Doctrine

DATA PROTECTION EU & US – TOWARDS A NEW AGREEMENT ON THE TRANSFER OF EUROPEAN PERSONAL DATA TO THE UNITED STATES

ALEXANDER ALBEN
LECTURER AT LAW, UCLA SCHOOL OF LAW
CHIEF PRIVACY OFFICER, WASHINGTON STATE 2015-19

LAETITIA BRECKPOT
PRINCIPAL, COMPLIANCE4BUSINESS
CERTIFIED COMPLIANCE OFFICER

ALEXANDRE BARTHOLOMEEUSEN
PRINCIPAL, COMPLIANCE4BUSINESS
CERTIFIED COMPLIANCE OFFICER
TEACHING ASSISTANT & PH.D. CANDIDATE
FREE UNIVERSITY OF BRUSSELS

For a long time now, the transfer of data from one continent to another has raised a host of questions. Numerous efforts have already been made to smooth data traffic between Europe and the United States. Recently, however, it seems that a more permanent solution could be found. In other words, the ambition is simple: to ensure that data is processed in a meaningful way according to European standards.

I. INTRODUCTION

On March 25, 2022, the President of the European Commission, Ursula Von der Leyen, and the President of the United States of America, Joe Biden, announced an agreement concerning the transfer of European personal data to the United States.

It follows the invalidation on July 16, 2020, by the Court of Justice of the European Union of Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield,[1] known as the "Privacy Shield" adequacy decision.

Its challenge is to provide a legal basis for transferring the personal data of European citizens to the United States that complies with the requirements of the General Data Protection Regulation.[2]

II. US AND EU CULTURES – DIFFERENCES AND SIMILARITIES

In addition to the economic stakes, the different viewpoints concerning the protection of personal data between the USA and the EU stem from a different approach to the legal concept of the protection of privacy. They shed light on the nature of the dispute.

Clearly, a common conception still prevails: the existence of the individual thought as first and of the State, second, supposed to guarantee the rights considered as fundamental of the first.

Nevertheless, the tension that we observe remains: giving priority to the State makes collective interests prevail against the sacred rights of the individual, whilst giving priority to the individual does not guarantee the defense of their autonomy by the State.

The issue of personal data protection is a case of application since the digitization of the world by new communication technologies requires common standpoints, these being without physical borders: our personal data, once given, are everywhere.

Yet, at present, it is not universally recognized that so-called privacy rights travel with an individual across international borders.

The European Union (hereinafter: "EU") has legislated generally by adopting a regulation that is binding on all EU

1. CJEU, the judgment of 16 July 2020, Schrems II, C-311/18, ECLI:EU:C:2020:559.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

countries (with the intention of binding outside its territory), while the United States has chosen the sectoral approach. (1)

The American and European approaches are therefore very different.

Considered a fundamental right, the right to privacy is enshrined in all international legal texts. It is autonomously recognized based on Article 12 of the Universal Declaration of Human Rights, which states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks", article 17 of the United Nations Covenant on Civil and Political Rights of 19 December 1966, article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 and article 7 of the Charter of Fundamental Rights of the European Union of 7 December 2000.

Although the U.S. Constitution contains no such specific provision, various specific provisions determined by the Supreme Court, particularly in recent years, leave no doubt that all Americans can claim such a right, although this has been somewhat cast into doubt by the recent Dobbs decision, in which the Supreme Court invalidated the long-held recognition of an abortion right.

In continental law, the right to privacy protects the individual not only against physical attacks (inviolability of the home) but also against moral attacks. One thinks mainly, but not necessarily, of the infringements permitted by the media (press, photography, television, new communication technologies, etc.). One thinks here of the offenses of slander or defamation. The notion of private life thus concerns various moral rights such as the right to one's image, the right to one's honor or reputation, and the right not to reveal one's beliefs.

In American law, the legal concept of a "right to privacy" was first proposed by two American lawyers from Boston, Samuel D. Warren and Louis D. Brandéis. In 1890, they proposed in a Harvard Law Review article that a new right be incorporated into the common law to remedy the invasion of privacy caused by the tabloid press. Case law followed in the following decades.

