in a given context. Otherwise, treating categories in the same way would establish 'an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former[132]'. Moreover, while Member States may have the main competence in relation to national security, the Union has shared competence with the Member States when it comes to the EU's internal security, particularly as regards the policy areas of terrorism and crime[133].

---

[128] Case C-623/17 Privacy International ECLI:EU:C:2020:790, para. 44 referring to data retention and referencing see, to that effect, judgments of 4 June 2013, *ZZ*, C-300/11, EU:C:2013:363, paragraph 38 and the case law cited; of 20 March 2018, *Commission* v *Austria (State printing office)*, C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020, *Commission* v *Poland, Hungary and Czech Republic (Temporary mechanism for the relocation of applicants for international protection)*, C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170.

[129] FRA (2023), Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – 2023 update, Vienna, p. 8.

[130] V. Mitsilegas, E. Guild, E. Kuskonmaz and N. Vavoula (2022), Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks, *European Law Journal*, Vol. 29, Issue 1-2, pp. 176-211. In particular Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790; and paragraphs 103 and 104 of Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v. Premier Ministre and Others*, ECLI:EU:C:2020:791. According to Mitsilegas et al., 'Read together, and in line with the existing case law, they constitute a revised EU legal framework within which security services of all Member States must operate and which must be fully respected by both the national and EU legislatures.'

[131] See Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 92 and judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para. 61 and the case law cited.

[132] Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 94.

[133] S. Carrera, E. Guild and J. Parkin (2014), *Who will monitor the spies?* CEPS Commentary, Brussels.

Some Task Force members from the private sector took the view that not all aspects of national security have been dealt with exhaustively by the Luxembourg Court and considered that for those aspects the ECHR continues to apply. The Task Force presentations also mentioned the value and high significance of the Council of Europe's 2018 Convention 108+ on the protection of individuals regarding the processing of personal data, signed by all EU Member States. In its Article 11 on 'Exceptions and Restrictions' it envisages and permits the 'protection of national security' as one of these exceptions as long as it 'is provided for by law, *respects the essence of the fundamental rights* and freedoms and constitutes a *necessary and proportionate measure in a democratic society*' (emphasis added[134]). That notwithstanding, EU law benchmarks provide a higher level of protection than the one under the Council of Europe.

4.3. DATA RETENTION AND INTERNATIONAL DATA TRANSFERS

The Court of Justice's data retention case-law has confirmed the applicability of EU law when evaluating the retention, access to and the use of commercial data for national security purposes. These data cannot be accessed for combating serious crime purposes, even in the context of international data transfers. In *Schrems I*, the Court of Justice had already used the data retention case *Digital Rights Ireland* by way of analogy to establish that the adequacy requirements should be read in light of the Charter and should be interpreted strictly when data are transferred to a third country[135].

Repeatedly, in both *Schrems* cases as well as in *Opinion 1/15*, the Court of Justice references its data retention case-law and uses it by analogy to also establish standards in the third state data transfer scenario[136]. In *Opinion 1/15* on the EU-Canada PNR Agreement, the Court references the *Digital Rights Ireland* and other data retention cases such as *Tele 2* multiple times[137] which is a clear indication of its applicability (by analogy) in transfer cases too[138].

---

[134] Furthermore, the same provision states that 'This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.' Article 23 GDPR also allows for restrictions of rights for national security purposes.

[135] *Schrems* I, para. 78.

[136] Compare, *Schrems* I referencing *Digital Rights Ireland* eight times at paras. 39, 58, 78, 87, 91, 92, 93 and 94, twice *by analogy* and Schrems II referencing *Digital Rights Ireland* twice at para. 170 and 171 and Opinion 1/15 at paras. 39, 52, 54, 123, 124, 126, 140, 141, 149, 191, 192 and 201, 202 etc.; the latter by analogy to *Tele 2*.

[137] *Opinion 1/15*, at paras. 39, 52, 54, 123, 124, 126, 140, 141, 149, 191 and 192, 201, 202 etc.; the latter by analogy to *Tele 2*.

[138] See also Drechsler/Kamara, Essential equivalence as a benchmark for international data transfers after Schrems II, in Kosta/Leenes, Research Handbook on EU data protection, Elgar Publishing, Chapter 13, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881875, p. 14 and Kuner, Christopher, Reality and illusion in EU data transfer regulation post Schrems, 18(4), German Law Journal (2017), pp. 881-919, here 895, 896 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346

Furthermore, as established in *Commissioner of An Garda Síochána and Others* and *Spacenet/Telekom* and confirmed in *Opinion 1/15*[139], the conditions which relate to the retention of personal data have an important effect on the rules for accessing such data. This means that the standard for retaining data (namely prohibiting the interdiction of the general and indiscriminate retention of data to combat serious crime) also applies in the context of access. Consequently, data exceptionally retained for national security purposes cannot be accessed for the purpose of combating serious crime or threats to public security[140]. This standard-building case-law is therefore of crucial importance. It stipulates the essential requirements for retaining, accessing, and using commercial data for national security purposes in the EU. This standard needs to be used at times of measuring third country standards in similar contexts.

Thus, in judgments such as *Digital Rights Ireland, La Quadrature Du Net, Privacy International, Commissioner of An Garda Síochána and Others and Spacenet/Telekom*[141] and further cases, the Court of Justice stipulated the basic constitutional requirements which EU Member States have to respect when national security agencies retain, access and use commercial data. These essential requirements deduced from the rich case-law on data retention add to the EU standard developed in the *Schrems* cases and can serve as benchmarks against which the equivalence of the US guarantees in the Adequacy Decision have to be checked.

Furthermore, The Court of Justice has confirmed that automated analysis must be based on specific, reliable and non-discriminatory criteria. This will allow the results to target individuals who might be under reasonable and evidence-based suspicion of participation in terrorist offences or serious transnational crime. These individuals must be subject to an individual re-examination by non-automated means. In *Privacy International*, the Court was confronted with EU-bulk data collection. The Court refers to the general and indiscriminate transmission and/or collection of traffic data and location data to security and intelligence agencies[142] as a violation of fundamental rights. The Court established that such direct transmission and access of traffic data and location data to security and intelligence agencies for the purpose of safeguarding national security is not in line with fundamental rights. This type of transmission 'is likely to generate in the minds of the

[139] Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, para. 212.

[140] Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 130 and judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para. 100.

[141] Joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net (LQDN) and others* , ECLI:EU:C:2020:791; Case C-623/17 *Privacy International* ECLI:EU:C:2020:790; joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702.

[142] Compare *Privacy International*, paras. 50-52 and 69.

persons concerned *a feeling that their private lives are subject to constant surveillance*' (emphasis added[143]).

For individuals to exercise their rights and receive effective remedies they must be notified of any surveillance measures: individuals subject to automated and real-time analysis must be made aware of such analysis by way of general information[144]. However, if the 'authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually[145]'. The notification should be carried out as soon as such information is no longer liable to jeopardise the tasks for which those authorities are responsible. These criteria also apply in the transfer context which was confirmed by the Court of Justice in *Opinion 1/15* and equally relate to the situation in which data are disclosed to other governmental authorities[146].

