International Journal of Human Rights Law Review

Volume 2 | Issue 3 Art. 14

2023

THE LEGAL IMPLICATIONS OF EXECUTIVE ORDER 14086 ON DATA PRIVACY IN THE EU

Z. Dimović

Recommended Citation
Z. Dimović, 'The Legal Implications of Executive Order 14086 on Data Privacy in the EU' (2023) 2 IJHRLR 265-285.
Available at www.humanrightlawreview.in/vol-2-issue-3/.

THE LEGAL IMPLICATIONS OF EXECUTIVE ORDER 14086 ON DATA PRIVACY IN THE EU

Z. Dimović[1]

ABSTRACT

The transfer of personal data between the EU and USA has become a highly debated and contentious topic. This can be attributed to significant disparities in data privacy regulations and growing concerns surrounding the potential misuse of personal information by U.S. companies and government agencies. The EU responded to these concerns by enacting the GDPR regulation in 2018, which introduced rigorous regulations to safeguard data privacy. These regulations include the explicit requirement for individuals' consent for the collection and processing of their personal data, as well as granting individuals the right to access and control their data. Moreover, the GDPR imposes restrictions on the transfer of personal data to countries outside the EU that do not offer comparable data protection measures. This provision aims to ensure that personal data is not compromised when transferred to jurisdictions that do not meet the EU's robust data privacy standards. Named legal challenges include concerns about the adequacy of data protection in the USA, especially in light of U.S. surveillance programs and the potential for government access to personal data. The restrictions on the transfer of personal data to countries without comparable data protection measures reflect the EU's commitment to maintaining a high level of data privacy and security. It is essential for governments, organizations, and individuals to navigate these challenges carefully and prioritize the protection of personal data in cross-border data transfers.

KEYWORDS

[1] Ph.D. Candidate in law, University in Maribor, Law Faculty, Slovenia.

Cross-border data transfer, Disparities in data privacy regulation, GDPR implications, Human rights, Personal data transfer.

1. INTRODUCTION

The flow of personal data from the European Union (EU) to the United States of America (USA; U.S.) has been a contentious issue in recent years. This is due to differences in the way data privacy is regulated in the two regions, as well as concerns over the potential misuse of personal data by U.S. companies and government agencies. The EU has long had strict regulations on data privacy, enshrined in the General Data Protection Regulation (GDPR)[2] which came into force back in May 2018. By coming into force, GDPR set a very high bar in privacy protection for individuals within EU member states. These regulations require companies to obtain explicit consent from individuals before collecting and processing their personal data,[3] as well as giving individuals the right to access and control their data. The GDPR also restricts the transfer of personal data to countries outside the EU that do not have similar regulations in place.[4]

The U.S, on the other hand, has a more fragmented approach to data privacy regulation and arguably the most significant difference in U.S. legislation[5] compared to EU is lack of a comprehensive data privacy law that applies to all U.S. companies and cover all types of private data. Those different acts cover different aspects of data privacy, like health data, data collected from children or financial information. There is no overarching federal law regulating data privacy, instead, data privacy is

[2] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, pp. 1-88.
[3] GDPR, Recital 32.
[4] GDPR, Articles 44 through 49.
[5] Halabi, S.F. (2022). Executive authority under the U.S. constitution to enter a pandemic treaty or other international agreement. *Harward international law journal online*, 63/2022, pp 1-23.

governed by a patchwork of state and sector-specific laws. The main federal laws are the Health Insurance Portability and Accountability Act (HIPAA)[6] and the Children's Online Privacy Protection Act (COPPA).[7] HIPAA is held by US department of health and human services and set rules how personal health information may be used or shared, and how to file a complaint if you think your rights were violated. COPPA on the other hand is based on CFR Article 16 of Children's online privacy protection Act of 1998 to which Chapter 91[8] set definitions for children's online privacy protection and furthermore imposes certain requirements on operators of websites or online services directed to children under 13 years of age. Furthermore, there are also two other acts. One is Gramm-Leach-Bliley Act (GLBA)[9] set by Federal Trade commission (FTC) which applies to financial institutions and sets out responsibilities and standards to protect the confidentiality and security of consumer's nonpublic personal information and to safeguard sensitive data, the other is The Federal Information Security Management Act (FISMA),[10] which is federal law requires federal agencies to develop, document, and implement an agency-wide program that provides information security. FISMA 2022[11] is a bipartisan update to FISMA that takes a cutting-edge and strategic approach to ensure federal IT systems can better prepare for and respond to today's cyber challenges that threaten federal information and information systems from unauthorized access, use, and disclosure.