For simplicity, the U.S. has recognized the right to "privacy" in 4 categories of harm:
- physical or other intrusions into the privacy of a person; (This is the 4th Amendment, relating to search and seizure);
- the fact of presenting someone in a different light ("false light privacy");
- revealing private facts in the absence of legitimate public interests;
- the use of the image for commercial purposes.

On the other hand, the American states have adopted legislative tools. For example, the "California Privacy Right", which will come into force on January 1, 2022, or the "VCDPA" of the State of Virginia, as well as three other state laws that go into effect in the near future. These state laws are supposed to work in tandem with specific federal privacy statutes, such as the "Electronic Communications Privacy Act" the "Stored Communication Act" – other major federal laws that protect specific categories of information such as HIPPA (personal health information), FERPA (student educational records), and COPPA (children's online privacy).

Having a right to privacy means in practice the recognition of freedom of privacy. Thus, the sanctity of the home or personal communications could be interpreted as the means to such freedom. The same is true for the three fundamental rights of freedom of movement, freedom of association, and freedom of enterprise.

Indeed, this right, given its purpose, creates a power: the power to object to the disclosure and investigation of privacy.

What remains to be defined is the notion of privacy in law.

The European Court of Human Rights has stated in this regard: "the notion of privacy is a broad notion, not susceptible of an exhaustive definition".

In the first sense, it can at least be said that its violation constitutes unlawful interference with the freedom of privacy. In a second, it is about information whose confidentiality is claimed, the right to personal development, and the right to establish relations with other human beings and the outside world.

In other words, would privacy be significantly different in European and American cultures, even though we are dealing with two political systems of democratic law concerned with individual freedom? If so, do these different conceptions influence our understanding of privacy, particularly with respect to our rights over our personal data?

In the United States, privacy can be violated in three ways. It can be violated by the state – this violation specifically concerns the right to liberty and the right to property. The second violation is by other individuals, press such as "peeping Toms". The third type of violation occurs when the press invades an individual's privacy. These third violations are assuredly perceived differently in Europe than in the United States. For example, Europeans (in general)

were appalled by the revelations of the Starr Report on President Bill Clinton's intimate relationship with Monica Lewinsky. A fourth type of privacy violation occurs when a corporation or other organization breaches a duty of privacy regarding personal information.

The difference is that the constitutional right to freedom of speech (1st Amendment) or freedom of the press can interfere with privacy. It is thus a more civil society-driven conception than a state interference with the privacy of individuals guaranteed by the Bill of Rights. On the other hand, in the absence of a constitutional basis equivalent to those that have prevailed in Europe, the notion of privacy has been identified by jurisprudence as "the right to be left alone".

This case law has been unified by Professor William P. Prosser. The reasoning surprises the continental jurist. The right to privacy is a legal construct based on property rights. Case law has held that the Fourth Amendment is inapplicable. Let us understand that the seizures made within a bank on information concerning a client (*in casu*, the plaintiff) no longer belonged to him. These internal documents were the property of the bank, so banks are not required to protect the privacy of their customers. Henceforth, private information held by a third party is no longer private, which has led to legislative interventions. But we'll come back to that, it was legislation in specific sectors like financial, banking, or medical.

Legally obtained information on a matter of public interest does not give rise to a liability claim. However, where the information is not public, the Ordinary law takes over.

In short, two hypotheses must be distinguished. The information may concern the life of a public person or a private person. A public person is by definition exposed to the public eye, they must accept that their private life is the same as their public life. A private person cannot prevent their private life from being discussed if the facts reported are public. On the other hand, American law contains serious restrictions against state intrusion. It is defined by the jurisprudential construction of the right to privacy.

Katz v. United States, however, demonstrates the flexibility of the concept and the possible dynamics of American jurisprudence when it extends the scope of privacy protection not to a place (the private home) but to the person. The doctrinal and jurisprudential debates in the United States are divided, but the question is well and truly raised: data entrusted to service providers within the meaning of this case law could benefit from the protection of the Fourth Amendment. However, Justice Harlan's test seems less rooted in the Fourth Amendment and more in a flexible notion of both private expectations and public recognition of areas of privacy. In this specific case, the Supreme Court concluded that an individual's "reasonable expectation of privacy" may be violated by the state, if the person's expectation was recognized by society as reasonable, given the prevailing technology of the day.

