BRIEFING

European Parliament

Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086

SUMMARY

United States (US) Executive Order 14086 and its accompanying regulation are the first building block of the new framework on EU–US data transfer, the 'EU–US Data Privacy Framework'. After the Court of Justice of the European Union declared parts of the predecessor framework invalid, on account of extensive US intelligence powers and insufficient redress mechanisms, data transfers from the EU to the US became subject to serious compliance risks.

The new US framework aims to enhance the level of privacy and data protection for EU data subjects in order to match, in essence, that of the EU and thereby meet EU requirements for data transfers. On 7 October 2022, US President Joe Biden signed an executive order on Enhancing Safeguards for United States Signals Intelligence Activities, mandating restrictions on US signals intelligence activities and establishing a two-tier redress mechanism for qualified foreign complainants. One week later, the US Attorney General amended the Department of Justice regulations to establish the second tier of the redress mechanism, the Data Protection Review Court, as instructed by the executive order.

Views on the new US framework diverge. While industry associations welcome the framework as a means of facilitating trade, digital rights organisations are critical that the level of protection falls short of EU standards. Disparate opinions in the research community reflect stakeholders' contrasting positions. Critics claim that the requirements used to limit signals intelligence activities, such as 'minimisation', 'legitimate objectives', 'necessity' and 'proportionality', are susceptible to liberal interpretation and, in parts, open to secret amendment by the President. They call into question the independence and effectiveness of the redress mechanism owing to its integration with the executive branch and transparency deficits.

To complete the framework and make it operational, the European Commission will determine whether the revised US data protection standards are 'essentially equivalent' to that of the EU, and adopt a draft adequacy decision.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Hendrik Mildebrath
Members' Research Service

PE 739.261 – December 2022

EN

Legal and economic background

According to the EU General Data Protection Regulation (GDPR), businesses may only transfer personal data from the EU/European Economic Area (EEA) to non-EU/EEA countries in compliance with special GDPR transfer mechanisms.[1] According to the prevailing interpretation of the *Schrems II* judgment by the EU Court of Justice (CJEU), operators may only transfer personal data to a non-EU/EEA ('third') country if the third country ensures an '**essentially equivalent**' level of data protection to that of the EU, or if exporters deploy supplementary measures to compensate for the lacunae in protection. In the words of the European Commission, 'when personal data is transferred outside the [EEA], special safeguards are foreseen to ensure that the protection travels with the data'. Operators can rely on the Commission's formal determination that a third country affords EU data an adequate level of protection, i.e. on a Commission implementing decision on data adequacy ('**adequacy decision**'). Particularly where an adequacy decision is absent, operators can avail themselves of the 'appropriate safeguards' under Article 46 GDPR and, where necessary, of 'supplementary measures' or of the 'derogations' under Article 49 GDPR. 'Appropriate safeguards' include alternative transfer instruments such as template contract terms adopted by the Commission (standard contractual clauses, SCCs) approved data protection policies binding every member within a group of undertakings or enterprises (binding corporate rules), codes of conduct, and certification mechanisms. The European Data Protection Supervisor (EDPS) suggests that these rules mitigate the risk of transferring personal data beyond the reach of EU data protection law. US-based companies remain free to collect and process data relating to US-based subjects ('US data') domestically according to US laws.[2]

Where the European Commission recognises, by way of an adequacy decision, that a foreign country's level of data protection is essentially equivalent to that of the EU, economic operators may conveniently share data with entities abroad. Under the former EU–US data transfer framework – the Privacy Shield framework – more than 5 300 US companies, including Microsoft, Facebook, Amazon, Google, IBM, Hewlett-Packard and NVIDIA, were certified and permitted to conveniently transfer data to the US. On 16 July 2020, the CJEU disrupted EU–US personal data transfers by invalidating the Privacy Shield Decision, the keystone of the broader Privacy Shield framework. The CJEU considered that the legal bases of certain US surveillance programmes, Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, do not sufficiently limit the powers conferred on US authorities, and lack actionable rights for EU subjects against US authorities. Consequently, the US failed to provide an essentially equivalent level of data and privacy protection. Contrary to the Commission's adequacy decision, the CJEU found that the Privacy Shield Ombudsperson mechanism does not compensate for a lack of redress mechanisms and the absence of actionable rights, and thereby fails to provide an essentially equivalent level of judicial protection.[3]

Where **no adequacy decision** or superior international agreement is in place, operators would need to reconfigure their operations or use alternative transfer mechanisms in order to comply fully with EU data protection rules. According to the prevailing interpretation of the CJEU judgment, companies availing themselves of alternative instruments would need to compensate, i.e. detect and mitigate, the uncovered US data protection deficits in order to transfer personal data to the US lawfully. Since companies would need to compensate both the (latent) risk of US intelligence agencies making use of their extensive powers and insufficient public redress mechanisms, effective mitigation strategies would entail high costs and legal uncertainty. Additionally, some alternative instruments are inherently costly/cumbersome, (arguably) narrow in scope, or still under development.[4] While companies resort to SCCs as a stopgap and precautionary measure, a robust and reliable adequacy decision presents the commercially preferred option as it provides welcome reassurance. According to a recent survey, privacy professionals rated the compliance with cross-border data transfer laws as their most difficult task, with 10 % of respondents saying their firms chose to localise data, stop transfers, or halt related services altogether.