In very limited and exceptional cases, EU Member States are allowed to retain data for national security purposes. However, three strict and cumulative conditions apply. These conditions relate to the existence of a serious threat to national security which is genuine and present or at the very least, foreseeable. Additionally, sufficiently concrete circumstances must have arisen to be able to justify a generalised and indiscriminate data retention measure. The decision imposing such an instruction must be subject to effective review, either by a court or by an independent administrative body whose decision is binding. The aim of that review is to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, as well as that the instruction is limited in time to what is strictly necessary[147].

Normally, general and indiscriminate retention of traffic and location data cannot be justified for other purposes, such as serious crime and the prevention of serious threats to public security. This is because the information and data concerned are sensitive and confidential. Retention of such data can have a dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter and the seriousness of

[143] Case C-623/17 *Privacy International* ECLI:EU:C:2020:790, para. 71; See, by analogy, judgments of 8 April 2014, *Digital Rights Ireland and Others*, paras. 27 and 37; *Tele2*, paras. 99 and 100.

[144] Joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net (LQDN) and others*, ECLI:EU:C:2020:791, paras. 190 and 191.

[145] Ibid. para. 191, referring to by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paras. 222 and 224.

[146] Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paras. 222-224.

[147] Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, paras. 72 and 93 under reference to judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para. 58.

the interference entailed by such retention. Retention should remain the exception and not the rule[148].

Nevertheless, there are limited exceptions under which the Court of Justice allows the retention of traffic and location data for purposes of serious crime prevention and the prevention of serious threats to public security. In this latter case, the Court sets clear limits on the methods of collection by prescribing that the retention needs to be targeted and limited, based on objective and non-discriminatory factors according to a geographical, personal or temporal criterion, for a period that is limited in time to what is strictly necessary. Thus, if states use targeted retention, such retention must be based on objective evidence making it possible to target persons 'whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security[149]'.

Clear and precise procedural rules to guarantee effective safeguards against the risks of abuse must underpin these exceptions[150]. These safeguards should be mirrored in the access conditions of the retained data. In *Commissioner of An Garda Síochána*, in *La Quadrature du Net*[151]*,* as well as in *Tele2*[152]*,* the Court recalled that 'legislation cannot confine itself to requiring that authorities' access to the data be consistent with the objective pursued by that legislation[153]'. Therefore, objective criteria which precisely define the conditions and circumstances in which national authorities must be granted access must be laid down by law[154]. Access by national authorities to retained data must equally be subject to prior review by an independent and impartial body, which can be a court or an independent administrative body. This body must have 'all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue[155]'.

Further, the review needs to be in advance of/prior to the use, as 'subsequent review would not enable the objective of prior review, consisting in preventing the authorisation

---

[148] Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 74.

[149] Ibid., para. 105, referring to judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para. 79 and the case law cited.

[150] Joined Cases C-793/19 and C-794/19 *Spacenet/Telekom*, judgment of 20 September 2022, ECLI:EU:C:2022:702, para. 75.

[151] Joined cases C-511/18, C-512/18 and C-520/18, judgments of 6 October 2020, *La Quadrature du Net and Others*, EU:C:2020:791, para. 189.

[152] Joined cases C-203/15 and C-698/15, judgment of 21 December 2016, *Tele2*, C-203/15, EU:C:2016:970, para. 119.

[153] *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para. 104 and Case C-623/17 *Privacy International* ECLI:EU:C:2020:790, para. 77.

[154] Ibid., para. 113.

[155] Ibid., para. 107.

of access to the data in question that exceeds what is strictly necessary, to be met[156]'. A subsequent review can therefore not substitute a prior independent review[157]. Such conditions also apply in the international data transfers context, as confirmed by the Court of Justice in its *Opinion 1/15*[158]. The same conditions governing the use of the data should apply if the retained data should be further transferred to third countries[159]. In practice, this requires that either there is an agreement between the EU and the third country equivalent to the EU-US DPF or an adequacy decision covering the third country authorities to which the data are disclosed[160].

[156] Ibid., para. 110.

[157] *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, para 112.

[158] Opinion 1/15, para. 202, 208, referring by analogy to judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paras 120 and 212.

[159] Opinion 1/15, para. 212.

[160] Compare Opinion 1/15, conclusion, point 3 (e).

4.4. EFFECTIVE REMEDIES AND JUDICIAL PROTECTION

One essential part of Article 47 of the Charter relates to the independence of courts, which 'forms part of the essence of the right to effective judicial protection and the fundamental right to a fair trial, which is of cardinal importance as a guarantee that all the rights which individuals derive from EU law will be protected and that the values common to the Member States set out in Article 2 TEU, in particular the value of the rule of law, will be safeguarded[161]'. On the Member State level, Article 19 TEU obliges them to provide remedies sufficient to ensure effective legal protection.

The Council of Europe and the ECHR standards/benchmarks are the minimum threshold of protection for interpreting corresponding rights in the EU Charter. In some cases, the EU Charter provides a higher level of protection[162]. That is the case, for instance, in relation to the scope of 'effective remedies' under Article 47 of the Charter, which focuses on access to justice by individuals as a core component of the EU rule of law – and effective legal/judicial protection – under Articles 2 and 19 TEU[163].

Article 47(1) of the Charter is linked to the right of access to a court and the right to a fair trial[164]. It establishes a substantive right of review, in particular in areas that affect rights of individuals directly[165], which is clearly the case regarding the provisions of the Adequacy Decision[166]. Like paragraph one of Article 47 of the Charter, the scope of paragraph 2 is wider than the corresponding Article 6(1) ECHR and comprises not only civil rights and obligations and criminal charges, but also public law proceedings[167].

The right to a fair and public hearing should ensure that each party to the proceedings is able to respond to the arguments of the other party and both parties are to be heard before the court[168]. The publicity of the hearing usually refers to public access to the hearing but that public nature can be restricted for example for national security purposes

---

[161] Joined Cases C-585/18, C-624/18 and C-625/18, AK, judgment of 19 November 2019 EU:C:2019:982 at para. 120 and LM, C-216/18 PPU, judgment of 25 July 2018 ECLI:EU:C:2018:586, para. 48, emphasis added.

[162] According to Drechsler (2023), the Court of Justice has not only raised the standard of the ECtHR by requiring a court but also by requiring specific remedies, namely to have access to the data, and the ability to rectify and erase them (all of which seem not ensured within the DPF). These three remedies form in a governmental access context the essence of Art. 47 (*Schrems* I, para. 95; and *Schrems* II, para. 187). L. Drechsler (2023), Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation, *Review of European Administrative Law*, 2023/1, pp. 35-54.

[163] E. Kosta and I. Kamara (2023), The Right to an Effective Remedy in International Data Transfers of Electronic Evidence: Past Lessons and Future Outlook, *Review of European Administrative Law*, Volume. 16, No. 1, pp. 57-83

[164] Lock/Martin, Article 47, para. 6.

[165] Ibid., para. 17.

[166] Schrems I, para. 95.

[167] Lock/Martin, Article 47, para. 4.