III. THE TRANSFER OF PERSONAL DATA – THEORETICAL ASPECTS

The transfer of personal data to a third country is governed by Chapter V of the General Data Protection Regulation (GDPR) comprising Articles 44 to 50.

The concept of transferring personal dateto a third country is not defined by the GDPR. Instead, it is defined by the European Data Protection Board ("EDPB") in its guidelines on personal data transfers.[3]

The guidelines define the concept of transfer of personal data as *"The sending or making available of personal data by an original controller or processor (exporter) who, for the given processing activity, is subject to the GDPR in accordance with its Article 3, to another controller or processor (importer) located in a third country, irrespective of whether the latter is subject to the GDPR in accordance with its Article 3."*[4]

The given processing activity is qualified as a transfer of personal data to a third country as soon as 3 criteria are met:

First, the controller or processor must be subject to the GDPR for the relevant processing activity in accordance with Article 3 of the EU Regulation.[5]

Secondly, the processing activity must consist of the disclosure or otherwise making available of personal data from the original controller or processor to another controller, joint controller, or processor.

3. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR of 18 November 2021.
4. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR of 18 November 2021 – point 19.
5. Article 3 of the GDPR provides that:
"1. This Regulation shall apply to the processing of personal data carried out in the course of the activities of an establishment of a controller or processor on the territory of the Union, whether or not the processing takes place in the Union.
2. This Regulation shall apply to the processing of personal data relating to data subjects located within the Union by a controller or processor who is not established in the Union, where the processing activities relate to: (a) the supply of goods or services to such data subjects within the Union, whether or not payment is required from such data subjects; or (b) the monitoring of the conduct of such data subjects, insofar as such conduct takes place within the Union.
3. This Regulation shall apply to the processing of personal data by a controller who is not established in the Union but in a place where the law of a Member State applies under public international law."

Finally, the importer of the personal data must be located in a third country[6] or be an international organization. However, this condition is independent of whether the importer is subject to the GDPR pursuant to Article 3.

The transfer of personal data to a third country can, as a matter of principle, only be carried out in compliance with the relevant articles of the GDPR.[7]

In order to be lawful, the transfer of personal data to a country may be based on an adequacy decision. Indeed, Article 45 of the Regulation provides for the possibility for the European Commission to determine, by way of a decision, the adequacy of the level of protection of personal data provided by a third country or an international organization.

Article 45(2) sets out the criteria to be taken into account by the European Commission in assessing the adequacy of the level of protection of personal data provided by the given third country or international organization.

This decision is, by virtue of § 4 of Article 288 TFEU, binding on all addressees of the latter.[8]

The purpose of negotiating and adopting such an agreement is to establish a legal framework that will ensure a level of protection for the personal data of European citizens equivalent to the level of protection provided by European regulations.

As soon as an equivalent level of protection is provided, the transfer of the above-mentioned data to the third country becomes, therefore, legal.

The adoption of an adequacy decision is not, however, the only mechanism under the GDPR for transferring personal data to a third country.

Indeed, Article 46 of the European Regulation provides that the transfer of personal data to a country is lawful if, in the absence of an adequacy decision adopted by the European Commission, appropriate safeguards are in place.[9]

These appropriate safeguards may correspond to the use of (a) binding corporate rules meeting the requirements of Article 47 of the GDPR; (b) a legally binding and enforceable instrument between public authorities or bodies; (c) standard contractual clauses adopted by the European Commission or by a supervisory authority when approved by the European Commission; (d) a code of conduct approved following Article 40 of the GDPR; or (e) a certification mechanism approved in accordance with Article 42 of the GDPR.