Since the US and Europe[5] are each other's most important commercial partners for digitally enabled services, disruptions in data flows have major impacts on digital trade. According to the US Bureau of

Economic Analysis (BEA), the US and EU traded potentially ICT-enabled services (including ICT services) worth over US$384 billion in 2019, consisting of US exports worth approximately US$249.35 billion and US imports worth US$134.69 billion. According to one study, the invalidation of the Privacy Shield framework may result in a 5 % to 6 % reduction in imports and exports of digital services, and lead to €19-31 billion (US$22-36 billion) in lost EU economic output annually. Notwithstanding, CJEU Judge Thomas von Danwitz, in a private capacity, emphasised during a debate:

> *The fact that [the EU] level of protection in third countries is not for free, or perhaps cannot be ensured at all, may have economic disadvantages for companies in individual cases; nevertheless, it is the necessary consequence of the fundamental decision taken in European data protection law to ensure a high level of protection of personal data.* [author's translation]

New US framework

Following the July 2020 *Schrems II* decision, the Commission negotiated with the administrations of the former (Donald Trump) and current (Joe Biden) Presidents on next steps to update or replace the Privacy Shield framework. In March 2022, President Joe Biden and European Commission President Ursula von der Leyen announced an agreement in principle, and on 7 October 2022, President Biden issued Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities, implementing the announced agreement. As authorised and directed by the executive order, the US Attorney General amended the Department of Justice regulations to establish a Data Protection Review Court one week after the President released the executive order. According to the Commission, the executive order introduces 'new binding safeguards to address all the points raised by the [CJEU], limiting access to EU data by US intelligence services and establishing a Data Protection Review Court'; the latter is the most difficult point of negotiations.

The new US framework includes **three components**: commercial data protection principles to which US organisations may self-certify, limitations on US signals intelligence activities, and a redress mechanism for complaints against US intelligence activities regarding data transferred to the US.

Commercial data protection principles. As suggested by the March 2022 White House fact sheet, many stakeholders assumed that companies would 'continue to be required to adhere' to the Privacy Shield principles under the new EU–US Data Privacy Framework. While in principle, this will likely remain accurate, US Secretary of Commerce Gina Raimondo announced that the privacy principles would be updated and renamed 'EU–US Data Privacy Framework Principles'. The US Department of Commerce is set to 'work with current Privacy Shield participants, 70 % of which are small and medium enterprises, to facilitate the transition to the updated privacy principles' under the data privacy framework. One expert reports that the Privacy Shield references to the invalid 1995 EU Data Protection Directive will be replaced by references to the EU GDPR, and that this would change the definition of personal data under the commercial principles. The seven privacy principles contained in the Privacy Shield include notice; choice; accountability for onward data transfer; security; data integrity and purpose limitation; access; and recourse, enforcement and liability. The Privacy Shield also sets out 16 mandatory supplemental principles.

Limitations on US signals intelligence activities. The executive order subjects US signals intelligence (SIGINT) activities consistent with the scope of application of Presidential Policy Directive 28 ('PPD-28') to additional safeguards. Like PPD-28, the executive order does not contain a definition of signals intelligence, which begs the question of whether the order will suffer from variations in application and uncertainties in scope like the PPD-28 it largely supersedes.[6] The US Office of the Director of National Intelligence (ODNI) defines signals intelligence as intelligence derived from signal intercepts. It comprises communications intelligence, electronic intelligence, and foreign instrument signals intelligence. The US National Security Agency (NSA) suggests that such intelligence may be derived from communications systems, radars, and weapons systems.

Section 2 of the executive order mandates that signals intelligence may be collected in pursuit of one or more of 12 **legitimate objectives**, and may not be conducted for five **prohibited objectives**. The

President may authorise (secret) updates to the list of legitimate objectives. Signals intelligence activities must be authorised and conducted in line with certain authorisation, necessity, proportionality and oversight '**principles**'. The necessity and proportionality principles stipulate that intelligence activities 'shall be subject to appropriate safeguards … so that … intelligence activities shall be conducted only' if determined to be necessary, and in a way that is proportionate to advance a 'validated intelligence priority'. The determination of necessity is based on a 'reasonable assessment' of all relevant factors.[7] The aim of the proportionality test is to achieve a proper balance between the importance of the 'validated intelligence priority' being advanced and the impact on the privacy and civil liberties of all people. The National Intelligence Priorities Framework containing the 'validated intelligence priorities' is classified; however, according to former ODNI General Counsel Robert Litt, much of it is reflected in the ODNI's unclassified annual Worldwide Threat Assessment.