[168] Ibid. para. 36.

or the protection of the private life of the parties[169]. Defence rights must exist, such as that the addressees of a decision that significantly affect their interests must 'be placed in a position in which they may effectively make known their views on the evidence on which the contested decision is based[170]'. A 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter[171]'.

The case-law of the European Court of Human Rights (ECtHR) has recognised that both judicial and administrative bodies are within the scope of the human right to effective remedies under Articles 6(1) and 13 ECHR. However, and crucially for the purposes of this Report, EU law provides a higher level of protection by putting special emphasis on the need to ensure an impartial and independent court/tribunal guaranteeing (internal and external) judicial independence and delivering effective judicial protection and remedies. Courts must be entitled to ensure the enforcement of those rights and be capable of effectively redressing the consequences if they are violated[172].

The notion of what constitutes an independent court/tribunal has equally acquired a specific and autonomous meaning under EU law through the Court of Justice's case law[173]. The term 'tribunal' in the sense of EU law must be understood in the same way as in Article 267 TFEU[174]. Paragraph 2 of Article 47 also specifies that the 'tribunal'

---

[169] Ibid., para. 38.

[170] Ibid., para. 40 referring to C-418/11, Textdata Softwarees, EU:C:2012:588, para. 83.

[171] *Schrems I* para. 95 quoting: to this effect, judgments in *Les Verts v Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, para 80.

[172] In para.186 of the 2020 *Schrems II* judgment C-311/18, the Court held that 'the first paragraph of Article 47 requires *everyone* whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an *independent and impartial tribunal*.' (emphasis added). Refer also to Paragraph 194 of the ruling where the Court stated that 'An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission's finding of limitations on *the right to judicial protection* must, in accordance with the requirements arising from Article 47 of the Charter and the case law recalled in para 187 above, start from the premise that data subjects must have *the possibility of bringing legal action before an independent and impartial court* in order to have access to their personal data, or to obtain the rectification or erasure of such data.' (emphasis added).

[173] A tribunal in EU law has to be understood in the same way as in Article 267 TFEU. The term requires factors such as 'whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is inter partes, whether it applies rules of law and whether it is independent.' Compare with Art. 267 TFEU Case C-175/11*, D. and A.*, EU:C:2013:45, para 83 with reference to Case C-53/03 *Syfait and Others* [2005] ECR I-4609, para 29; Case C-517/09 *RTL Belgium* [2010] ECR I-14093, para 36; and Case C-196/09 *Miles and Others* [2011] ECR I-5105, para 37. See V. Mitsilegas, Autonomous Concepts, Diversity Management and Mutual Trust in Europe's Area of Criminal Justice, *CMLR* 57 (2020), 45.

[174] Lock/Martin, Article 47, para. 4 referring to Case C-175/11, *D. and A.,* EU:C:2013:45, para. 83, compare also *Tzanou/Vogiatzoglou*, In search of legal certainty regarding 'Effective Redress' in international data transfers: unpacking

mentioned in paragraph 1 needs to be 'independent and impartial' and 'established by law'. The latter condition was specified in cases C-487/19 and C-132/20, in which it was found that 'established by law' should ensure that 'the organisation of the judicial system does not depend on the discretion of the Executive, but that it is regulated by law emanating from the legislature in compliance with the rules governing its jurisdiction[175]'.

This requirement reflects the principles of the rule of law and relates not only to 'the legal basis for the very existence of a tribunal, but also the composition of the bench in each case and any other provision of domestic law (…)[176]'. Connected with this principle is independence. As mentioned above, in *AK*, the Court recently confirmed that the requirement of courts being independent:

> '.. is inherent in the task of adjudication, forms part of the *essence of the right to effective judicial* protection and the *fundamental right to a fair trial,* which is of cardinal importance as a guarantee that all the rights which individuals derive from EU law will be protected and that the values common to the Member States set out in *Article 2 TEU*, in particular the value of *the rule of law*, will be safeguarded (emphasis added[177])'.

The terms judiciary respectively judicial authorities refer 'to authorities that administer justice', 'unlike inter alia administrative authorities or police authorities, which are within the province of the Executive[178]'. The judiciary is to 'be distinguished, in accordance with the principle of the separation of powers which characterises the operation of the rule of law, from the Executive[179]'. Consequently, administrative bodies or complaint and/or accountability mechanisms are therefore not a permissible substitute of an effective right to appeal before an independent Court under Article 47 EU Charter. Further, the underlying concept of judicial independence[180] builds a pre-requisite for being a 'court'

---

the conceptual Complexities and clarifying the substantive requirements, *Review of European Administrative Law* Vol. 16, NR. 1, 11-34c 2023-1, pp. 11-34.

[175] C-487/19, WZ, judgment of 6 October 2021, EU:C:2021:798 at para. 129 and C-132/20, judgment of 29 March 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, para. 121.

[176] C-487/19, WZ, judgment of 6 October 2021,EU:C:2021:798 at para. 129 and C-132/20, judgment of 29 March 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, para. 121.

[177] Joined Cases C-585/18, C-624/18 and C-625/18, AK, judgment of 19 November 2019 EU:C:2019:982 at para. 120 and LM, C-216/18 PPU, judgment of 25 July 2018 ECLI:EU:C:2018:586, para. 48, emphasis added.

[178] *Poltorak*, C-452/16 PPU, EU:C:2016:858, para. 35.

[179] *Poltorak*, C-452/16 PPU, EU:C:2016:858, para. 35.

[180] To that concept compare in detail: V. Mitsilegas (2020), Autonomous Concepts, Diversity Management and Mutual Trust in Europe´s Area of Criminal Justice, *Common Market Law Review* 57, pp. 45-78.

or 'tribunal' in the sense of the Charter[181]. A court/tribunal that lacks the necessary independence is not a court within the Article 47 (2) of the Charter[182].

The Court then reflects, e.g. on the 'imperviousness' of the respective 'court' to external factors, 'in particular, to the direct or indirect influence of the legislature and the Executive, and as to its neutrality with respect to the interests before it (...)'[183]. Whether factors such as the secondment of judges[184] or the retrospective unconstitutionality of a panel leads to a violation of judicial independence[185] is to be assessed together with other measures[186]. It is therefore very surprising that the EDPB Opinion 5/2023 makes use of and seems to give priority to the standards developed by the European Court of Human Rights under Article 13 ECHR, instead of those by the Luxembourg Court. The opinion concludes that the DPRC does not need to be a judicial authority, and that 'the specific redress mechanism created under EO 14086 as opposed to redress in Article III courts is not per se insufficient[187]'.

[181] In *Hungary v. Parliament* and *Poland v. Parliament* the Court insisted that 'the second subparagraph of Article 19(1) TEU, interpreted in the light of Article 47 of the Charter, imposes on the Member States a clear and precise obligation as to the result to be achieved that is not subject to any condition as regards the independence which must characterise the courts called upon to interpret and apply EU law (…)'. Refer to C-156/21, *Hungary v. Parliament*, judgment of 16 February 2022, ECLI:EU:C:2022:97, para. 162 and *Poland v. Parliament,* judgment of 16 February 2022, ECLI:EU:C:2022:98, para. 198.