This fragmented approach to data privacy regulation has led to concerns over the adequacy of data privacy protections in the USA, particularly in

[6] https://www.hhs.gov/hipaa/index.html.
[7] https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.
[8] 15 USC 6501.
[9] https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
[10] Public law no: 113-283 (12/18/2014) at https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[11] https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf.

light of high-profile data breaches and revelations about the extent of government surveillance programs. Namely in 2013, former National Security Agency (NSA) contractor Edward Snowden[12] revealed the extent of U.S. government surveillance, including the collection of data from internet and phone companies. This sparked concerns among EU citizens about the safety of their personal data when it is transferred to U.S. companies.

As will be seen, the transfer of personal data from the EU to the U.S. is a multifaceted and contentious matter as can be seen from article, carrying significant ramifications for individuals, businesses, and governments across the Atlantic. The existence of mechanisms like Standard Contractual Clauses (SCCs)[13] which arise from recitals 81 and 109 and with accordance with Article 93(2) of GDPR or Binding Corporate Rules (BCR)[14] arising from Article 46 and Article 47 of GDPR enables data transfers, yet doubts persist regarding the sufficiency of data protection regulations in the U.S. Undoubtedly, this issue is poised to remain a subject of ongoing deliberation and examination in the foreseeable future.

2. The Executive Order's Efforts to Expand Privacy Protections to Non-U.S. Persons: Progress or Inadequate Safeguards?

On July 26, 2000, the European Commission (EC) issued its initial adequacy decision regarding the U.S. data privacy,[15] acknowledging the

[12] He was former computer intelligence consultant and »whistleblower" who leaked highly classified information from NSA into public in 2013. His disclosure revealed numerous global surveillance programs, many run by the NSA and Five Eyes intelligence alliance and by that prompted discussion about individual privacy.

[13] According to the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries and have to be pre-approved by the EC.

[14] Are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. The data protection authority in the EU will approve the BCRs in accordance with the consistency mechanisms set out in Article 63 of GDPR.

[15] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by

sufficiency of the privacy principles under the »US Safe Harbour framework",[16] which certain organizations could adhere to. However, this decision was rendered invalid by the Court of Justice of the European Union (CJEU) in its Schrems I judgment.[17] CJEU declared that legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications and must be regarded as compromising the essence of the fundamental right to respect for private life,[18] as guaranteed by Article 7 of the Charter of Fundamental rights of the European Union (Charter),[19] especially more on Articles 8, 16, 47 and 52 thereof, referring to ruling judgements.[20] Consequently, the »Safe Harbour« privacy principles were superseded by a new framework known as the EU-US Privacy Shield, widely recognized as the "Privacy Shield." Subsequently, on July 12, 2016, the Commission issued a second decision affirming the adequacy of the Privacy Shield's protective measures. This decision granted permission for seamless and unrestricted transfers of personal data to certified companies in the U.S. under the provisions of the Privacy Shield.

However, the CJEU rendered the aforementioned decision invalid in its ruling on Schrems II.[21] The origins of the case lie in activist Maximilian Schrems' appeal to the Irish Data Protection Commissioner to invalidate the SCCs used by Facebook to transfer personal data to its headquarters in the U.S. Schrems argued that both during transit and storage in the US, the personal data could be accessed by U.S. intelligence agencies,

---

the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). OJ L 215. 25. 8. 2000, pp 7-47.

[16] Article 1 of Decision C (2000) 2441.

[17] Judgment of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650.

[18] Paragraph 94.

[19] EU Charter of Fundamental Rights: Charter of Fundamental Rights of the European Union, OJ 2010 C 83/ 389.

[20] Paragraph 39 of CJEU judgements C-293/12 and C-594/12, *Digital Rights Ireland and Others*.

[21] Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, C-311/18, EU:C:2020:559.

potentially violating the GDPR and broader EU laws. The GDPR establishes a primary rule that prohibits transfers of personal data outside the EU and EEA unless adequate safeguards are in place. These safeguards include the EC's adequacy decisions, where the EC evaluates and determines that a country's data protection laws are essentially equivalent to the GDPR following a thorough assessment of its national regulations. Additionally, prior to the »Schrems II« ruling, the mechanisms available for secure transfers outside the EU/EEA included the Privacy Shield, the EU SCC, and BCR (only for intra-group transfers). Article 49 also provides exemptions to the general principle, allowing for derogations when there are specific circumstances or legal grounds justifying the transfer to a country without an adequate level of protection.

