TRANSATLANTIC RETAIL INDUSTRY VIEWS ON PRELIMINARY ADEQUACY DECISION OF EUROPEAN COMMISSION REGARDING EU-U.S. DATA PRIVACY FRAMEWORK

On December 12, 2022, EuroCommerce and the National Retail Federation (NRF) welcomed the European Commission's preliminary decision[1] that the EU-U.S. Data Privacy Framework (DPF) provides adequate protections for European citizens required under EU law. We said then that we would provide further analysis ahead of final approval of the adequacy decision in 2023. This paper provides that analysis.

We believe that the DPF represents a clear improvement over the EU-U.S. Privacy Shield program and framework for individuals and businesses. Following more than two years of uncertainty and disruption, it would facilitate responsible transatlantic transfers of personal data. Retailers that operate storefronts in Europe or sell goods online to Europeans need to work under a reliable and legally valid transfer mechanism between the EU and U.S. that allows them to serve their customers in the EU while maintaining the highest data protection standards for all individuals involved.

The preliminary adequacy decision explains why the European Commission believes the DPF and legal steps taken by the U.S. under the Executive Order 14086 signed by President Biden on 7 October 2022, including the accompanying regulations promulgated that date by the U.S. Department of Justice, are adequate to comply with EU data protection law and should be approved.

Since 2016, NRF and EuroCommerce have maintained continuous cooperation on EU data privacy regulations, holding annual joint meetings with EU officials with the goal of developing approaches to safeguard consumers while fostering regulatory certainty for transatlantic retailers. As part of our joint efforts, we have analysed the European Commission's draft adequacy decision and present in this paper our key findings.

Based on the legal analysis provided in the Appendix, EuroCommerce and NRF make the following key findings and recommendations regarding the adequacy decision:

Key findings and recommendations

- We urge relevant institutions on both sides of the Atlantic to swiftly adopt, implement, and apply a framework that ensures legal certainty and provides a durable, long-term mechanism for safeguarding EU-U.S. data flows.

[1] European Commission, Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 13 December 2022, https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

  - The current requirements to implement Standard Contractual Clauses (SCCs) and the EDPB's recommendations on supplementary measures to be taken by businesses before transferring personal data to the U.S., in particular the requirement to assess the U.S. laws, court systems, and legal structure to ensure an adequate level of protection, create high costs and legal uncertainty for retail SMEs operating in the EU, making it difficult to effectively compete.
  - The draft adequacy decision of the European Commission supports the intention to bring closure to these concerns in favor of European individuals who will benefit from improvements as regards necessity and proportionality of government access, as well as redress in this area, in line with the requirements of the Court of Justice.

- By resolving the issues associated with transatlantic data transfers through adoption of the DPF, retailers may benefit their customers by allocating more of their limited resources toward other critical activities to protect the privacy and security of consumers' personal data, such as:
  - fortifying online systems' defenses against cyber-attacks;
  - investing in further advanced training of personnel; and
  - assessing, monitoring, and mitigating privacy and security risks from service providers' processing of retail customer's personal data in the context of rapidly evolving cybersecurity threats.

- EuroCommerce and NRF consider that the DPF would provide adequate protections for EU citizens and improve the framework for retailers operating in the EU, as compared to the previous Privacy Shield framework and alternative transfer tools that led to associated legal uncertainties, for the following reasons that are all further discussed in greater detail in the legal analysis that follows in the Appendix:
  - The DPF introduces concepts of necessity and proportionality with regard to U.S. intelligence-gathering of individual's personal data;
  - The U.S. legal system authorizes the creation of administrative tribunals, like the Data Protection Review Court (DPRC), which is the mechanism adopted to meet the CJEU requirements for a redress mechanism for handling complaints of EU individuals implicating matters of U.S. national security;
  - The DPRC is empowered within the U.S. legal system to be competently comprised of qualified judges to exercise independent authority to issue final and binding decisions directing remedial measures to be undertaken by U.S. intelligence agencies;
  - The DPRC meets the CJEU's requirements of providing adequate and effective redress, including through the establishment of a two-tiered redress mechanism;
  - In light of the decades of collaboration between the EU and U.S. in an effort to establish a legally valid and durable mechanism for

EU-U.S. data transfers, we believe the U.S. is committed to a long-term durable agreement and it is unlikely that the Executive Order or regulations establishing the DPRC will be repealed or modified; and
- The DPF provides more adequate protection for Europeans under EU law than the former Privacy Shield framework.