[182] Similar with regard to Art. 267 TFEU, Harbarth/Spielmann (2023), EU review of judicial independence in the Member States: its foundations and limits, *E.L. Rev*., 48(6), pp. 681-695.

[183] Joined Cases C-585/18, C-624/18 and C-625/18, *AK*, EU:C:2019:982 at para. 153.

[184] Joined Cases C-748/19 to C-754/19, WB et al., ECLI:EU:C:2021:931, paras 73 et seq.

[185] C-132/20, Getin Noble Bank SA, ECLI:EU:C:2022:235, paras 126-127.

[186] Harbarth/Spielmann, p. 8.

[187] Para 220 of EDPB Opinion 5/2023. Furthermore, as explained above in this Report, there is no consensus that the DPRC actually constitutes an Article III Court under US constitutional law.

5. FITNESS CHECK

5.1. PRIVACY, NATIONAL SECURITY AND LAW ENFORCEMENT IN LIGHT OF THE RULE OF LAW

The Task Force meetings and some of the interviewees underlined how the conversation on US-EU data transfers has shifted from having a comprehensive data protection framework similar to the GDPR and the fundamental right of privacy, to a discussion focused on the inner-workings and accountability regimes of national security, surveillance and intelligence communities in both sides of the Atlantic, as well as the use of a balance metaphor between data protection and national security[188]. This marked a noticeable transition from a data protection approach to a more technical and narrower debate centred on national security and intelligence services[189].

Transatlantic data flows are not exclusively an issue of 'national security'. A key finding of this Task Force is that national security is often used in transatlantic data transfer debates to frame the matter of adequacy exclusively from a security and intelligence community's perspective. This securitarian focus first disregards the wider issues related to law enforcement/criminal justice cooperation and commercial matters covered by the Adequacy Decision and the DPF[190]. It also shifts the conversation from the obligation to uphold privacy and data protection and effective remedies standards, to another centred around the use of a balance metaphor of individual rights and collective security. Previous scholarly work has demonstrated[191] that this has tended to translate in policies that

[188] In his introductory remarks in a session titled 'Moving towards a sustainable and functional EU-US Transfers Framework part of the 2023 Computers, Privacy and Data Protection (CPDP) International Conference,' former European Commissioner for Justice Didier Reynders, who led the EU negotiations with the US authorities, highlighted that, 'EU values need to be fully upheld in an interconnected world and that EU protections will travel with the data to other parts of the world'. He also noted that 'the negotiations of the new EU-US Framework revealed one of the most sensitive issues for any society: the balance between individual rights and collective security'. Available at https://www.youtube.com/watch?v=6zsDvertlTg The balance metaphor was also mentioned by several EU official speakers and representatives of the private sector during some Task Force meetings.

[189] Some Task Force members expressed the view that the transition from a comprehensive data protection framework to more specific discussions on national security, surveillance, and foreign intelligence could be largely attributed to the *Schrems II* ruling by the Luxembourg Court.

[190] In 2019, the EDPB raised, for instance, concerns about the commercial component of the Privacy Shield regarding issues of insufficient oversight and supervision regarding the substance of the Privacy Shield principles. It also concluded that 'it is important that the Commission continues monitoring cases related to automated decision-making and profiling and to contemplate the possibility to foresee specific rules concerning automated decision-making to provide sufficient safeguards, including the right to know the logic involved and to challenge the decision obtaining human intervention when the decision significantly affects him or her,' pp. 15 and 16. EDPB (2019), EU-US Privacy Shield – Third Annual Joint Review, November.

[191] According to Guild, Carrera and Balzacq (2010), 'The constitutive problem of the metaphor is the belief that freedom and security are analogous concepts, and thus can be compared with and weighed against each other. This belief is difficult to uphold. Freedom, and its more concrete formulation as liberty, is a central value that can be found at the heart of not only the EU treaties but also of all international human rights treaties….What is common to all the understandings of liberty is that it is the defining value: democracy, the rule of law and fundamental rights are designed

prioritise national security over civil liberties and rule of law impacts. In that regard, the Court refers to the separation of powers which operationalise the rule of law and require an independence of the judiciary in 'relation to the legislature and the Executive'. Judges must therefore be protected from external interventions or pressure and any direct and indirect influence[192]. Furthermore, the involvement of an independent court is particularly salient to ensure fair trial principles. These require procedural fairness, including fair and public hearing, duty to give reasons and defence rights. This is especially important in national security cases and their linkages with the use of 'e-evidence' in criminal investigations[193].

There are far-reaching differences between the standards enshrined in EO 14086 and those currently applicable in the EU as regards the scope of 'national security' and the grounds justifying 'bulk' or large-scale surveillance by intelligence communities and law enforcement actors. The EU autonomous definition of national security is much narrower in material scope. It does not include 'serious threats to public security' or serious criminal offences as lawful grounds or considerations. The EO 14086 has been drafted with conceptual ambiguity and a wide margin of discretion and is characterised by a lack of legal precision and foreseeability.

The EU legal standard developed for the targeted collection of data, as established in the CJEU data retention case law also serves as a benchmark for international data transfers. Direct indiscriminate transmitting and providing access to traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security is not in line with fundamental rights under the EU Charter. This is even more problematic because there was no prior review by an independent body in the US and there was not an effective and impartial ex post review.

During the Task Force meetings several presentations highlighted the current misapplication or lack of enforcement of EU data protection standards, and how some EU Member States face obstacles in accessing effective remedies regarding actions by their intelligence communities. A Letter issued by former Commissioner for Justice Didier Reynders to US Attorney General Garland and US Secretary of Commerce Raimondo on 20 June 2023[194] underlined that there are common limitations and safeguards applying

to protect the liberty of the individual within the society.' E. Guild, S. Carrera and T. Balzacq (2010), The Changing Dynamics of Security in an Enlarged European Union, in D. Bigo, S. Carrera, E. Guild and R.B.J. Walker (eds), *Europe's 21st Century Challenge: Delivering Liberty*, Ashgate, pp. 31-48. See also D. Bigo, 'Liberty, whose Liberty? The Hague Programme and the Conception of Freedom', in T. Balzacq and S. Carrera (eds), *Security versus Freedom? A Challenge for Europe's Future,* Aldershot: Ashgate Publishing, 2006, pp. 35-44.

[192] Joined Cases C585/18, C624/18 and C625/18, *AK*, judgment of 19 November 2019 EU:C:2019:982 at para. 125.

[193] S. Carrera and M. Stefan (2020), *Access to Electronic Data for Criminal Investigation Purposes in the EU*, CEPS Liberty and Security Series, Brussels, pp. 55-57.

[194] Letter from Commissioner Reynders, Ares(2023) 6488529 s, signed on 20/06/2023 16:44 (UTC+02) in accordance with Article 11 of Commission Decision (EU) 2021/2121

to government access to data for reasons of national security across the EU, and that 'while they are implemented in various ways in different national systems, they are comparable to the limitations and safeguards that were the subject of the negotiations between the European Commission and the United States' Government'.