Subsection (c) lays down **privacy and civil liberties safeguards** that 'shall fulfil' the necessity, proportionately and oversight **principles**. It mandates rules for **(i)** collection of signals intelligence, **(ii)** bulk collection of signals intelligence and its use, **(iii)** handling of personal information collected, and **(iv** and **v)** update, publication and review of certain policies and procedures of the Intelligence Community (composed of 18 organisations). Under the privacy and civil liberties safeguards, signals **intelligence collection** activities must be 'as tailored as feasible' to advance a 'validated intelligence priority', and must 'not disproportionately' impact privacy and civil liberties. The wording of this safeguard is not consistent with the wording of the proportionality principle. In principle, **bulk collection**[8] must only be authorised 'based on a determination' that the information cannot reasonably be obtained by targeted collection. Bulk collection may only be used for six designated objectives (e.g. protecting against terrorism, espionage, cybersecurity threats). The President may facilitate secret updates to the list of objectives. When the Intelligence Community **handles personal information** collected through signals intelligence, it must ensure procedures for minimisation, data security and access, data quality, permissions to perform bulk collection queries, and documentation. Finally, the heads of Intelligence Community organisations are instructed to **update policies and procedures** as necessary to implement the privacy and civil liberties safeguards, and **publish** them within one year of the executive order's issuance. The Privacy and Civil Liberties Oversight Board (PCLOB) is encouraged to **review** the updates. Finally, Section 2(d) reinforces existing oversight mechanisms.

Redress mechanism. Paired, Section 3 of the executive order and the Department of Justice (DOJ) regulation create a two-tier redress system to process 'qualifying complaints'[9] transmitted from 'qualifying states'[10] concerning US signals intelligence activities for any 'covered violation'[11] of US law. Appropriate public authorities from a qualifying state may submit complaints on behalf of individuals (complainants) against US intelligence activities regarding data transferred to the US for adversely affecting the complainant's privacy and civil liberties interests, and violating certain elements of the US legal order (including the executive order itself). For purposes of the redress mechanism, the Attorney General is authorised to designate a foreign country or regional economic integration organisation (REIO) as a qualifying state, if the Attorney General determines that:

a) their laws require appropriate safeguards in the conduct of signals intelligence for US persons'[12] personal information that is transferred from the US to their territories (reciprocity provision);
b) they permit, or are expected to permit, the transfer of personal information for commercial purposes from their territory to the US;
c) the decision would advance US national interests.

The **ODNI's Civil Liberties Protection Officer** (CLPO) serves as the first tier of the redress system. The CLPO is required to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. Once the review is complete, the CLPO must inform the complainant through the appropriate public authority, without confirming or denying that the complainant was subject to US signals intelligence activities. In essence, this amounts to the CLPO stating that 'the review

either did not identify any covered violations or the [CLPO] … issued a determination requiring appropriate remediation'. The executive order promotes the independence of the CLPO from the Director of National Intelligence through non-interference duties and limiting possible reasons for removing the CLPO. It mandates that the Intelligence Community must cooperate with the CLPO and comply with the CLPO's determinations.

The executive order requires the Attorney General to establish the **Data Protection Review Court** ('DPRC' or 'Court') by issuing regulation. The Attorney General issued a regulation establishing the DPRC within the Department of Justice (DOJ) one week after the executive order. According to this framework, the DOJ's Office of Privacy and Civil Liberties (OPCL) provides the Court and the Special Advocates with administrative support. The Attorney General must appoint **at least six judges** to serve as judges on the DPRC for four-year renewable terms subject to certain selection criteria, including expertise and security clearance. Additionally, the Attorney General must appoint **at least two Special Advocates** for two-year renewable terms.

The complainant (through the qualifying state) or an element of the Intelligence Community may seek review of the CLPO's determinations with the DPRC. A three-judge panel will then review the application. A Special Advocate, selected by the DPRC panel, is required to assist the panel, including by advocating regarding the complainant's interests (hybrid function). The Special Advocate does not foster an attorney-client relationship with the complainant. The Special Advocate may submit to the DOJ's Office of Privacy and Civil Liberties written questions for the complainant or the complainant's counsel. The DPRC will conduct its review based on the record of the CLPO's review and any information or submissions provided by the complainant, the Special Advocate, or an element of the Intelligence Community. Its determinations must be guided by relevant US Supreme Court decisions. The DPRC must interpret the executive order 'in light of [US} law and the [US] legal tradition, and not any other source of law'. After the DPRC issues a written decision (majority vote), the DPRC will notify the complainant through the appropriate public authority, without confirming or denying that the complainant was subject to US signals intelligence activities. The wording of the notification corresponds to that of the CLPO under the neither-confirm-nor-deny principle. The executive order promotes the independence of the DPRC from the Attorney General by exempting the DPRC from the Attorney General's day-to-day supervision and limiting possible reasons for removal and other adverse actions against judges. The Intelligence Community must cooperate with the CLPO (acting on the DPRC's request) and comply with the DPRC panel's determinations.

European Parliament position

In its resolution on the *Schrems II* ruling, the Parliament considers that reforms to US surveillance laws are a prerequisite for any new US adequacy decision. Parliament had called for suspending the EU–US Privacy Shield as early as two years prior to the *Schrems II* ruling, in a 2018 resolution.