The CJEU arrived at this determination after conducting a thorough examination of US surveillance laws, particularly Section 702 of the Foreign Intelligence Surveillance Act (FISA)[22] and Executive Order 12333,[23] alongside the EU-US Privacy Shield decision itself. Based on this review, the CJEU concluded that these U.S. laws do not impose adequate limitations or effective oversight on the access of public authorities to personal data originating from the EU. Additionally, the CJEU determined that the Privacy Shield fails to provide EU individuals with actionable and effective rights before the courts against such public authorities. In particular, the CJEU emphasized that the Privacy Shield Ombudsman is unable to effectively address these shortcomings. Consequently, the CJEU held that the Privacy Shield framework is incompatible with the safeguards and requirements mandated by EU law, citing these reasons as the basis for its decision.

[22] 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871. 1978. Office of Justice Programs.
[23] https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf.

In its assessment, the CJEU emphasized the lack of compatibility between the decision and Article 45(1) of the GDPR, while considering the provisions stated in Articles 7, 8, and 47 of the Charter. The CJEU expressed concerns about the broad access to data granted to U.S. surveillance authorities and identified shortcomings in the oversight mechanism of the Privacy Shield. As a result, the CJEU concluded that these factors did not provide adequate legal protection for EU citizens. Consequently, the U.S. and the EC initiated negotiations to establish a framework that ensures personal data transfers to the U.S. maintain an essentially equivalent level of protection as required by the CJEU »Schrems II« ruling. This effort led to a significant development, with the EC and the U.S. reaching a preliminary agreement for a new EU-US Data Privacy Framework called the Data Privacy Framework (DPF)[24] by the end of March 2022. The DPF represents an updated version of the framework applicable to certified commercial entities involved in processing personal data transferred from the EU. It represents an important milestone in safeguarding data privacy. Considering data protection and privacy issues stated in Schrems II ruling and DPF, President Biden made a noteworthy move by endorsing an Executive Order 14086 (EO)[25] that introduces more stringent constraints on surveillance programs within the U.S. Simultaneously, the order establishes a new mechanism for individuals residing outside the country to seek recourse. This includes, by his opinion, two core components: proportionality[26] in intelligence gathering and the increased role for the U.S. Department of Justice (DOJ) with the Data Protection Review Court (DPRC). New EO include three main components: commercial data protection principles to which U.S. organizations may self-certify, a presidential EO and DOJ regulations. Maybe most important part is that newly specify term of personal data under the commercial principles, which link directly to

[24] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632.
[25] https://ofac.treasury.gov/media/913011/download?inline.
[26] Lindsay, D. (2018). The role of proportionality in accessing Trans-Atlantic flows of personal data. *Cambridge University press*.

GDPR and not to Directive 1995 Data Protection Regulation[27] as it was in the Privacy Shield. Combined together aim to address necessity and proportionality limits[28] on U.S. surveillance programs and insufficient redress rights to challenge unlawful government surveillance. Both the substance and legal structure of these components matter under the CJEU's essential equivalence test.

In terms of content, the EO establishes substantial limitations on surveillance programs by explicitly requiring the adherence to principles of necessity and proportionality. Furthermore, it provides an explanation of what these requirements entail and outlines oversight mechanisms to ensure intelligence agencies comply with the newly defined rules. The order articulates the following in Sec. 2 (a)(i)(A): *signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and (B) 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 authorized, 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.*[29]

These safeguards encompass various aspects, including the scope of signals intelligence collection, its permissible uses and sharing, as well

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, pp. 31-50.
[28] As in Schrems II rulling »[n]either Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary."
[29] Refer to Sec. 2(a)(i)(A).

as the duration for which it can be retained. The EO proceeds to outline 12 specified »legitimate objectives, such as safeguarding personnel within the U.S. or its allies, which signals intelligence activities must align with. Additionally, the order identifies four prohibited objectives, such as impeding or restraining criticism, dissent, or the free expression of ideas or political opinions.[30] The EO paired with DOJ regulations creates two-step redress mechanism, including new DPRC. This system is specifically designed to fulfill the second fundamental requirement of essential equivalence, which was identified by the CJEU as lacking in both the Privacy Shield and the U.S. legal system. CJEU's ruling stated that there is a "gap in judicial protection" concerning interferences with intelligence programs and that neither PPD-28 nor Executive order 12333 provide data subjects with actionable rights in court against U.S. authorities, thereby denying them an effective remedy. The decision further clarifies that the Privacy Shield Ombudsman does not address these shortcomings adequately because it lacks the authority to issue binding decisions on intelligence authorities and lacks independence from the executive branch, as the Ombudsman may be dismissed.