The same letter emphasised that these safeguards 'apply regardless of the nationality or place of residence of concerned individuals and are therefore also applicable to the data of US persons transferred to the territory of the EU', and crucially that 'the principles mentioned in this letter are reflected in the constitutional law of the EU Member States and are applied by their courts'. Additionally, any individual, regardless of nationality or place of residence, may, after exhausting such domestic remedies, bring a claim before the European Court of Human Rights.

The FRA has concluded that all EU Member States 'provide the opportunity for individuals to complain about privacy and other rights violations before a judge[195]'. The FRA Report confuses access to effective complaint mechanisms before administrative bodies with the scope of Article 47 EU Charter of effective remedies before an independent tribunal or Court in EU law when concluding that ,'EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals' complaints related to surveillance', and that, 'while such remedies do not need to be of a judicial nature, they need to be effective.' A complaint mechanism may well complement but cannot be a substitute for effective remedies before a court.

Some Task Force participants pointed out that transatlantic data transfer debates should not be a 'beauty contest', finger-pointing or an 'everybody does it' approach[196]. This could, otherwise, lead to a race to the bottom in accountability and justice safeguards around the world. In any case, if and when any EU Member States' intelligence communities/actors engage in similar practices than those considered unlawful by the Luxembourg Court case law[197], they are or would be engaging in unlawful or illegal practices in the EU legal system and would be subject to responsibilities and liabilities[198].

---

[195] Refer to FRA (2023), p. 35.

[196] For an analysis arguing the variation that currently exists in EU Member States as a way to call the CJEU to apply a 'flexible approach' in its adequacy assessment refer to C. Kerry (2023), Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?, Lawfare.

[197] According to Rojszczak (2021), 'The bulk interception of communications from other Member States is not necessary to protect national security. Similarly, cooperation with the intelligence services of third countries in order to eavesdrop on European neighbours does not strengthen mutual trust among EU countries'. M. Rojszczak (2021), Extraterritorial Bulk Surveillance after the German BND Act Judgment, *European Constitutional Law Review*, Vol. 17, Issue 1, pp. 53-77.

[198] According to Kuner 'Strictly speaking, the data protection standards of Member State intelligence agencies are irrelevant for judging the standard of protection offered by third countries, and a violation of fundamental rights by a

Ensuring effective democratic and judicial checks and balances of intelligence communities – and their linkages with the Executive power – is a core component of the EU's notion of the rule of law. Despite this, the current state of intelligence and law enforcement communities in EU Member States, as well as their accountability, is legally irrelevant and is not included in the material scope of the Adequacy Decision made by the Commission under the GDPR and LED. Nor is it included in the CJEU's external examination/legal check of the relevant foreign law and its adequacy or 'essential equivalence' with EU law benchmarks. EU law requires that the core focus of assessment must be the extent to which they are *EU Charter-proof*.

5.2. EFFECTIVE REMEDIES AND JUSTICE

The two-level redress mechanism model envisaged by EO 14086 is not fully in line, or essentially equivalent with Article 47 EU Charter standards as interpreted by the Luxembourg Court. The role of effective legal and judicial protection is different from the need to ensure independent oversight and accountability by an administrative body. This raises incompatibility issues when ensuring the effectiveness of EU law and the rule of law in Articles 2 and 19 TEU.

Unlike some authors' opinions[199], and the EDPB interpretation[200] even if Chapter V of the GDPR on international data transfers refers to 'effective judicial or *administrative* redress' or an '*administrative body*[201]', EU primary law – which includes the EU Charter of Fundamental Rights – has a higher hierarchical value in the EU legal system. Therefore, EU secondary legislation must be interpreted consistently with the Charter and not the other way around. This confirms that Article 47 EU Charter applies extraterritorially. Additionally, the judicial nature of the remedies at issue is crucial[202] to upholding fair trial principles under this same Charter provision. This is particularly important in the context

third country cannot be excused because Member State standards may be lacking.' *Kuner* adds that from a moral and political point of view, 'it would enhance the legitimacy of EU law in the eyes of third countries if national security was clearly brought within the ambit of EU fundamental rights law'. C. Kuner (2017), Reality and illusion in EU data transfer regulation post Schrems, 18(4), *German Law Journal*, pp. 881-919, here 899, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

[199] See Section 186 of the *Schrems II* judgment as analyzed by M. Barczentewicz (2023), *Key Legal Issues of the EU's New U.S. Data Protection Adequacy Decision*, Transatlantic Technology Law Forum (TTLF) Working Papers, No. 99, Vienna; and T. Christakis, K. Propp and P. Swire (2022), *The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC*, International Association of Privacy Professionals (IAPP), available at https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/

[200] European Data Protection Board (EDPB), Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para 47.

[201] However, Article 79(1) GDPR foresees the 'right to an *effective judicial remedy* against a controller or processor' (emphasis added).

[202] For a similar scholarly conclusion refer to *Tzanou and Vogiatzoglou*, In search of legal certainty regarding 'Effective Redress' in international data transfers: Unpacking the conceptual complexities and clarifying the substantive requirements, *Review of European Administrative Law* Vol. 16, NR. 1, 11-34, 2023-1, pp. 11-34.

of increasing use and extra-territorial requests of 'e-evidence' held by private companies for purposes related to both 'national security' and criminal justice investigations.

It is unclear whether the DPRC qualifies as an independent court, separate from the US Executive branch, with the power to deliver 'rule of law' and issue decisions of a judicial nature as required by EU law. This is true for both the US and EU legal systems, which also questions the existence of an effective remedy for EU law purposes. The DPRC does not fully comply with the EU autonomous definition of 'what is a tribunal' and 'effective remedies' anchored in EU primary law. This is particularly true with respect to the tribunal's full independence/autonomy, as well as its impartiality, which is at stake for instance in light of the DPRC's prohibition to interpret the notions of 'necessity and proportionality' on any grounds different from those in US policy and US Supreme Court rulings. The inherently classified/secret nature of proceedings and outputs[203], the standardised response to every complainant/and the lack of possibility for damages and compensation, as well as the lack of a right of appeal before relevant US Courts, all contribute to the tribunal's failure to fully comply with EU standards.

The EO does not offer EU citizens and residents a meaningful opportunity to pursue effective legal remedies which are actionable before relevant US Courts to access their own data, or to obtain the rectification or erasure of such data. It is uncertain to what extent the EO redress mechanism can be expected to safeguard the essence of the substantial and procedural components comprising the right to 'effective remedies' under Article 47 EU Charter. This right is essential to the rule of law in the EU, as emphasised by the Luxembourg Court[204]. Therefore, based on the above analysis, it is understandable that key stakeholders, including data citizens and companies, seek more legal certainty. However, the current DPF framework still generates legal uncertainty. Despite noticeable improvements, US policy does not fully satisfy the essential equivalence test and the Luxembourg Court benchmarks[205].

---

[203] There is a noted problem of overclassifying information in the US, and thus it appears unlikely that more information about the process will become available through Freedom of Information Act (FOIA) requests. On the issue of overclassifying information refer to A. B. Zegart (2022), *Spies, lies, and algorithms*, Princeton University Press, pp. 29-33.