Finally, in the absence of an adequacy decision adopted by the European Commission and appropriate safeguards as set forth above, transferring personal data to a third country remains lawful if based on one of the limited exemptions listed in Article 49 of the GDPR.[10]

In the absence of an adequacy decision, appropriate safeguards, and derogation expressly provided for by the GDPR, the transfer of personal data may only take place if the transfer concerned is necessary for overriding legitimate interests of the controller or processor and provided that the national supervisory authority of the transfer has been informed in advance.[11]

IV. EVOLUTION OF THE AGREEMENTS UNDERPINNING THE TRANSATLANTIC TRANSFER OF PERSONAL DATA

A. The "Safe Harbour" adequacy decision

As mentioned above, the transfer of personal data to a third country, a fortiori the United States, is only compliant with the GDPR when based on one of the mechanisms expressly provided for by the European Regulation.

---

6. The notion of a third country refers to a country not within the European Economic Area.

7. Article 44 of the General Data Protection Regulation.

8. Article 288(4) TFEU: *"A decision shall be binding in its entirety. Where it designates addressees, it shall be binding only upon them."*

9. Article 46 of the General Data Protection Regulation.

10. Article 49 of the GDPR states that *"In the absence of an adequacy decision under Article 45(3) or appropriate safeguards under Article 46, including binding corporate rules, a transfer or set of transfers of personal data to a third country or to an international organization may take place only under one of the following conditions:*
(a) the data subject has given his or her explicit consent to the proposed transfer after having been informed of the risks that the transfer might entail for him or her due to the lack of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise, or defense of legal claims;
(f) the transfer is necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer takes place from a register which, in accordance with Union law or the law of a Member State, is intended to provide information to the public and is open to consultation by the public in general or by any person who can demonstrate a legitimate interest, but only insofar as the conditions laid down for consultation in Union law or the law of the Member State are met within the case in question.

11. In accordance with Article 49, paragraph 2, the transfer of personal data to a third country must not be repetitive and must only affect a limited number of data subjects.

The European Commission has twice adopted adequacy decisions making the transatlantic transfer of personal data lawful.

The first adequacy decision called the "Safe Harbour" decision,[12] was adopted in 2000 to allow the transfer of personal data to the United States in accordance with the requirements of the European data protection framework.[13]

Under the Safe Harbour decision, the lawful transfer of data to the United States could only occur if two cumulative conditions were met. First, U.S. companies wishing to benefit from this type of transfer had to commit to respecting the key principles set out in the annex to the adequacy decision. Second, they had to be subject to the supervision of one of the bodies listed in the annex to the decision. *In practice,* U.S. companies wishing to benefit from the transfer of personal data from Europe had to adhere to and comply with the self-certification system set up by the adequacy decision.[14]

Once these two conditions were met, the U.S. company concerned was deemed to provide an adequate level of protection for personal data, thus allowing the transfer of such data. This system worked well for over a decade, allowing the growth of the Internet and associated e-commerce in the EU, led by many American companies. However, the premise that these companies were providing the same level of privacy protection as mandated in the EU was never really tested until 2015.

The Safe Harbour adequacy decision was invalidated by the Court of Justice of the European Union in its judgment of October 6, 2015, known as the "Schrems" judgment.[15] The Court of Justice found that, although based on national security, the interferences of U.S. security authorities with personal data from Europe are not based on a criterion or criteria that would distinguish their justified or unjustified nature. The Court of Justice found that such a lack of criteria does not ensure adequate protection of personal data from Europe. It seems odd that the "inadequacy" in Schrems rests on the activities of American spy agencies, while the vast majority of the data moving between the U.S. and the EU by American companies is strictly for commercial purposes, such as the operation of social networks or the fulfillment of e-commerce. Nevertheless, the "inadequacy" proclaimed by the Court of Justice invalidated the entire apparatus of cross-continental data transfer. Something was required to replace the Safe Harbour before a major disruption of global commerce occurred.

B. The Privacy Shield adequacy decision

Following the invalidation of the "Safe Harbour" adequacy decision, a new adequacy decision allowing transfers of personal data to the United States was adopted by the European Commission on July 12, 2016[16]. This decision, known as the "Privacy Shield" adequacy decision, is the result of two years of negotiations between the European Commission and the United States Department of Commerce.