- Because the entry into force of the European Commission's adequacy decision is conditional upon full implementation of the Executive Order and regulations by all relevant U.S. agencies and availability of the redress mechanism for EU individuals, EuroCommerce and NRF look forward to the adoption of the final adequacy decision, including any modifications the Commission finds necessary to address the views of other EU institutions including the Council, European Parliament, and European Data Protection Board.

The Appendix below provides a detailed legal analysis, particularly with respect to the establishment of the DPRC under U.S. law, that supports the key findings and recommendations of EuroCommerce and NRF that we have summarised in bulleted form above. We encourage all relevant institutions on both sides of the Atlantic to review our analysis and to contact us if they would like to discuss any of the key findings or recommendations of this paper, including the legal analysis provided in the Appendix.

APPENDIX:

LEGAL ANALYSIS OF THE MERITS OF THE EU-U.S. DATA PRIVACY FRAMEWORK

A. The new DPF benefits EU citizens as well as retailers and wholesalers operating in the EU, particularly as compared to the previous Privacy Shield framework and alternative transfer tools.

EU citizens, retailers and wholesalers operating in the EU must have an effective and sound EU-U.S. data transfer framework in place, as this will provide both citizens and organizations with the legal guarantees that privacy rights are respected whenever personal data flows from EU member states to the U.S..

EuroCommerce and NRF believe that the DPF would embody an effective and sound framework for transatlantic data flows and, in particular, we welcome that it will provide:

- Legal certainty, allowing organisations to set out long term strategies embedding current and future data related regulations and initiatives;

- Trust on an aligned view and assessment of local legislation that applies to U.S. data controllers and processors. When relying on the DPF, EU-based retailers and wholesalers will not be required to make Transfer Impact Assessments for data transfers to the U.S., thereby avoiding potentially different interpretations of the associated risks;

- A level playing field among entities to avoid significant competitive disruption to the market. The DPF prevents distortion of international data protection arrangements, whereby data exporters could be required to apply different rules to jurisdictions offering similar levels of data protection;

- Choice of proven solutions, with sufficient knowledgeable supporting resources also available in the EU versus the uncertainty of new entries on the market and their associated risks; and

- Choice between more suppliers, allowing the market competition to play, especially to the benefit of SMEs which are in need of both efficient and affordable solutions to conduct data transfers.

A new adequacy decision would also enable retail organizations to address other important areas of data protection to the benefit of European consumers. For example, retailers would be in a position to provide enhanced privacy protection to

the benefit of their customers by allocating a great portion of their limited resources toward critical activities protecting the privacy and security of personal data, such as:

- fortifying online systems' defenses against cyber-attacks;
- investing in further advanced training of personnel; and
- assessing, monitoring, and mitigating privacy and security risks from service providers' processing of retail customer's personal data in the context of rapidly evolving cybersecurity threats.

By means of an adopted adequacy decision on the DPF, Europe will have more leverage to accomplish changes and improvements in the processing of personal data and data protection, through its regular reviews, than any individual organization. Therefore, the work of the Commission and the U.S. to establish a new DPF that protects the personal data and privacy rights of our customers is of the utmost importance to our sector.

The importance of this agreement, as well as its improvements compared to the EU-U.S. Privacy Shield, have been acknowledged by the European Data Protection Board (EDPB). That said, the EDPB also raised some remaining concerns and requests for further clarification. In addition, during the discussions on a draft resolution in the European Parliament, several points have been raised regarding whether the DPF would meet the standard set by the Court of Justice of the European Union (CJEU) in its *Schrems II* decision.[2] We address these points in the following section.