EU–United Kingdom data transfers

In a May 2021 resolution, the European Parliament objected to the European Commission's United Kingdom (UK) draft adequacy decisions on account of shortcomings in UK data protection standards, finding that the draft act was not consistent with the Commission's implementing powers. Although the Commission subsequently amended its decision, experts see shortcomings remaining. In a February 2020 resolution and a June 2020 recommendation, Parliament had raised concerns about the UK's data protection level. Main findings by Annalisa Tardino (ID, Italy), Head of Delegation, and Gwendoline Delbos-Corfield (Greens/EFA, France) from a recent data protection-themed visit to the UK diverge.

First reactions to the new US framework

Stakeholders

Industry associations such as DigitalEurope and the Information Technology Industry Council (ITIC) welcome the executive order and highlight its economic advantages including business

certainty. Conversely, **digital rights advocacy organisations** such as NOYB, the Electronic Privacy Information Center (EPIC), the Center for Democracy and Technology (CDT) and AccessNow take a critical stance, emphasising deficits in aligning US with EU standards. NOYB criticises that the executive order only follows the letter, not the spirit of EU restrictions on bulk surveillance (divergent understandings of proportionality), and that the redress mechanism fails to meet EU standards of judicial protection, not least because the DPRC is part of the executive branch as opposed to the judicial branch (the '"Court" is not a real Court'). EPIC criticises that the overly broad justifications for surveillance and insufficient restrictions on bulk surveillance do not meet EU data protection standards. Additionally, the executive oversight of the CLPO, staffing conditions and practices relating to DPRC judges, and the complex and secretive redress mechanism raise concerns about a lack of independent and effective redress. Similarly, the CDT questions whether the executive order sufficiently defines limitations and the scope of surveillance to pass the EU proportionality test. It recommends that the Intelligence Community and the PCLOB should publicly clarify procedures and restrictions, and recommend Congress to consider limiting Section 702 FISA. CDT also takes issue with the redress mechanism: (i) the CLPO and DPRC lack the authority to compel cooperation of the Intelligence Community through, for instance, enforceable subpoenas; (ii) the Special Advocate institution may not provide individuals with 'the possibility of being advised, defended and represented' within the meaning of Article 47 of the EU Charter of Fundamental Rights; (iii) the DPRC relies on documentation of the CLPO, which is part of the executive branch, suggesting a lack of independence; and (iv) the individual lacks an explicit avenue of appeal to a federal court. Consequently, CDT recommends modifications that would allow Special Advocates to communicate freely with the complainant, give the DPRC subpoena authority, and provide individuals with the opportunity to appeal DPRC decisions before a federal court.

Supervisory authorities

At time of writing, two German regional data protection authorities had made preliminary assessments.

The Hamburg Data Protection Authority (Hamburg DPA) notes that, at present, the US has not reached an essentially equivalent level of data protection to that of the EU, since the executive order provides for an implementation period of up to one year, and its implementation will require several months. Nevertheless, according to Hamburg DPA, 'reflexive and sweeping criticism' is misplaced, since the US has moved a long way towards the European tradition of fundamental rights. Hamburg DPA considers that an assumption that the US interpretation of 'proportionality' would not meet CJEU standards is speculative. However, Hamburg DPA criticises that it is not clear from the text to what extent the new proportionality requirement applies to bulk surveillance. It also notes that the redress procedures are hardly transparent and comprehensible for complainants.

In an internal assessment, released by a platform facilitating freedom of information requests, the Baden-Württemberg Data Protection Authority (Baden-Württemberg DPA) welcomes the executive order, while identifying shortcomings. It considers that the modifiable and revocable nature of an executive order does not provide sufficient legal certainty. Moreover, the interplay between the executive order and the Cloud Act remains uncertain. Furthermore, the Baden-Württemberg DPA pinpoints discrepancies between EU and US interpretations of 'proportionality', pointing out that the permission of bulk surveillance does not meet CJEU standards. Finally, it criticises that lodging a complaint with the CLPO is subject to the fulfilment of substantial requirements, which may present a means of preventing 'unwelcome' complaints; that the order envisages the DPRC as being part of the executive branch, which runs contrary to judicial independence; and that the neither-confirm-nor-deny principle hampers effective redress.

Research community

Disparate opinions in the **research community** reflect stakeholders' contrasting positions.

Critical views

In their two-part analysis, Elizabeth Goitein and Ashley Gorski acknowledge that the executive order enhances the protection of foreign nationals against unfettered surveillance; at the same time, they determine that the level of protection falls short of EU standards. In the **first part**, Goitein submits that the US framework accommodates extensive bulk surveillance and lacks reliable limitations. The requirements used to limit signals intelligence activities, such as 'minimisation', 'legitimate objectives', 'necessity', and 'proportionality', are susceptible to liberal interpretation and, in part, open to secret amendments by the President. By way of example, the regulation accompanying the executive order binds the DPRC to interpreting the executive order exclusively in light of US law and legal tradition. According to Goitein, this 'gives little confidence' that the necessity and proportionality test 'will be applied in a way that would provide for meaningful checks on US surveillance activities'.[13] Goitein also considers that the proportionality test stipulated in the executive order is inherently flawed owing to its (presumed) 'extremely high level of generality'.