It should be noted that the negotiation of a new agreement is not only the result of the invalidation of the "Safe Harbour" decision, as this process was already underway before the Schrems decision of the Court of Justice of the European Union.

Negotiations between the two partners mentioned above began in 2014, even though the first "Safe Harbour" decision was still in effect. However, it already appeared necessary to make improvements[17] to the first decision to ensure effective protection of the personal data of European citizens regarding the transfer and processing of their data in the United States.[18]

The invalidation of the "Safe Harbour" adequacy decision has, therefore, only made it necessary to revise the agreement under the benefit of urgency, with transatlantic data transfers having lost their legal basis, OR else to base them on one of the other mechanisms provided for by the RGPD.

The second adequacy decision is equally based on a self-certification system, the principles of which are detailed and listed in the annex to the decision, and on the same control mechanisms.

The "Privacy Shield" adequacy decision presents notable progress, notably concerning the possibilities of recourse offered to European citizens against American companies

12. Commission Decision 2000/520/EC of July 26, 2000, on the adequacy of the protection provided by the safe harbor principles and related frequently asked questions, issued by the U.S. Department of Commerce.
13. The "Safe Harbour" adequacy decision was then adopted on the basis of 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, a directive that has been repealed by the General Data Protection Regulation.
14. This system allowed the United States to avoid having to modify its regulations.
15. C.J.U.E., October 6, 2015, (Maximilien Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd), No. C-362/14.
16. Commission Implementing Decision (EU) 2016/1250 of July 12, 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Data Protection Shield.
17. Ramirez, E., "Appendix 4: Letter from Ms. Edith Ramirez, Chair of the Federal Trade Commission," July 7, 2016.
18. European Commission, "Commission issues guidance on transatlantic data transfers and calls for a swift definition of a new framework following the Schrems ruling," Press Release IP/15/6015, November 6, 2015.

benefiting from the transfer of their data. The new decision introduces a new system of binding arbitration, but also the possibility to lodge a complaint against companies that transfer their data. Finally, European citizens also have a remedy against public authorities when they believe that the latter have collected their data in an unlawful manner.[19]

In addition, the "Privacy Shield" decision strengthens the safeguards regarding the processing of European data by U.S. security authorities.

However, the "Privacy Shield" adequacy decision did not fare any better than its predecessor, since it was invalidated by the European Court of Justice in its "Schrems II" ruling.[20]

In the aforementioned judgment, the Court of Justice of the European Union ruled on two points, namely, (i) the validity of the European Commission's standard contractual clauses and their use in the event of a transfer of personal data to a third country and (ii) the validity of the "Privacy Shield" adequacy decision.

The Court of Justice analyzed the American legislation concerning access to data of Internet Schrems providers and telecommunications companies by the U.S. security authorities. It concluded that the harm caused by the use of the data by the U.S. security authorities was disproportionate to the requirements of the Charter of Fundamental Rights. Indeed, the Court of Justice ruled that the collection of the data in question did not meet the requirements of proportionality and that the remedies available to European citizens were insufficient.

As such, it decided to invalidate the second adequacy decision providing a legal basis for transatlantic data transfers.

V. WHAT FUTURE FOR PERSONAL DATA TRANSFERS TO THE UNITED STATES

The invalidation of the Safe Harbour adequacy decision in the first instance, and the "Privacy Shield" adequacy decision in the second instance, has created considerable uncertainty as to the lawfulness of the transfer of personal data to the United States regarding to data protection requirements.

Indeed, it is the American legislation on surveillance that is at issue in these decisions, which is intended to apply to all processing of personal data, including data transfers from Europe.

It should also be noted that the other mechanisms provided by the GDPR that allow for the transfer of personal data to a third country, including the use of Business Corporate Rules (BCR) or standard contractual clauses, do not easily allow for the transfer of personal data to the United States.

Although the legality of these mechanisms has not been in court, their use must be accompanied by the implementation of complementary measures in view of the American legislation, which has the effect of diminishing or even eliminating the effectiveness of the protection offered for these mechanisms.