[204] Case C-216/18 PPU *Minister for Justice and Equality* [2018], ECLI:EU:C:2018:586, para. 51. See also Case C-64/16 *Associação Sindical dos Juízes Portugueses* [2018] ECLI:EU:C:2018:117, para. 36; and *Schrems II* in para. 187.

[205] For a similar conclusion refer to Drechsler et al., who have concluded that 'Based on our analysis we can see enough issues within the draft DPF that could enable the CJEU to annul it, should it be requested to review its legality…Yet, this new regime fails to sufficiently address some of the key concerns of the CJEU when it comes to necessity and proportionality of governmental access, and the legal remedies that should be available to individuals. We are therefore closer to essential equivalence but at least from our perspective, not quite there yet.' L. Drechsler, A. Elbi, E. Kindt, E. Kun, J. Meszaros and K. Vranckaert (2023), Third time is the charm? The draft Data Privacy Framework for international personal data transfers from the European Union to the United States, *CiTiP Working Paper Series*, 23 May 2023, KU Leuven Centre for IT and IP Law, p. 37.

6. POLICY RECOMMENDATIONS

Based on the assessment provided above, we put forward the following policy recommendations:

Policy Recommendation 1: The European Commission should pursue a merited or deserved trust paradigm when negotiating, adopting and monitoring Adequacy Decisions with third countries that are fully consistent with CJEU case law. The Commission should first give priority to complying with its role as guarantor of the EU Treaties and the enforcement and uniform application of EU law (e.g. GDPR and LED), when conducting its own assessment on the adequacy and 'essential equivalence' of the level of protection in all non-EU countries, including the US. The Commission should comply with the prescribed material scope of assessing Adequacy Decisions, which does not expressly include geopolitical or foreign affairs considerations. In any case, the Commission is constitutionally required to promote and ensure full consistency with EU values in all its foreign affairs policies (Article 21 TFEU), including the EU Charter and the rule of law (Articles 2 and 19 TEU).

Policy Recommendation 2: The Commission should increase the transparency of its adequacy assessment methods and its internal assessment capacities by setting up of a new independent monitoring mechanism composed of a permanent Panel of leading academics with the highest integrity standards and proven long-standing scientific record on data protection and the rule of law. This panel should study the scope, implementation and relevant data protection/privacy developments in third countries in light of EU law and case law benchmarks from an EU values perspective. Some Task Force members questioned the value added and potential impact of such a Panel given how little consideration there is to independent evidence in current EU policies and their impacts on privacy and the rule of law.

To ensure this new Panel is effective, the Commission should commit to consulting the Panel's opinion when adopting, amending or suspending relevant Adequacy Decisions, as well as ask for its inputs during the envisaged DPF Joints Reviews and – in line with the 2016 Interinstitutional Agreement on Better Law-Making – report back to the European Parliament on the way in which it has considered their findings. The Panel's outputs should be also made available to the public to ensure transparency. The Panel should be a constitutive component of the Commission's wider Annual Rule of Law Report, to complement the Commission's own political assessments with an analysis meeting the highest independence and scientific integrity standards[206].

[206] Refer to https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2023-rule-law-report_en

Policy Recommendation 3: The European Commission should carry out more periodical reviews of its Adequacy Decisions and their practical application. The upcoming review in the scope of the Adequacy Decision with the US should prioritise the effective application and consistent interpretation of the DPF's principles and safeguards, both in law and practice. It should fully ensure all the relevant EU law benchmarks[207]. Furthermore, special attention should be paid to: (i) effective remedies; (ii) issues on onward transfers outside the US; and (iii), the exact scope, applicable legal rules and the impacts on 'adequacy' due to the increasing use of automated decision-making and AI in international data transfers in line with EU and CJEU legal benchmarks[208].

Policy Recommendation 4: The material scope and independence of the assessment carried out by the EDPB under Article 70.1.s GDPR in an opinion on the adequacy of the level of protection in a third country, and the 'European Essential Guarantees for Surveillance Measures' should be further guaranteed, clarified and narrowed down. In its assessments, the EDPB should take not only EU data protection secondary law as its point of departure (chiefly the GDPR and the LED) but also broader EU rule of law and fundamental rights, Treaty and EU Charter values. It should also consider all relevant CJEU benchmarks which are specific and autonomous in the EU legal system, and which provide a *higher level of protection* than those under the ECHR, e.g. CJEU data retention case law, what qualifies as effective remedies under Article 47 EU Charter of Fundamental Rights, etc.[209].

Policy Recommendation 5: Several Task Force participants referred to the practical hurdles of the complaint mechanism within the EU. They noted that information on how to bring individual claims before EU data protection authorities if personal data has been transferred to third states is missing. This is now resolved by the EDPB's complaint form and the information note on the DPF. However, the template complaint form confirms that complainants should be aware that the 'notification (by the DPRC) will neither

[207] The European Parliament Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), 9_TA(2023)0204, concluded that 'the EU-US Data Privacy Framework fails to create essential equivalence in the level of protection', and underlined in Paragraph 18 'that the Commission was not in a position to assess the effectiveness of the proposed remedies and proposed measures on access to data "in practice"; concludes, therefore, that the Commission can only proceed with the next step of an adequacy decision once these deadlines and milestones have first been completed by the United States to ensure that the commitments have been delivered in practice"'

[208] CJEU, C-817/19 *Ligue des droits humains v Conseil des Ministres*, 21 June 2022.

[209] Hofmann and Mustert have noted that, 'The Commission's problem in conducting adequacy assessments might be its "political capture", i.e. the Commission's mixing of foreign trade concerns with fundamental rights protection' and have recommended that, 'A solution may lie in expanding the EDPB's competences, for instance, based on a system similar to the European supervisory authorities' competence to develop technical standards in the context of the European system of financial supervision…. Importantly, this allows for such standards to be more technical or evidence-based, less based on political and strategic considerations of Commission policy preferences in other matters', p. 5. H. Hofmann and L. Mustert (2023), Procedures Matter – What to Address in GDPR Reform and a new GDPR Procedural Regulation, Law Research Paper Series, No. 2023-02.

confirm nor deny whether you have been the target of surveillance, nor will it confirm the specific remedy that was applied[210]'. This wording might discourage individuals from submitting complaints at all, which is an additional structural and practical hurdle that cannot be overcome by a simple template.

Policy Recommendation 6: If the European Commission's plan to explore the adoption of non-legally binding guidance for EU Member States on national security goes ahead, this guidance should ensure full alignment with CJEU case law benchmarks[211]. In any case, the applicability of national security under EU law will always be subject to the CJEU's interpretation regardless of any EU instrument in this domain.

The Commission should ensure more effective and timely enforcement of CJEU benchmarks and the EU data protection *acquis*, including in the scope of the Data Protection Law Directive (LED), by EU Member States' intelligence and law enforcement authorities. The EU should monitor the intelligence and surveillance practices of its Member States more systematically. This should be a self-standing theme within the material scope of Article 2 TEU values monitoring and the Annual Rule of Law Report. In some cases, this could include launching rule of law infringement proceedings against relevant Member States whose intelligence communities have rule of law deficiencies[212].