In the **second part**, Gorski identifies shortcomings in the new redress mechanism. She explains, and implies, that federal judicial recourse is obstructed for EU data subjects by multiple layers of secrecy and the prerequisite that a litigant must establish actual 'injuries' (resulting from privacy breaches) to be heard in court ('standing'). Against this backdrop, no civil lawsuit challenging the lawfulness of surveillance under Section 702 FISA or Executive Order 12333 had resulted in a US court opinion addressing the legality of that surveillance. Turning to the new US framework, Gorski raises five main issues. **First**, the independence of both tiers of redress is undermined by their integration with the executive branch. 'The fact-finding will be conducted by an ODNI office, not a court; the [DPRC] judges will be selected by the Attorney General, not a third-party agency outside of the intelligence community; there's no limitation on the President's ability to remove the judges; and the court's decisions can be overruled by the President.' Moreover, the dependence of DPRC judges on the executive for the potential renewal of their four-year terms may lead to biased judgements. **Second**, the categorical confidentiality of findings and evidence at the first redress stage prevents complainants from cognising evidence, and raises doubts about the essential equivalence of the redress process. **Third**, the executive order enables the redress bodies to give generic summary responses neither confirming nor denying surveillance and without disclosing further details on the facts and merits, 'making it impossible for the complainant to bring a meaningfully informed appeal'. **Fourth**, in absence of a timely obligation to inform surveillance targets ex post about surveillance measures ('notification duties'), 'Europeans would rarely have a reason to file a complaint or an appeal in pursuit of a remedy'. **Fifth**, the executive order does not cover US government purchases of (bulk) data. **In conclusion**, the researchers encourage Congress to amend FISA and some aspects of Executive Order 123333. Specifically, they call for interventions that limit the collection and use of signals intelligence more effectively, and for improving the effectiveness of redress procedures, for instance by prescribing timely notification duties. Ashley Gorski et al. already recommended such legislative reforms to the Biden administration back in January 2021. Douwe Korff comes to similar conclusions drawing on CJEU case law and EDPB guidance.

Other noteworthy approaches

Granting EU data subjects standing before a federal court. Peter Swire explored statutory and non-statutory ways to enable EU data subjects' judicial redress before the Foreign Intelligence Surveillance Court (FISC), which is a federal court with judges enjoying lifetime tenure. Similarly, Ian Brown and Douwe Korff recommend granting EU complainants standing before the FISC.

Legislative intervention to strengthen the new framework. Without taking a position on these issues, Eric N. Holmes of the US Congressional Research Service raises legislative interventions as an issue of potential Congressional interest. Congress could bolster the executive order's safeguards by enshrining them in legislation. If the CJEU determines that US surveillance activities do not meet EU standards, despite the new US framework, Congress could use the upcoming expiry of Section 702 of FISA (end of 2023) as an occasion to propose broader reforms to the law.

Favourable views

Conversely, Paul Rosenzweig suspects that the executive order is 'the very best that is feasible within the construct of American statutory and constitutional law'. He adds: 'If that is insufficient, then, candidly, nothing is likely to satisfy the EU's legal demands.'

Théodore Christakis et al. have written extensively on redress mechanisms. In articles pre-dating the executive order, they analysed EU redress requirements, suggesting a non-statutory approach combining an executive order and a DOJ regulation to replace the Privacy Shield framework. In an October 2022 article, Christakis et al. conclude that the second tier **DPRC redress mechanism** 'represents a creative and good-faith effort to meet the relevant EU requirements on "independent" redress, while complying with US law'. Like other researchers, they recognise that EU litigants would face substantial difficulties in establishing the necessary 'standing' to sue *intelligence agencies* over surveillance actions in federal courts. However, they submit that an unsatisfied individual may possibly appeal the decision of an *independent administrative body* (such as the DPRC) before a federal court. As Kenneth Propp indicates, while the executive order does not clearly identify such a path, it does not rule it out, either.

Contrary to critics, Christakis et al. consider that **EU law does not necessarily require judicial avenues of redress *sensu stricto***, and that an independent administrative body with quasi-judicial functions, such as the DPRC, may thus satisfy EU standards. They support their claim with five arguments. **First**, a systematic interpretation suggests that the right to effective remedy under EU law is consistent with the more permissive standard of the European Convention on Human Rights. **Second**, 'essential equivalence' must only be established *in essence*, implying some flexibility on the means for achieving the ends. **Third**, the Advocate General's opinion in *Schrems II* gives the impression that judicial review *sensu stricto* is only required in cases where the redress body itself is not independent. **Fourth**, the EU Fundamental Rights Agency (FRA) notes in its 2017 study that in most [25] EU Member States, non-judicial redress bodies exist, and that they appear 'better' [simpler, cheaper and faster] than judicial ones; FRA found that 'across the EU only in a few cases can decisions of non-judicial bodies be reviewed by a judge'. **Fifth**, these observations are even more relevant when one focuses on international surveillance. Similarly, Christopher Docksey considers that the CJEU signalled in its *Schrems II* judgment that a qualified extrajudicial redress mechanism may satisfy EU requirements for effective remedy; however, he states that it would be prudent to provide for an appeal to a federal judicial court. In their October 2022 article mentioned above, Christakis et al. consider that the DPRC may be seen 'similarly to an independent administrative authority exercising quasi-judicial functions, as with several intelligence oversight/redress bodies in Europe such as France's *Commission nationale de contrôle des techniques de renseignement* (CNCTR) or Germany's G 10 Commission'. Like the redress bodies under the executive order, the CNCTR follows the neither-confirm-nor-deny principle. In this context, the following is worth noting: (i) Member States' legal orders and practices do not, by themselves, determine the standard of essential equivalence; (ii) FRA identified avenues for judicial redress in all Member States; and (iii) complaints to the G 10 Commission and the CNCTR do not exclude judicial redress systematically (see more in the annex to this briefing).