In order for transfers of personal data to the United States to take place, it is then necessary to adopt and implement additional measures to completely prevent access to the data by U.S. security authorities.

A. Newly adopted agreements between the European Commission and the US government – EU-US Data Privacy Framework

In light of the above-mentioned difficulties in preventing transfers of personal data from Europe to the United States, the European Union, and the U.S. government have initiated discussions to find a new solution to end the impossibility of such transfers.

After an agreement in principle was reached on March 25, 2022, between Ursula von der Leyen, President of the European Commission, and President Joe Biden,[21] the latter finally signed an executive order[22] on October 7, 2022, laying the foundations for a new text allowing and regulating transfers of personal data to the United States.

The purpose of the Executive Order and its accompanying regulation is to provide new safeguards to respond favorably to the numerous comments made by the Court of Justice of the European Union in its "Schrems I" and "Schrems II" rulings that invalidated the "Safe Harbour" and "Privacy Shield" adequacy decisions. These new safeguards are intended to limit access to European personal

19. Annex I to Commission Implementing Decision (EU) 2016/1250 of July 12, 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Data Protection Shield.

20. E.U.J. July 16, 2020, (Maximilien Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd), No. C-311/18.

21. United States and European Commission Joint Statement of 25 March 2022 on Trans-Atlantic Data Privacy Framework.

22. Executive Order of the White House of 7 October 2022 on Enhancing Safeguards for United States Signals Intelligence Activities.

data by U.S. security authorities and to create a new body responsible for ensuring the protection of personal data in the context of their transfer to the United States.

As mentioned, these safeguards relate first to the processing of the personal data of European residents by U.S. security authorities. Indeed, the processing of personal data from Europe by the U.S. security authorities is limited to processing that is "necessary" and "proportionate" to the national security objective. The authorities will have to justify and prove that the processing is strictly necessary and proportionate to the objective pursued.

The executive order sets out 12 national security objectives that are assessed as legitimate, and allow the processing of European personal data.[23] These so-called "legitimate" purposes include, among others, protection against terrorism, espionage, or cyber attacks, and the assessment of foreign government capabilities and activities. In addition, the executive order emphasizes the targeted collection of personal data to meet these legitimate purposes. The aim is to limit processing to the personal data necessary to achieve the purpose and to avoid, where possible, the massive collection of personal information.[24]

The decree formally establishes a list of so-called "non-legitimate" purposes that cannot constitute a legal basis for the processing of security authorities. These include the collection of information related to the fight against criticism or freedom of expression, as well as the collection of discriminatory information based on criteria such as gender, ethnic origin, or race. The collection of commercial data to give U.S. companies a competitive advantage is also expressly prohibited.

Second, U.S. supervisors are required to review their policies and procedures to incorporate the new safeguards adopted by Executive Order.[25]

Finally, the new agreement further modifies the remedies available to European citizens regarding the processing of their personal data in the United States, including the establishment of an independent and impartial redress mechanism, through the creation of a Data Protection Review Court (DPRC) to review and resolve complaints regarding access to European citizens' data by U.S. national security authorities.[26]

The new agreement aims to establish a two-tiered redress mechanism.

At the first level, European citizens are offered the possibility of filing a complaint with the "Civil Liberties Protection Officer". This person, appointed within the U.S. security authorities, is then responsible for ensuring that privacy and fundamental rights are respected by the American intelligence agencies.

At the second level, European citizens will have the possibility to appeal the decision of the Civil Liberties Protection Officer before the Data Protection Review Court. The Data Protection Review Court will be composed of members selected from outside the U.S. government. The members will be appointed on the basis of specific qualifications and can only be removed from their position in case of serious reasons. The body in question is therefore completely independent of any instructions from the American government.

The Court may make binding corrective decisions, including the deletion of personal data collected in violation of the safeguards set forth in the Decree.

The Court will be assisted by a specialized lawyer with relevant experience, allowing the interests of the complainant (European citizen) to be represented before the Court. Both parties are duly represented to ensure a fair trial.