Policy Recommendation 7: Several Task Force members and interviewees have referred to the need to ensure 'legal' instead of 'geopolitical' measures on transatlantic data transfers. They have also stressed the importance of increasing investments and innovation (digitalisation) to ensure the more effective application of the only two international agreements which have been ratified by the US Congress after 9/11. These agreements specifically deal with mutual legal assistance (MLAs) and extradition[213]. Furthermore, negotiations and the potential future adoption of any new international

---

[210] Refer to https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en, page 3 of the template.

[211] Refer to European Commission (2023), follow up to the European Parliament non-legislative resolution on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, SP(2023)436, 15 November 2023. The Commission states that, 'the Commission is exploring the possibility of presenting *a non-legislative initiative clarifying the boundaries and the interplay between EU law*, in particular the data protection and privacy acquis, and national security.' It adds that 'even where the use of spyware surveillance software, such as Pegasus, is linked to national security, *there is a need for national checks and balances* to ensure that safeguards are in place. Recourse to such tools by Member States' security services needs to be subject to sufficient checks and *to fully respect EU law*. In this regard, where relevant, the country chapters have included the functioning of national checks and balances for concerns over investigations into the use of spyware surveillance software' (emphasis added).

[212] Paras. 32, 42 and 121 of the European Parliament Recommendation of 15 June 2023 following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP), P9-TA(2023)0244, 15 June 2023.

[213] See Agreement with the United States on mutual legal assistance | EUR-Lex (europa.eu) For a study on the effectiveness and untapped potential of MLAs refer to S. Carrera, M. Stefan and V. Mitsilegas (2020), *Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*, Task Force Report, CEPS, Brussels.

agreement between the EU and the US, such as a future EU-US e-Evidence Agreement[214], must fully align and provide the required EU legal and judicial benchmarks complying with the principles of EU Treaties, the EU Charter of Fundamental Rights as well as the CJEU standards examined in this Report.

Policy Recommendation 8: The discussions held during the various Task Force meetings, as well as most interviews held with US scholars and experts, have highlighted the gap in the US regarding the non-existence of a comprehensive federal data protection law[215] and a federal independent data protection authority. The US Congress may finally consider such a law during its current session following the public unveiling of the new 'Comprehensive Data Protection Legislation' entitled 'The American Privacy Rights Acts', which was published on 7 April 2024[216]. Interviewees underlined the need for US companies to support such a reform and envisage the required safeguards for EU citizens and residents.

[214] Refer to Politico (2024), *EU, US near deal on police access to online data*, 18 January 2024, available at https://www.politico.eu/article/eu-us-near-deal-police-access-online-data/

[215] According to Rotenberg, 'The original recommendations for the US have only become more urgent: (1) enact comprehensive federal privacy legislation, (2) establish an independent data protection agency, and (3) ratify the Council of Europe Privacy Convention', in M. Rotenberg (2020), *Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection, *Eur Law J.*, pp.1-12.

[216] Refer to https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation and the Draft is available here https://www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F It is interesting to note that the proposed Bill includes references to the EU-inspired concepts of proportionality and purpose limitation under Section 3.d Titled 'Data Minimisation' (Permitted Purposes) Refer also to Section 3.d.12 which refers to 'to prevent, detect, protect against, or respond to an imminent or ongoing public safety incident (such as …a national security incident)'. Regarding the personal scope, Section 2.24 defines 'individual' as 'a natural person residing in the United States'.

ANNEX I - INTERVIEWS

Occupation	Date of the interview
Representative of EU national data protection authority	8 December 2023
Representative of EU agency	12 December 2023
Academic; former officer in a US national intelligence authority	8 February 2024
Academic in the US	21 February 2024
Academic in the US	21 February 2024
US Civil society representative; attorney	28 February 2024
US Legal practitioner; attorney	29 February 2024
Academic in the US	15 March 2024
Officer at a US national intelligence authority	27 March 2024

ANNEX II – TASK FORCE MEETINGS AGENDAS

TASK FORCE

EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy

First Meeting

7 December 2023, 13:00pm to 16:00pm

AGENDA

13:00 13:10	Welcome & Introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice andHome Affairs Unit, CEPS
	Keynote Speech by Wojciech Wiewiórowski *European Data Protection Supervisor (EDPS)*	
	Opening Panel: The New EU-US Data Privacy Framework	
13:25 14:15	Chair Sergio Carrera CEPS	• Bruno Gencarelli, Head of Unit, European Commission, DG JUST,International Affairs and Data Flows • Franziska Boehm, Professor, Karlsruhe Institute of Technology
14:15 14:35	Q/A Session	All Task Force Participants

14:35 14:45	Break	
	Which ways forward and any policy/legal solutions in the EU?	
14:45 15:45	Chair Sergio Carrera CEPS	• Herwig Hofmann, University of Luxembourg • Zuzanna Gulczynska, University of Ghent • Peter Kimpian, Data Protection Unit, Council of Europe • Valsamis Mitsilegas, Professor, University of Liverpool
15:45 16:00	Q/A Session	All Task Force Participants
16:00	Closing remarks & Next steps	• Sergio Carrera CEPS

TASK FORCE

EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy

Second Meeting

18 January 2024, 13:00 to 15:30

SCOPE & QUESTIONS

This second Task Force meeting aims at assessing the new EU-US Data Privacy Framework (DPF) in light of the main changes and latest developments introduced in US policy and the US surveillance and privacy/information policies, laws and practices. The meeting seeks to examine the main themes at stake in US law and policies which are of the highest relevance for determining the adequacy of data transfers from the EU. Particular attention will be paid to their relationship and compatibility with the points raised by the Luxembourg Court, the European Parliament and the European Data Protection Board (EDPB). The following questions will be examined:

- What is the state of play and the main innovations in current US policy/law?
- What are the expected practical impacts of these new arrangements for EU citizens, companies and the rule of law?
- Are there any key outstanding questions and dilemmas when reading these in combination with EU law? In which ways could these be comprehensively addressed?

AGENDA

12:30 13:00	Registration & Light Lunch	
13:00 13:10	Welcome & Introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice andHome Affairs Unit, CEPS
	PANEL	
13:10 14:40	Chair Karel Lannoo CEPS	• Lisa Büttgen, Border Travel and Law Enforcement EDPB Subgroup (BTLEESG) - *Online* • Marc Rotenberg, Centre for AI and Digital Policy (CAIDP) - *Online* • Emilio de Capitani, Queen Mary University of London and Former Secretary of European Parliament LIBE Committee • Joe Cannataci, University of Groningen and Former UN SpecialRapporteur Right to Privacy • Calli Schroeder, EPIC & Transatlantic Consumer Dialogue (TACD) - *Online* • Anitha Ibrahim, Amazon AWS • David Pendle, Microsoft - *Online*
14:45 15.30	Debate and Q/A Session	All Task Force Participants
15:30	Closing remarks and Next Steps	• Sergio Carrera

TASK FORCE

EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy

Third Meeting at CEPS Ideas Lab Session

Beyond Adequacy: Fixing the EU-US privacy quarrel

4 March 2024
The Square, Brussels, 17:15pm - 18:30pm

SCOPE

In July 2023 the Commission published a new Adequacy Decision (the so-called EU-US Data Privacy Framework) giving the green light to transatlantic data transfers. This is the third attempt to establish a transatlantic data transfers framework in compliance with the GDPR. The two previous Adequacy Decisions - Safe Harbour and the Privacy Shield were invalidated by the Luxembourg due to their failure to secure an equivalent level of data protection in the US and the violation of the essence of EU privacy and effective remedies rights. The new Adequacy Decision is expected to end up before the Luxembourg Court once more, which leads to legal uncertainty and mistrust. It will discuss a toolbox of ideas to overcome the EU US privacy unresolved dilemmas, in particular, how can independence in the Adequacy Decisions and the effectiveness of EU citizens' rights be better guaranteed?