While this EO aims to replace the outdated Privacy Shield initiative, it is doubtful that it will fully meet the legal requirements set by the EU to ensure privacy protection. The current concern revolves around whether this repetitive pattern of dismantling and rebuilding will continue indefinitely or instead act as a foundation for wider multilateral cooperation or even advancements in U.S. federal legislation. The objective would be to establish commercial data protections that are universally binding for individuals, irrespective of their nationality or place of residence, akin to the standards set for their national security counterparts. So there seems to be a progress to make data protection on

[30] Refer to Section 2(b).

trans-Atlantic data flow more concise, but safeguards are yet not adequate to sustain EC or CJEU tests.[31]

3. TRANS-ATLANTIC DATA FLOW PROTECTION AND PRIVACY REDRESS MECHANISMS

There are few Trans-Atlantic data flow protection mechanisms, which guarantees data flow protection between EU and U.S. One of such mechanisms are Standard Contractual Clauses (SCCs), which are pre-approved contracts that set out data protection obligations for companies. SCCs have been used for many years as a way of transferring data to countries outside the EU, and they remain a popular mechanism for transferring data to the U.S. However, there are concerns that SCCs may not offer sufficient protection for personal data in light of the EU Court of Justice ruling. Other safeguard as BCR can be found as per Article 47(1) of GDPR, to which it can have influence either on controller with accordance with Article 79 of GDPR, DPO by Article 37 of GDPR or to processor according to Article 22 of GDPR.

Amidst the prevailing uncertainty, the EC has emphasized the necessity for companies to uphold robust obligations regarding the processing of data transferred from the EU. Therefore, companies should carefully evaluate whether they wish to incorporate the Transatlantic Data Privacy Framework (TADPF)[32] as one of their data transfer solutions. If they opt for TADPF, companies should review and familiarize themselves with the Privacy Shield Principles, upon which the TADPF is based. They should assess their ability to comply with the extensive requirements outlined in the principles, covering aspects such as notice, choice, onward transfers, security, access, recourse, enforcement, and liability. While the specific TADPF compliance requirements are not yet fully defined, it is reasonable

[31] https://www.europarl.europa.eu/factsheets/en/sheet/12/competences-of-the-court-of-justice-of-the-european-union.
[32] McCabe, D. 2022. U.S. and European leaders reach deal on trans-Atlantic data privacy. The New York Times.

to anticipate similarities with those of the Privacy Shield. In the interim until EC adequate final decision is made and until the TADPF is finalized, companies should continue utilizing approved data transfer mechanisms such as BCR or SCCs. It is also advisable to conduct transfer impact assessments (TIAs)[33] as needed. TIAs help identify potential risks to the security of the transferred personal data and determine whether additional security measures are necessary, considering the laws of the importing country. For U.S.-related TIAs, the enhanced checks and balances introduced by EO should be considered as part of a comprehensive risk assessment. Companies intending to rely on the TADPF adequacy decision as a valid transfer mechanism, should it be adopted, will need to be certified by the Department of Commerce under the new Framework. In anticipation of this certification process, companies can take preliminary steps by updating their data maps, inventories, and compiling the necessary policies and procedures that require revisions. Companies with an active Privacy Shield certification may consider renewing it to potentially facilitate the transition to TADPF registration from an administrative perspective. It should be noted that the TADPF may not serve as a long-term solution due to potential administrative and legal challenges in both the EU and the U.S. Nevertheless, companies can presently benefit from the TADPF by utilizing it as a transfer mechanism until its adequacy or legality is determined.

As for Privacy redress mechanisms in conjunction, Section 3 of the EO and the regulation DOJ establish a two-tier system for addressing grievances. This system processes "qualifying complaints" that are transmitted from "qualifying states" concerning U.S. signals intelligence activities that may involve a "covered violation" of U.S. law. Public

[33] A transfer impact assessment clarifies your organization's risks for transferring EU residents' data to countries without adequacy under the GDPR. It is a questionnaire that needs to be completed by either party to the data transfer i.e., data importer or data exporter.

authorities from a qualifying state are authorized to submit complaints on behalf of individuals (complainants) against U.S. intelligence activities that impact the privacy and civil liberties interests of the complainant, particularly regarding data transferred to the U.S. These complaints may allege violations of specific elements of U.S. law, including the executive order itself. To facilitate the redress mechanism, the Attorney General (AG) has the authority to designate a foreign country or regional economic integration organization (REIO) as a qualifying state.