B. The European Commission's preliminary adequacy decision on the DPF, including its analysis of the redress mechanism, should be supported on its merits because the DPF provides more adequate protections for Europeans under EU law than the former Privacy Shield framework

EuroCommerce and NRF, and our respective member companies, are supportive of the DPF agreement reached by the EU and U.S. and we would like to highlight a number of points which support the European Commission's preliminary decision that this agreement would provide adequate protections for European individuals as required under EU law.

Crucially, from our perspective, ***the DPF addresses the key concerns raised by the CJEU in its decision on Schrems II***. The CJEU found that the limitations to the protection of personal data arising from U.S. domestic law on the access and use by U.S. national security authorities of data transferred from the EU to the U.S. were not essentially equivalent to those under EU law, as regards the ***necessity and proportionality*** of such interferences with the right to data protection. It also found that no cause of action was available which offered an essentially equivalent ***right to an effective remedy***.

[2] *CJEU ruling in Schrems II, 16 July 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155*

The DPF rectifies the deficiencies of the Privacy Shield framework invalidated by the CJEU in *Schrems II* by:

- Providing for binding safeguards that ***limit access to data by U.S. national security authorities*** to what is ***necessary and proportionate*** to protect national security; and
- Establishing an ***independent and impartial redress mechanism***, which includes a new Data Protection Review Court (DPRC), to investigate and resolve complaints regarding access to EU citizens' data by U.S. national security authorities.

In addition, regarding the commercial aspects, the DPF includes updated procedures as regards the administration and oversight of the framework-.

This White Paper will now explore three key reasons why EuroCommerce and NRF are supportive of the European Commission's preliminary adequacy decision.

1. Clear limitations on access to data by U.S. national security authorities

When it comes to U.S. national security authority access to data transferred to the U.S., we share the view of the European Data Protection Board (EDPB) that Executive Order (EO) 14086 contains "*significant improvements*" as compared with the EU-U.S. Privacy Shield.

As highlighted by the EDPB, these improvements include:

- The introduction of "*concepts of* ***necessity and proportionality*** *with regard to U.S. intelligence-gathering of data (signals intelligence)*;"
- Listing the specific purposes for which collection can and cannot take place, including in relation to bulk data collection, requiring authorities to further substantiate those purposes into more concrete intelligence priorities and detailing a procedure for validation of those priorities; and
- The requirement for all U.S. national security authorities to update their policies and procedures to implement EO 14086 by 7 October 2023, to do so in consultation with relevant bodies (in particular the Privacy and Civil Liberties Oversight Board (PCLOB)), and, where possible, to make these policies and procedures public.

Regarding bulk collection, which was not excluded by the Court in *Schrems II*, EO 14086 emphasises that targeted collection should be prioritised over bulk collection and that, when bulk collection is necessary, technical measures should be applied to limit the collection of non-pertinent information.

The EDPB has called for not only the entry into force but also the adoption of the decision to be conditional upon *inter alia* the implementation of EO 14086 by all U.S. national security and intelligence agencies. ***As the draft adequacy decision already makes its entry into force conditional upon full implementation of the EO and regulations by all relevant U.S. agencies and availability of the redress mechanism for EU individuals, EuroCommerce and NRF look forward to the***

***adoption of the final adequacy decision, including any modifications the European Commission finds necessary to address the views of other EU institutions, including the Council, European Parliament, and EDPB*.**

2. Independent and impartial redress mechanism

We share the EDPB's opinion that the redress mechanism contained in the DPF contains "*significant improvements relating to the powers of the Data Protection Review Court ('DPRC') and its enhanced independence compared to the Ombudsperson*" and would agree that the practical functioning of this mechanism should be closely monitored, including to ensure the longevity of the DPF.

In its draft motion for a resolution, the rapporteur of the European Parliament's Civil Liberties (LIBE) Committee criticises the redress mechanism, arguing *inter alia* that the DPRC is "*part of the executive branch and not the judiciary*".

We would like to take a moment to further examine and explain why this redress mechanism is the most certain and reliable method available through U.S. law to meet the CJEU's requirements and how it would give EU individuals a redress mechanism in the U.S..