AGENDA

17:15 17:20	Welcome & Introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice andHome Affairs Unit, CEPS
17:20 18:15	Chair Sergio Carrera CEPS	Speakers: • Margot E. Kaminski, Professor, University of Colorado, EUI • Neil M. Richards, Professor, Washington University • Marc Rotenberg Executive Director and Founder of the Center for AIand Digital Policy - CAIDP *Discussants:* • Franziska Boehm, Professor, Karlsruhe Institute of Technology • Camille Ford, Researcher, CEPS
18:15 18:30	Q/A Session	All Task Force Participants & Ideas Lab Invitees

TASK FORCE

EU-US Data Transfers and their Impacts on Trust, Rule of Law and Privacy

Final Meeting

8 April, 13:00 to 15:30
CEPS Conference Room (Place du Congrès 1, 1000 Brussels)

SCOPE

This ultimate meeting will present the findings and policy recommendations of the Task Force on the new EU-US Data Privacy Framework (DPF). This meeting includes a final report brief, which provides a synthesis of key findings and recommendations. Throughout this final meeting, the Co-Rapporteurs will present the main conclusions and ways forward, while immediate remarks will be provided by six discussants representing European institutions, companies, NGOs and universities. Finally, there will be an opportunity for a discussion with all present Task Force members on the Report and the way forward.

AGENDA

12:30 13:00	Registration & Light Lunch	
13:00 13:10	Welcome & Introduction by the Chairperson	• Sergio Carrera, Co-Rapporteur, Senior Research Fellow and Head of the Justice and Home Affairs Unit, CEPS
13:10 14:20	Presentation of the Final Report	**Presenter** • Franziska Boehm, Co-Rapporteur, FIZ Karlsruhe **Discussants** • Anna Buchta, Head of Unit, 'Policy & Consultation', European Data Protection Supervisor (EDPS) • Paul Nemitz, Principal Adviser on the Digital Transition, DG JUST, European Commission • Maria Tzanou, Senior Lecturer, University of Sheffield and Permanent Scientific Advisor to the Greek Ministry of Justice on data protection issues • Corinna Schulze, Senior Director of EU Government Affairs, SAP (online) • Silvia Lorenzo Pérez, Programme Director for Security, Surveillance and Human Rights, Centre for Democracy and Technology (CDT) Europe • Gloria González Fuster, Research Professor, VUB and Director, Law, Science, Technology and Society (LSTS) Large Research Group
14:20 15.30	Debate and Q&A Session	
15:30	Closing remarks and next steps	• Sergio Carrera, CEPS

ANNEX III – TASK FORCE PARTICIPANTS

María Álvarez
Government Affairs & Public Policy Google Cloud EMEA, Iberia-Privacy Lead

Ralf Bendrath
Adviser on Civil Liberties, Justice and Home Affairs, The Greens, European Parliament

Adam Thomas Bowering
Political Adviser, S&D Group, European Parliament

Joe Cannataci
Former UN Special Rapporteur Right to Privacy and University of Groningen

Arnaud David
AWS Director for European Affairs, Amazon

Emilio De Capitani
Visiting Professor - Department of Law at Queen Mary University of London

Laura Drechsler
Research Fellow, KU Leuven, Research Unit KU Leuven Centre for IT & IP Law (CiTiP)

Gloria Gonzalez Fuster
Research professor, VUB

Zuzanna Gulczynska
Doctoral researcher, University of Ghent

Fanny Hidvegi
Europe Policy and Advocacy Director, Access Now

Lorelien Hoet
CELA, Microsoft

Herwig Hofmann
Professor of European and Transnational Public Law, University of Luxembourg

Chiara Manfredini
EU Policy Associate, AccessNow

Marisa Monteiro Borsboom
DPO and privacy consultant, MQM Legal Center

David Nosak
Political Adviser, E PP G roup, European Parliament

Marc Rotenberg
Executive Director
Center for AI and Digital Policy (CAIDP)

Corrina Schulze
Relations, Digital Government at SAP

Eva Simon
Senior Advocacy Officer
Civil Liberties Union for Europe

Georgia Skouma
Security & Privacy Director, Deloitte Cyber Services

Marco Stefan
Political Adviser, The Greens/EFA Group, European Parliament

Valentin Steinhauer
EU Representative Office Brussels, Deutsche Telekom AG

PRINCIPLES AND GUIDELINES FOR THE TASK FORCE

Task Forces are processes of structured dialogue among national and EU policymakers, industry representatives, practitioners and civil society actors/NGOs, who are brought together over several meetings. Task Force Reports are the final output of the discussions and the research carried out independently by CEPS in the context of the Task Force. Task Forces are organised and implemented in full compliance with the CEPS Integrity Statement.

Participants in a Task Force

- Rapporteurs are CEPS and external researchers/academics who organise and implement the Task Force, conduct the research independently and draft the Final Report.
- Participants can include for-profit entities, membership organisations, NGOs and scholars. This ensures that discussions are balanced and evidence-based, making the modus operandi and final output truly multi-stakeholder. Observers are policymakers or key stakeholders who are invited to attend the Task Force meetings and provide oral and written input.

Objectives of a Task Force report

- Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on the Task Force discussions, available data and literature as well as qualitative research.
- Reports seek to provide readers with a constructive and critical basis for discussion. Conversely, they do not seek to advance a single position or misrepresent the complexity of any subject matter. Task Force reports also fulfil an educational purpose and are therefore drafted in a manner that is easy to understand.

The role of the Task Force participants

- Participants' contributions may take the form of participation in informal debates or formal presentations during the meetings, or a written submission. Participants are given opportunities to provide observations on the Task Force report before it is published, as detailed below.

Drafting of the Final Report and Recommendations

- The Final Report is drafted in accordance with the highest integrity and scientific standards.
- Task Force participants are invited to comment and send their observations on the draft version(s) of the report. Task Force reports feature a set of key findings and conclusions. To draft these conclusions, rapporteurs mainly consider the research findings and consider members' evidence-based views. Task Force reports feature a set of policy recommendations. Task Force participants are not expected to endorse these recommendations.
- The overall content of the report remains the sole responsibility of the rapporteurs, and its content may only be attributed to them and not their own institutions or the Task Force participants.

CEPS
PLACE DU CONGRES 1
B-1000 BRUSSELS