Christakis et al. argue that the new DOJ regulation also sufficiently safeguards the **independence of the DPRC** through appointment, supervision, and removal rules, as well as through its reliable and binding legal nature.[14] The regulation limits the Attorney General's influence on the DPRC by defining selection criteria for judges, exempting the DPRC panel and its judges from day-to-day supervision, and prohibiting the removal of judges prior to the end of their term or unduly influencing or taking any other adverse action against a judge arising from service on the DPRC. They consider that public procedure protects the regulation from arbitrary or sudden changes, and ensures that the DPRC would continue to act independently unless its rules are changed definitively and publicly. The regulation has the binding force of law and ultimately binds the entire executive branch, including the President and the Attorney General.

Moreover, in their article, Christakis et al. consider that the DPRC is equipped with sufficiently **effective investigative and decisional powers**.[15] First, they argue that information access rights for investigators, cooperation duties on the intelligence community, and sanctions mechanisms for defiant personnel would ensure effective investigations. Second, they consider that the explicitly mandated binding effect of DPRC determinations and the (not further examined) oversight procedures ensure decisional powers, which the Ombudsperson lacked.

Unlike Gorski, Christakis et al. claim that a statutory approach, aiming to grant EU data subjects access to US federal courts, would enable only a few people to challenge the surveillance actions of intelligence agencies in courts, owing to the strict 'standing' requirements defined by the US Supreme Court's constitutional jurisprudence. They explain that pragmatic, political and legal difficulties favoured the adoption of an executive act over a statutory approach.

Next steps and outlook

With the US adoption of the executive order, the European Commission can now draft an adequacy decision determining whether the revised US data protection standard is essentially equivalent to that of the EU. As part of the formal adoption procedure, it will then need to obtain a non-binding opinion from the EDPB and approval from the Article 93 Committee, which consists of Member States' representatives ('comitology procedure'). The European Parliament and the Council should receive information on the committee proceedings and can request that the Commission maintain, amend, or withdraw an adequacy decision at any time if they perceive the Commission exceeds its implementing powers under Article 45 GDPR. The Parliament may weigh in with a non-binding resolution at any stage. Although major revisions are unlikely, the Commission can adjust the draft decision in response to input from the EDPB, Parliament, Council and other stakeholders. Historically, the process of adoption has taken four to five months once the Commission finalises its draft.

The Commission has highlighted significant improvements in the new US framework compared with the Privacy Shield. Experts anticipate that the Commission will issue a positive draft adequacy decision, despite possible shortfalls. To facilitate transparency and accountability, it would help to discern EU internal standards by scenarios (scenario-specific EU standards),[16] single out factors that shape EU internal standards,[17] and pinpoint any flexibility arising from the CJEU's 'essential equivalence' standard explicitly.[18]

RELATED EUROPEAN PARLIAMENT RESEARCH PUBLICATIONS

Brown I. and Korff D., Exchanges of Personal Data After the Schrems II Judgment, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, July 2021.

Mildebrath H., EU–UK private-sector data flows after Brexit: Settling on adequacy, EPRS, European Parliament, April 2021.

Mildebrath H., The CJEU judgment in the Schrems II case, EPRS, European Parliament, September 2020.

Monteleone S. and Puccio L., From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules, EPRS, European Parliament, 2017.

Monteleone S. and Puccio L., The Privacy Shield: Update on the state of play of the EU-US data transfer rules, EPRS, European Parliament, 2018.

ENDNOTES

1 The exact scope of application of Chapter V of the GPDR remains controversial. For details, see the public consultation on draft guidelines by the European Data Protection Board (EDPB) on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. For more details on Article 3 GDPR, see the EDPB's guidelines on the territorial scope of the GDPR.

2 e.g. processing of US data by operators established in the US, and US-based processing of US data; possibly even processing of US data abroad as an extension of regulating US-based commercial activities.

3 For more information on *Schrems II* and the relevant US intelligence framework, see Exchanges of Personal Data After the Schrems II Judgment, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, July 2021, and EU Data Transfer Requirements and U.S. Intelligence Laws, Congressional Research Service, 17 March 2021.

[4] See H. Mildebrath, EU–UK private-sector data flows after Brexit: Settling on adequacy, EPRS, European Parliament, April 2021, in particular, comparative table on pp. 12-13.

[5] Including the EU, Norway, Russia, Switzerland, Turkey, the United Kingdom and others.