Before reviewing the key features of the DPRC that meet the CJEU's requirements, we first observe that there are important contextual considerations that the DPF needed to address and then find a workable solution within the U.S. legal system. What is essential to the CJEU is that the DPF redress mechanism enables independent investigations and decisions that have binding authority to redress any identified violation of US law. For example, if data was unlawfully collected, a review court must be able to order the deletion of the data and have the authority to direct U.S. intelligence agencies to do so. We believe the DPRC, as established by the EO and implementing regulations of the U.S. Department of Justice, effectively accomplishes these goals and meets the requirements of the CJEU's *Schrems II* decision.

The following key points highlight in more detail why we believe that this is the case.

a. The Structure of the Two-Tiered Redress Mechanism Established by EO 14086

On 7 October 2022, President Biden's issuance of EO 14086 and the regulations promulgated by the U.S. Department of Justice established a two-tiered review system to fully address valid privacy complaints of EU citizens, establish an initial investigation and decision process, and provide a review court as a second tier to review those decisions, empowering it to issue independent, final and binding orders directing national intelligence agencies to undertake remedial measures when determined by the DPRC they are necessary to provide effective redress to the complainant.

The first tier requires the Civil Liberties Protection Office (CLPO) of the Director of National Intelligence (ODNI) to investigate, review and determine "*whether a covered violation occurred and, where necessary, the appropriate remediation in response to a qualifying complaint*." The second tier requires a three-judge panel of the DPRC to review the determination of the ODNI's CLPO if one is sought by the complainant or an element of the U.S. Intelligence Community.[3]

To provide EU complainants with representation within the DPRC process, the presiding judge on the DPRC panel will select a Special Advocate who, in accordance with the EO 14086, will assist the judicial panel by "*advocating regarding the complainant's interest in the matter and by ensuring that the panel is well informed regarding the issues and the law*." The regulations also permit the complainant to supplement the record "*by any information or submissions*" and empowers the DPRC to "*request that the ODNI CLPO supplement the record in response to specific questions from the panel*."[4]

Lastly, the regulations require the DPRC panel's decision to be by majority vote and for the DPRC to "*issue a written decision setting out its determination and the specifications of any appropriate remediation*."[5]

b. The U.S. legal system authorizes the creation of administrative tribunals by the executive branch, which is the mechanism used to establish the DPRC for handling complaints implicating matters of national security

The DPRC has been established through regulations promulgated by the U.S. Department of Justice under its existing rulemaking authority granted by an act of Congress. The Department of Justice, was directed by the EO to use its existing authority to establish the DPRC as an administrative tribunal within the executive branch by Executive Order 14086 of the President of the United States.

The DPRC has been designed to meet the requirements of the CJEU laid out in the *Schrems II* ruling that invalidated the European Commission's "adequacy decision" for the United States on the then-existing EU-U.S. Privacy Shield framework. The DPRC must be appropriately established and authorized to operate within the U.S. legal system to provide an available redress mechanism for complaints regarding classified national security information, which accounts for the structure described above. For example, DPRC judges and special advocates must have national security clearance to serve in their respective roles given the complaints to be heard regarding EU individuals' rights regarding personal data that is potentially subject to

[3] See Part II of Supplementary Information in U.S. Department of Justice Final Rule on Data Protection Review Court: "Each DPRC panel will review the application before it to determine whether the ODNI CLPO's determination regarding whether a covered violation occurred was legally correct under the applicable law and supported by substantial evidence and whether any appropriate remediation was consistent with the Executive Order of October 7, 2022."
[4] Part II of Supplementary Information in U.S. Department of Justice Final Rule on Data Protection Review Court
[5] Id.

U.S. signals intelligence.[6] The DPRC is also designed to be comprised of qualified judges empowered to exercise independent authority as discussed in further detail below.

c. The DPRC is established by a regulation promulgated by the U.S. Department of Justice, which is empowered to do so by the U.S. Congress under the Administrative Procedure Act of 1946 (APA). The President directed the Attorney General of the Department of Justice, through Executive Order 14086, to use this existing regulatory authority to create the DPRC, which is appropriately and constitutionally empowered within the U.S. legal system and comprised of qualified judges to exercise independent authority to issue final and binding decisions directing remedial measures to be undertaken by U.S. intelligence agencies.