Furthermore, EO establishes a two-tiered redress mechanism for individuals whose personal data may have been collected by intelligence agencies. The first tier consists of a Civil Liberties Protection Officer (CLPO) investigating, reviewing, and, if necessary, ordering remediation for qualifying complaints which are defined as complaints that; a) allege a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the U.S. from a qualifying state; b) include the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to U.S. signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the U.S.; the identities of the U.S. government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures; c) are not frivolous, vexatious, or made in bad faith; d) are brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and e) are transmitted by the appropriate public authority in a qualifying state, after it has verified the

identity of the complainant and that the complaint satisfies the conditions set out above.

But there are few shortcomings in the new redress mechanism. As of first, 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 U.S. court opinion addressing the legality of that surveillance. Also, there are also few other implications. 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 AG, 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 cognizing 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 EO does not cover US government purchases of (bulk) data.

However, U.S. companies can only receive personal data from the EU if thy either join EU-U.S. Privacy Shield program, provide appropriate safeguards (SCC, BCR) or refer to one of the GDPR's derogations as per Article 49 of GDPR.

4. PRINCIPLES OF GDPR VS EXECUTIVE ORDER

The principles of "necessity" and "proportionality" are closely intertwined in both EU law and the Article 8 of the European Convention on Human Rights (ECHR).[34] Article 51 of the Charter states that limitations can only be imposed if they are necessary and genuinely serve objectives of general interest, subject to the principle of proportionality. The European Court of Human Rights (ECtHR)[35] has determined that the term "necessary" includes the concept of proportionality. In other words, a restriction on a Convention Right cannot be considered "necessary in a democratic society" unless it is proportionate to the legitimate aim pursued.[36] The EO seeks to distinguish these concepts and express them in a manner that aligns with U.S. legal traditions, maily as per Privacy act for U.S. citizens.

Although the GDPR in the EU provides a robust framework for protecting personal data, the level of protection can be compromised when transferring or remotely accessing data to and from third countries (countries outside the EU or EEA). This is due to conflicting national laws and international obligations in these third countries that cannot be reconciled with the GDPR, resulting in a lower level of data protection. The U.S., in particular, grants authorities extensive access rights to data, which may require a company to disclose personal data even if it is

[34] Rome, 4. XI. 1950. Accessed on https://www.echr.coe.int/documents/d/echr/convention_eng
[35] https://www.echr.coe.int/
[36] European Court of Human Rights, August 31, 2020, para. 26. Available at https://www.echr.coe.int/documents/guide_art_8_eng.pdf

prohibited under the GDPR. Consequently, the GDPR imposes additional requirements for international data transfers.[37]

The fundamental principles of the GDPR, rooted in the longstanding tradition of protecting human rights within the EU, include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. In comparison to the EO, it is worth noting that the GDPR mandates individuals to give their consent (opt-in) before businesses can collect their data, while there is no such opt-in requirement in the EO or the California Consumer Privacy Act (CCPA),[38] which closely resembles the GDPR in the U.S. To ensure adequate protection in specific countries, the EC evaluates the level of data protection in those countries and issues "adequacy decisions"[39] if the level is deemed equivalent to that within the EU. These decisions simplify the process of transferring personal data to those countries. A list of these third countries can be found, but the U.S. is not included in that list.

The EO enhance to find the principle of "proportionality" by stipulating that signals intelligence activities should only be conducted to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized. The aim is to strike a proper balance between the significance of the validated intelligence priority being pursued and the impact on the privacy and civil liberties of all individuals, irrespective of their nationality or place of residence. This provision emphasizes the importance of achieving a proportionate approach that respects privacy and civil liberties while advancing intelligence priorities as per section 2(a)(ii)(B) of EO.

[37] Art. 44 GDPR et seq.
[38] Assembly Bill No. 375. (2018). Chau, Privacy. California legislative information. Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[39] Art. 45 GDPR.

The term "proportionality" is not explicitly mentioned in U.S. surveillance law, although it holds legal significance in other areas of U.S. law. Within U.S. constitutional law, certain areas incorporate proportionality as a principle or include elements of "structured proportionality review" commonly utilized in foreign constitutional jurisprudence. This review may involve examining "narrow tailoring" or considering "less restrictive alternatives," as seen in the U.S. strict scrutiny analysis.[40] Under strict scrutiny, if a government action pertains to "fundamental rights," it must demonstrate that the action or legislation is "necessary" or "narrowly tailored" to serve a compelling government interest. This concept is familiar to U.S. lawyers.