[6] According to a de-classified 2018 oversight report, the PPD-28 does not define 'signals intelligence activities' and, 'As a result, the application varies across the IC [intelligence community]'. This has also been criticised by researchers. President Obama issued the PPD-28 in the aftermath of the Snowden revelations to limit bulk collection and safeguard individuals' (even non-citizens') personal information. The PPD-28 articulated principles to guide 'why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes'. In its *Schrems II* judgment, the CJEU indicated that the PPD-28 does not sufficiently compensate privacy and data protection deficits in the US intelligence framework to provide for an essentially equivalent standard to that of the EU. The new Executive Order 14086 supersedes PPD-28 and President Biden partially revoked all but two sections of the PPD-28.

[7] Additionally, 'signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority'.

[8] According to Section 4(b), '"bulk collection" means the authorized 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)'.

[9] Defined in Section 4(k). NB: The reference to 'section 4(k)(i)-(iv)' mentioned in Section 4(k)(v) would appear to read 'section 5(k)(i)-(iv)' instead.

[10] Section 3(f) determines the procedure and prerequisites for the designation of a 'qualifying state'.

[11] Defined in Section 4(d).

[12] Defined in Section 4(m) Executive Order 14086 in conjunction with Section 3.5(k) Executive Order 12333.

[13] In its 2017 report on surveillance by intelligence services – Volume II, FRA identified disparate notions of interference in the EU and US legal order (see pp. 34-35). In the US – contrary to the EU – 'an interference is considered to occur [only] when intelligence services use the data, and not when they collect them'. The executive order stipulates limitations on data collection, but mandates that the DPRC must be guided by relevant US Supreme Court decisions.

[14] In an article predating the executive order, they derive EU standards of independence from criticism voiced by EU institutions against the now defunct Privacy Shield redress mechanism. EU requirements consist of: (a) protection of the members of the redress body against dismissal or revocation; (b) protection of redress authorities against external intervention or pressure; (c) impartiality of redress bodies; (d) appropriate distance between redress bodies and the intelligence community preventing conflict of interests but enabling informed oversight.

[15] In an article predating the executive order, they derive EU standards of effective remedial powers from criticism voiced by EU institutions against the 2016 Privacy Shield Ombudsperson mechanism. Any new redress system would need to have two types of powers, i.e. investigative and decisional powers, which the Ombudsperson lacked.

[16] e.g. by distinguishing Member State surveillance of EU data held on EU territory, US surveillance of EU data on US territory and on EU territory, international and domestic surveillance operations, and surveillance operations performed by intelligence agencies and those involving private electronic communications providers (direct and indirect surveillance).

[17] e.g. by considering the relevance of the following factors for determining EU standards: common minimum standards implemented nationally; European Convention on Human Rights standards; EU standards of their own kind.

[18] In the EU, data subjects have varying redress avenues depending on surveillance scenario and Member State. It is worth comparing redress mechanisms and their varying benefits and drawbacks to assess whether they might be *essentially* equivalent.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Annex

EU standard of essential equivalence

The EU data *acquis* and case law determines the necessary standard of essential equivalence. Considering disparate interpretations of the *Schrems II* judgment and several open questions, it is not yet fully settled against which redress standard the new US framework must be measured. In light of Article 53 of the EU Charter of Fundamental Rights (and Member States' submission to the European Convention on Human Rights (ECHR) standards), it may be said that the ECHR and its accompanying jurisprudence define the minimum standard. However, the CJEU may draw on commonly agreed EU rights and values to establish a higher level of protection when determining open questions in future case law.

Commentators have repeatedly illustrated EU double standards by pointing out that Member States' frameworks and practices fall short of CJEU standards, and that Member States do not accord US data the *Schrems II* data protection standard. Strictly speaking, Member States' surveillance frameworks and practices do not present the appropriate benchmark for essential equivalence, and some of these frameworks are themselves subject to judicial proceedings (see example of France below). The analysis by Ian Brown and Douwe Korff referenced above indicates that discrepancies between EU internal and external standards may be less pronounced once Member State laws and practices are brought in line with applicable CJEU and ECHR standards. The *Schrems II* judgment reveals that the difference in treatment is rooted in the EU data *acquis* and the distribution of powers between the EU and its Member State, rather than in political considerations. Section 3(f)(i)(A) of the new Executive Order 14086 now also contains a reciprocity provision, which makes EU data subject's access to the redress mechanism conditional on 'appropriate safeguards in the conduct of signals intelligence activities for [US] persons' personal information that is transferred from the [US] to the territory of the country or a member country of the regional economic integration organization'.

FRA conclusions on judicial redress in Member States

In its 2017 report on surveillance by intelligence services – Volume II, the Fundamental Rights Agency (FRA) stated that 'across the EU, only in a few cases can decisions of non-judicial bodies be reviewed by a judge' (p. 114), and that 'data show that non-judicial oversight mechanisms are more accessible to individuals than judicial remedies as they are simpler, cheaper and faster' (p. 14). The 2017 report does not supersede the findings from the 2015 report on surveillance by intelligence services – Volume I, but rather updates the legal analysis where warranted, mainly focusing on non-judicial oversight (see, in particular, p. 73). In its 2015 report, FRA clarified that 'every Member State gives individuals the possibility to complain about privacy violations via the courts, regardless of whether these have occurred because of targeted or signals intelligence', but that this path is very cumbersome and possibly obstructed (p. 66). 'Once domestic remedies have been exhausted, individuals can bring a case before the ECtHR [European Court of Human Rights], alleging that surveillance measures are violating their human rights' (2017 report, p. 33 and pp. 133-134). While FRA considers that in many Member States the path of judicial redress is more cumbersome than seeking non-judicial remedy, the ECtHR (in the context of discussing supervisory control) highlights that judicial control offers the best guarantees of independence, impartiality and a proper procedure.