The United States, by the issuance EO 14086 and the implementing regulations promulgated by the U.S. Department of Justice on 7 October 2022, established the independence of qualified judges from outside the government with requisite national security clearance to ensure they were not subject to the supervision of the U.S. Attorney General and had the independent authority to issue final and binding orders directing remedial measures to be undertaken by U.S. intelligence agencies.

The DPRC is empowered under U.S. law to independently exercise the authority granted by Congress and reserved to the Attorney General under 28 U.S.C. 511 and 512 "*to provide advice and opinion on questions of law*." This authority was delegated[7] to the DPRC to be exercised independently from the Attorney General.[8]

Further, the DPRC will be comprised of judges who must hold "requisite security clearances to access classified national security information" and will consist of "*individuals chosen from outside the United States Government, to provide independent and impartial review of applications for review*."[9] The terms of the DRPC

[6] See §201.11(b) of Part 201 of Chapter I of Title 28 of the Code of Federal Regulations establishing the Data Protection Review Court: "Judges may serve on a DPRC panel convened under section §201.7(a) of this part, and Special Advocates may be selected to assist a DPRC panel under §201.8(a) of this part, only if they hold the requisite security clearances to access classified national security information."

[7] The Supreme Court of the United States has recognized the authority of the Attorney General to establish independent bodies with decision-making power, including to adjudicate individual cases, see in particular *U.S. ex. rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) and *U.S. v. Nixon*, 418 U.S. 683, 695 (1974).

[8] See Part I of Supplementary Information in U.S. Department of Justice Final Rule on Data Protection Review Court: "Exercising the Attorney General's authority under 28 U.S.C. 511 and 512 to provide his advice and opinion on questions of law and the authority delegated to the Attorney General under the Executive Order of October 7, 2022, as delegated to the DPRC in this rule by the Attorney General pursuant to 28 U.S.C. 510, the DPRC will review whether the ODNI CLPO's determination regarding the occurrence of a covered violation was legally correct and supported by substantial evidence and whether, in the event of a covered violation, the ODNI CLPO's determination as to the appropriate remediation was consistent with the Executive Order of October 7, 2022."

[9] Part I of Supplementary Information in U.S. Department of Justice Final Rule on Data Protection Review Court

judges are protected as well, with dismissal prior to the expiration of their term of office only possible in narrowly defined circumstances.

Most importantly, the DPRC judges have been granted the *independent* authority to issue remedial measures that are *final* and *binding* on U.S. intelligence agencies, as discussed in the Final Rule of the U.S. Department of Justice establishing the DPRC:

> "*To facilitate their independent and impartial review, DPRC judges will not be subject to the day-to-day supervision of the Attorney General and will be subject to removal protections. DPRC decisions, including the direction of appropriate remedial measures to be undertaken by United States intelligence agencies, will be final and binding*."[10]

As part of their independent authority, it is also important to note that DPRC judges have investigative powers to obtain all the information they need from intelligence agencies, which in turn are obligated to provide such information.

d. Based on this analysis, EuroCommerce and NRF believe the DPRC provides the strongest possible mechanism that can effectively operate within the U.S. legal system to meet the CJEU's Requirements to Provide Adequate and Effective Redress Required by EU Law

The DPRC has been established as an administrative tribunal with all the authority necessary to meet the requirements mandated by the CJEU in its *Schrems II* decision and to provide the strongest possible mechanism that can effectively operate within the U.S. legal system and its traditions.

An important reason that the DPRC was established as an administrative tribunal by a regulation of the Department of Justice, using its existing rulemaking authority granted by Congress, was to ensure that redress could be provided to EU individuals as required by the CJEU. The availability of a redress mechanism cannot be assured under the U.S. legal system in U.S. federal courts (courts within the judicial branch) due to the constitutional requirements for an individual to have *standing* in federal court, which require the complainant to demonstrate an injury in fact, causation (a causal connection between the injury and the challenged action of the defendant), and the injury's likely redressability by the court.[11]

Because of the nature of national security and signals intelligence activities, it is unlikely individual complainants would have sufficient factual information to demonstrate an injury in fact or causation to the extent required to meet the

---

[10] Id.