As can be seen EU main principles in EO was not followed sufficiently which may led to inadequate guarantees of data privacy under EO.

5. IMPLICATIONS FOR DATA TRANSFERS AND COMPLIANCE

Importantly, the EO have two significant shortcomings that could potentially lead to legal conflicts under EU laws.

The executive order subjects US signals intelligence (SIGINT)[41] activities consistent with the scope of application of Presidential Policy Directive 28 (PPD-28)[42] to additional safeguards. Like PPD-28, the EO 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. 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 NSA suggests that such intelligence

[40] Jackson, V.C. (2015). Constitutional Law in an age of Proportionality. *The Yale law journal, pp. 3094-3193.*

[41] https://www.nsa.gov/Signals-Intelligence/Overview/.

[42] https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities.

may be derived from communications systems, radars, and weapons systems.

Section 2 of the EO 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 European Parliamentary Research Service (EPRS)[43] stated that President may authorize (secret) updates to the list of legitimate objectives. Signals intelligence activities must be authorized and conducted in line with certain authorization, 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. 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 (NIPF)[44] containing the validated intelligence priorities is classified; however, much of it is reflected in the ODNI's unclassified annual Worldwide Threat Assessment.[45] 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 organizations). Under the privacy and civil liberties safeguards, signals intelligence collection activities must be »as tailored as feasible" to

[43] https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis.
[44] Intelligence Community Directive 204. 1. 1. 2021.
[45] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

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 must only be authorized 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). When the Intelligence Community handles personal information collected through signals intelligence, it must ensure procedures for minimization, data security and access, data quality, permissions to perform bulk collection queries, and documentation. Finally, the heads of Intelligence Community organizations 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)[46] is encouraged to review the updates. Finally, Section 2(d) reinforces existing oversight mechanisms.

Also, the U.S. has not reached an essentially equivalent level of data protection to that of the EU, since the EO provides for an implementation period of up to one year, and its implementation will require several months. To take into consideration 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[47] remains uncertain. Furthermore, there discrepancies between EU and US interpretations of "proportionality", pointing out that the permission of bulk surveillance does not meet CJEU standards.

The provisions discussed above apply to all types of signals intelligence activity, whether it is »targeted" or »bulk collection." The scope of the »bulk" collection in the context of surveillance programs under EO

[46] https://www.pclob.gov/.
[47] H.R. 4943. 2017-2018. 115th American Congress.

12333, which was authorized by PPD-28, was not delimited in a sufficiently clear and precise manner as already stated.

What is more to add is that redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data and DPRC didn't meet the standards of impartiality or independence under the Charter as the "complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence," and also that there was no route for federal appeal for the data subject.

6. SUMMARY OF KEY FINDINGS AND INSIGHTS

With the U.S. adoption of the EO, the EC can now draft an adequacy decision determining whether the revised U.S. 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,[48] 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 EC maintain, amend, or withdraw an adequacy decision at any time if they perceive the EC exceeds its implementing powers under Article 45 GDPR. To facilitate transparency and accountability, it would help to discern EU internal standards by scenarios (scenario-specific EU standards), single out factors that shape EU internal standards,[49] and pinpoint any flexibility arising from the CJEU's »essential equivalence" standard explicitly.[50] The EO also puts

[48] Mildebrath, H. (2022). Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086. European Parliamentary Research Service. PE 739.261.
[49] 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.
[50] 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

new restrictions on electronic surveillance by U.S. intelligence agencies and gives EU citizens new avenues to file complaints when they believe their personal information has been unlawfully collected by U.S. intelligence agencies. It provides the bases for a new DPF which, if approved, will facilitate data flows between the EU and U.S. and allow for necessary and proportionate collection of signals intelligence to protect U.S. national security interests, while at the same time safeguarding individual privacy interests and civil liberties. Despite the imposition of new limitations on U.S. surveillance programs, the EO still allows for the bulk collection of personal data in many situations.

Furthermore, the purpose limitations contained in the order are expansive and may be subject to revision by the President, which raises concerns about their effectiveness in preventing the misuse of personal data. While the newly established redress mechanism represents an improvement over previous frameworks, it remains uncertain whether it will be sufficiently independent and effective to enable individuals to fully exercise their privacy rights.

What is worth saying is that it will be very interesting to see if EO and DPF may become either Privacy Shield II or Scherms III. Considering historical development and native U.S. patriotism, I would bet on the latter.