Preliminary remarks on redress mechanisms in Germany and France

Germany's and France's legal orders respectively provide people with avenues for judicial redress against decisions of the German G 10 Commission and the French National Commission for the Oversight of Intelligence Techniques (CNCTR). These are not without practical challenges.

In **Germany**, the Article 10 Act provides intelligence agencies with legal bases for **surveillance operations** with a domestic nexus (domestic communications and foreign-domestic/domestic-foreign communications). The Act limits individual judicial redress but does not exclude it. Subject to the conditions outlined in Section 12, intelligence authorities may suspend providing individuals with ex-post notification. If the intelligence authority intends to defer the notification for more than

12 months, it requires the approval of the competent oversight body, the G 10 Commission (consensus necessary). Section 13 excludes judicial redress against targeted surveillance measures and certain strategic surveillance measures for the period prior to the individual being notified. The limitation of judicial redress applies only to one out of the nine types of strategic surveillance available under the Article 10 Act; this type of surveillance has not been documented in publicly available reports covering the 2012 to 2019 period. Where Section 13 does not exclude judicial redress, individuals may file a lawsuit with German administrative courts but will likely face onerous evidentiary standards. Individuals may lodge a complaint with the G 10 Commission even before being notified (which may entail a conflict of interest where notification was deferred). Upon exhausting domestic remedies, individuals may file constitutional complaints with the German Federal Constitutional Court, even in cases where notifications are absent. The Constitutional Court appears to apply a more lenient evidentiary standard (reasonable-likelihood-of-acquisition theory) than the administrative courts.

The German Act on the Federal Intelligence Service (BND Act), as amended following the German Federal Constitutional Court's *BND-judgment*, regulates telecommunications **surveillance of foreigners** in other countries (foreign-foreign traffic). Although the Federal Constitutional Court established the extraterritorial reach of fundamental rights, holding that recourse to the German Supreme Administrative Court remains unaffected, it remains unclear to what extent foreigners surveilled abroad by the German Federal Intelligence Service will be able to obtain judicial protection against intelligence measures before German courts. Sceptics criticise onerous evidentiary standards, and regret that the new BND-Act does not provide foreigners with a right to initiate court-like oversight before the Judicial Control Body of the Independent Control Council (*Unabhängiger Kontrollrat*). Other avenues for complains include the G 10 Commission and the German Federal Commissioner for Data Protection and Freedom of Information (*Unabhängige Datenschutzkontrolle*, *Beanstandungen*) – which may raise questions as to the division of powers and lead to complex coordination processes.

In **France**, individuals who suspect being subject to **domestic surveillance** may file complaints with the French Supreme Administrative Court (the Conseil d'État) after completing a prerequisite administrative appeal to the National Commission for the Oversight of Intelligence Techniques (CNCTR). Conversely, under the **international surveillance** law of November 2015, potential surveillance targets are, in principle, not qualified to file complaints with the Conseil d'État. Instead, only the CNCTR may refer the matter to the Conseil d'État (referral mechanism). International surveillance rules apply to the monitoring of electronic communication emitted or received abroad. Since the 2018 amendment, this may exceptionally include monitoring of communications associated with technical identifiers linked to the French territory, such as a French telephone numbers. As a corollary, individuals may appeal before the Conseil d'État to verify that they were not subject to irregular surveillance of communications linked to the French territory under Article L. 854-2(V) of the Internal Security Code. However, they cannot file an appeal to verify that they were not subject to spot checks (*vérifications ponctuelles*) under Article L. 854-2(IV). In 2018, the CNCTR suggested extending the judicial redress mechanism to all forms of international surveillance. The French Government and Parliament did not follow this suggestion. Moreover, the French Constitutional Council (*Conseil constitutionnel*) confirmed the constitutionality of limited judicial redress regarding international surveillance, and the Conseil d'État in 2018 rejected an appeal by Sophie in 't Veld, MEP (Renew, the Netherlands) on the grounds of this restriction (see a summary). Applicants have raised the issue before the ECtHR. According to the CNCTR, this presents only one of at least 14 complaints before the ECtHR relating to the French surveillance framework.

Furthermore, it is worth noting that the CJEU's *La Quadrature du Net* ruling of October 2020 demonstrated that, despite the national security exemption in Article 4(2) of the Treaty on European Union, EU law applies to French legislation, which empowers security authorities to oblige electronic communications providers to retain personal data. The judgment lays down minimum standards for data retention, including notification duties. The French government has made substantial efforts to push back on the ruling. Lastly, the French Conseil d'État adopted a compromise interpretation, which received significant criticism from commentators such as Arthur Messaud and Noémie Levain and Théodore Christakis for following the judgment's letter, not its spirit.