[11] See *Lujan vs. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). As discussed in this opinion of the U.S. Supreme Court, and pursuant to its precedents on standing, the plaintiff must personally have suffered some actual or threatened injury or harm that can meet strict requirements of being (a) a "concrete and particularized" injury, and (b) an "actual or imminent, not 'conjectural' or 'hypothetical'" injury). Second, there must be a "fairly trace[able]" causal connection between the defendant's actions and the injury or harm suffered by the plaintiff. Third, the injury must be "likely" to be "redressed by a favorable decision."

constitutional requirements for standing in U.S. federal court. To overcome the uncertainty whether the availability of redress required by the CJEU could be met by federal courts established within the U.S. judiciary that are subject to these constitutional requirements for standing, the U.S. established the DPRC as an administrative tribunal within the executive branch to permit EU individuals to bring complaints without first needing to demonstrate injury or harm, or even that their personal data was collected by US intelligence agencies.

As demonstrated by this discussion and the analysis provided in the preceding sections, the DPRC provides the strongest possible mechanism to effectively meet the standards for redress under EU law while respecting the nature of the U.S. legal system.

e. EO 14086 and its Implementing Regulations Establish a Durable Legal Framework under U.S. Law that is Unlikely to be Modified or Repealed

We have taken note of concerns from the EDPB, as well as the discussions in the European Parliament, about the fact that EO 14086 can be amended by the U.S. President, with the former arguing that any changes should "*trigger the adoption of immediately applicable implementing acts suspending, repealing or amending the adequacy decision*" and the latter calling for the draft adequacy decision to include a sunset clause limiting the duration of the agreement to four years.

During a hearing in the European Parliament, EDPB Chair Jelinek acknowledged that "*[a]n Executive Order can be revoked, but also a law can be changed*."[12] Further, the Data Protection Authority of the German state of Hamburg issued an opinion on EO 14086 in November 2022 stating that it was not "second-class law" in the U.S. legal system. The DPA also noted that the criticism about an EO being subject to withdrawal or modification by the U.S. government was also true of parliamentary laws and it pointed out that the European Commission could promptly withdraw its own adequacy decision in reaction to any modification or withdrawal of the EO.[13]

The authority of the U.S. president to issue Executive Orders directing the establishment of government programs is well-established under U.S. law. Like other U.S. law, it is subject to challenge by parties with standing and subject to judicial review in U.S. courts of law established by Congress, including federal courts and the U.S. Supreme Court.

---

[12] See European Parliament Civil Liberties (LIBE) Committee exchange of views on the draft motion for resolution on the EU-U.S. Data Privacy Framework, 1 March 2023.

[13] Opinion of Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit issued 29 November 2022, stating: "Die Rechtsform als Executive Order ist das probate Regelungsinstrument in den USA für extraterritoriale Anordnungen. Es handelt sich nicht um ein Gesetz zweiter Klasse. Sie ist insofern nicht mit der eher schwachen deutschen Verordnung zu vergleichen. Robuste Eingriffe wie Wirtschaftssanktionen und Terrorismusbekämpfung werden seit Jahrzehnten wirksam per Präsidentenanordnung durchgesetzt. Dass sie z.B. nach einem Regierungswechsel zügig zurückgenommen werden kann, ist richtig. Dies gilt für parlamentarische Gesetze jedoch ebenfalls. Die EU wird darauf mit sofortiger Aberkennung des Angemessenheitsstatus reagieren können."

In our review of the EO and its implementing regulations, we considered the decades of collaboration between the EU and U.S. in an effort to establish a legally valid and durable mechanism for EU-U.S. data transfers. Based on this history and other factors discussed below, we believe the U.S. is committed to a long-term durable agreement and it is unlikely the EO or the Department of Justice regulations establishing the DPRC will be repealed or modified if this mechanism is deemed to meet the requirements for an adequacy decision to be issued by the European Commission.

Since the establishment of the original U.S.-EU Safe Harbor Framework that took effect in 2000, the European Commission and U.S. Department of Commerce have worked diligently and negotiated and adopted successive EU-U.S. data transfer frameworks to ensure a consistent, legally sound framework to safeguard EU-to-U.S. cross-border data transfers and subject them to appropriate EU and U.S. privacy protections and enforcement mechanisms to protect individual rights.

After the CJEU invalidation of the Safe Harbor in 2015 (in the first *Schrems* decision), the European Commission and U.S. Department of Justice worked very closely and collaboratively to devise and establish in 2016 the EU-U.S. Privacy Shield framework as a replacement for the invalidated Safe Harbor framework. These institutions also held annual reviews of that framework on both sides of the Atlantic in the years after its adoption to determine if any modifications were necessary until the invalidation of the Commission's adequacy decision for the Privacy Shield framework by the CJEU's *Schrems II* decision in 2020.

Since that time, these EU and U.S. institutions developed and agreed to the EU-U.S. Data Privacy Framework (or DPF) in a good faith effort, consistent with their past two decades of collaborative work together, to adequately address the courts concerns by strengthening the oversight mechanisms in the new cross-border data transfer framework to provide more adequate protections for EU individuals under EU law compared to the previous Privacy Shield framework, as called for by the CJEU.

All of the activities described above reflect a consistent objective on the part of both the EU and U.S. institutions to establish and maintain a legally valid and durable EU-U.S. data transfer framework to safeguard individuals' personal data, and it is notable they have occurred over the course of five U.S. presidential administrations, alternating between Democrat and Republican control of the Executive Branch.[14]

Consistent with their history of cooperation and shared objectives, we believe that the European Union and the United States will continue their long-standing

[14] This remarkably consistent objective from the U.S. has not altered even as control of the White House and federal government, and the control of the U.S. Congress, have alternated between political parties. The commitment of the U.S. has carried through the administrations of President Bill Clinton (Democrat), President George W. Bush (Republican), President Barack Obama (Democrat), President Donald Trump (Republican) and President Joe Biden (Democrat). The actions of the federal government, in particular the Department of Commerce, have also been supported by the U.S. Congress despite its alternating control of one or both of its two chambers during that time by the Democrat and Republican parties.

productive relationship and commitment to safeguarding EU-U.S. data flows by maintaining legally valid data transfer mechanisms. We have seen nearly a quarter-century of consistent support from both sides of the Atlantic to maintain an effective international data transfer framework adopted by the European Commission and U.S. Department of Commerce. This is further evidenced by their nearly continuous efforts since 2015 to re-establish and maintain a viable and legally binding transfer mechanism whenever one was invalidated by the CJEU.

In light of the above factors, we expect the U.S. to maintain the Executive Order and implementing regulations given their fundamental importance and necessity to ensure a durable EU-U.S. framework that is adequate under EU law. Additionally, the historical U.S. commitment over many presidential administrations to maintaining a legal and long-term cross-border data transfer framework with the EU counters concerns raised that U.S. executive orders are capable of being amended and/or repealed, which is the case for any democratic institution that operates under the rule of law established by the representatives of its people and subject to the review of its independent courts of law.

Based on the above analysis of the shared objectives and cooperation between the EU and U.S., as evidenced by EU-U.S. data transfer frameworks adopted since 2000, we believe the U.S. is unlikely to repeal EO 14086 or its implementing regulations. Additionally, as a significant check on any possible amendment or repeal of the EO and its implementing regulations that would undermine the level of protection on which adequacy under EU law was determined, the European Commission has reserved in the DPF its authority to immediately suspend, repeal or amend its adequacy determination.[15]

We urge the relevant institutions on both sides of the Atlantic to also fully consider these factors that provide significant context for assessing the risk of any modification or repeal of the EO or its implementing regulations in ways that may undermine the adequacy decision, or in assessing the strength of the commitment by the U.S. to the requirements of the DPF – risks that, in our view, are fully addressed and mitigated by the counter-veiling factors discussed above.

f. Conclusion: The EO and its implementing regulations established an independent and impartial redress mechanism that provides adequate protections for EU individuals

Our key findings and conclusions discussed in subsections a through e above form the basis of our strong belief that the two-tier redress mechanism, including the DPRC, established by the United States in October 2022 through regulations promulgated by the Department of Justice, is an independent and impartial redress mechanism that is durable, unlikely to be modified or repealed, and meets the

[15] The draft adequacy decision already provides that, "*[o]n duly justified imperative grounds of urgency, for example if EO 14086 or the AG Regulation would be amended in a way that undermines the level of protection described in this Decision, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 93(3) of [the GDPR], immediately applicable implementing acts suspending, repealing or amending this Decision*."

CJEU's requirements by providing adequate protections for EU individuals under EU law.

3. Strengthened administration and oversight

Similar to the EU-U.S. Privacy Shield, companies that self-certify to the DPF will be required to adhere to the DPF Principles. The DPF requires organisations to re-certify their adherence to the Principles on an annual basis.

We greatly appreciate the central focus that continues to be placed on EU individual's rights. In particular, we acknowledge that the following principles are maintained:

- Transparency obligations of DPF organisations vis-à-vis EU-based individuals with the requirement that privacy policies of DPF organisations must disclose a full list of elements, including *inter alia* (i) the participation of the organization in the DPF; (ii) the type of data collected; (iii) the purpose of the processing; (iv) the type or identity of third parties to which personal data may be disclosed and the purposes for doing so; (v) their individual rights; (vi) how to contact the organization; and (vii) available redress avenues;
- The obligation for DPF organisations to minimise processing of personal data to what is necessary to the specific purpose of processing;
- The requirement for DPF organisations to implement security measures which must take into account the risks involved in the processing and the nature of the personal data; and
- The fact that EU-based individuals can request access to their personal data and must obtain from DPF organisations confirmation as of whether the organisation is currently processing personal data of those individuals, obtain the full list of personal data processed by the organisation and information on the purpose and categories of recipients. The rights of rectification, erasure, and objection for processing of personal data for materially different (but compatible) purposes and marketing are also actionable by the EU-based individuals vis-à-vis DPF organisations.

And we highlight the following amendments further improving protection of EU individuals' rights compared to the previous Privacy Shield Framework:

- The clarification that key-coded data can be transferred on the basis of the DPF for research purposes (recital 11 of the draft adequacy decision);
- The additional checks that will be carried out by the U.S. Department of Commerce as part of the (re-)certification process (recital 50);
- The checks that will be carried out by the U.S. Department of Commerce as part of its compliance monitoring and search for false claims (section 2.3.2 and 2.3.3 of the draft decision); and
- The increased focus on future U.S. enforcement action more on compliance with substantive provisions of the DPF (see annex IV to the draft decision).

TRANSATLANTIC RETAIL INDUSTRY VIEWS ON PRELIMINARY ADEQUACY DECISION OF EUROPEAN COMMISSION REGARDING EU-U.S. DATA PRIVACY FRAMEWORK

About EuroCommerce

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading global players such as Carrefour, Ikea, Metro and Tesco, and many small businesses. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates 1 in 7 jobs, providing a varied career for 29 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector. https://www.eurocommerce.eu/

About NRF

The National Retail Federation, the world's largest retail trade association, passionately advocates for the people, brands, policies and ideas that help retail thrive. From its headquarters in Washington, D.C., NRF empowers the industry that powers the U.S. economy. Retail is the nation's largest private-sector employer, contributing $3.9 trillion to annual GDP and supporting one in four U.S. jobs — 52 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies. https://nrf.com/

Contacts

Ilya Bruggeman
Director, Digital, Single Market, and Consumer Policy
EuroCommerce
bruggeman@eurocommerce.eu

Paul Martino
Vice President and Senior Policy Counsel
National Retail Federation
martinop@nrf.com