In addition to the new redress mechanisms for EU citizens, the Executive Order also establishes a number of principles that U.S. security authorities must follow regarding the processing of personal data. First, the processing of personal data of EU citizens in the course of the activities of these authorities must be authorized by law or other legislative acts and must comply with existing laws and presidential directives.

Second, such data may be processed only after it has been determined that it is necessary to advance a legitimate intelligence priority and only to the extent that it is proportionate.

Finally, the U.S. security authorities are expected to comply with a number of obligations to ensure adequate protection of European personal data, including compliance with limitations on the retention of such personal data. Because this pledge was not honored under the old Safe Harbour regime, doubt remains as to whether this new obligation will hold.

It is also provided that the Office of the Director of National Intelligence (ODNI), as part of its current responsibility to present the National Intelligence Priorities

23. *Ibid.,* section 2 "Signals Intelligence Activities."
24. It should be noted, however, that the massive collection of personal data, although not encouraged, is not formally prohibited by the said executive decree.
25. European Commission, "Questions & Answers: EU-U.S. Data Privacy Framework".
26. Executive Order of the White House of 7 October 2022 on Enhancing Safeguards for United States Signals Intelligence Activities, "Signal Intelligence Redress Mechanisms".

Framework (NIPF) to the President of the United States on a regular basis, must obtain a prior assessment from the Civil Liberties Protection Officer as to whether the processing of European personal data by the US intelligence agencies pursues a legitimate purpose and whether the processing is proportionate.

B. The next steps

Following the adoption of the Executive Order and its accompanying regulation on October 7, 2022, the European Commission has prepared a draft adequacy decision to ensure and regulate transfers of personal data of European citizens to the United States.

The draft adequacy decision, adopted by the European Commission on December 13, 2022[27], was then submitted to the European Data Protection Board ("EDPB") for its opinion, in accordance with the procedure. On February 28, 2023, the EDPB has adopted its opinion on the draft adequacy decision regarding the EU-U.S. Data Privacy Framework.[28]

While it welcomes the improvements made by the draft adequacy decision to the framework for the transfer of personal data, the EDPB still has reservations about both the processing of data for commercial purposes and by public U.S. security authorities.

Regarding the transfer and the processing of personal data for commercial purposes, the EDPB notices that a significant part of the principles remains the same as under the "Privacy Shield". The EDPB thus reiterates its criticism of the lack of clarity regarding key concepts. It also invites the European Commission to specify that the safeguards must be adopted considering possible subsequent data transfers and therefore requires an analysis of the legislation of the third countries envisaged. The EDPB also stresses the importance of clarifying the exemptions from self-adherence to the principles contained in the draft adequacy decision.

Regarding the U.S. processing of personal data by the U.S. security authorities, the EDPB welcomes the introduction of the key notions of necessity and proportionality which will condition the processing of personal data of European citizens by the U.S. security authorities. However, the EDPB raises a lack of transparency regarding the prior authorization of the processing of personal data in bulk and draws attention to the need for clarification.

In summary, while the EDPB welcomes the implementation of improvements to the "Privacy Shield", it remains wary and recommends that the European Commission provide numerous clarifications regarding the processing of personal data of European citizens to ensure the adequacy of the principles applicable to both private and public entities in the U.S. and thus guarantee the sustainability of the EU-US Data Privacy Framework.

The adequacy decision was finally adopted and came into force on July 10, 2023[29]. The Commission has then decided that the United States ensures an adequate level of protection for personal data transferred from the European Union to organizations in the U.S. that are includes in the "Data Privacy Framework List". The list is maintained and made publicly available by the U.S. Department of Commerce.

This means that data transfers to one of the listed organizations can take place without additional measures.

On the contrary, the transfer of personal data to an organization not on the aforementioned list still requires the implementation of additional measures, as provided for by Article 46 of the RGPD[30]. The data controller will then have to adopt transfer tools such as standard contractual clauses or binding corporate rules to legitimate the transfer of personal data to U.S. unlisted organization.

VI. CONLUSION: WHAT FUTURE FOR THIS NEW ADEQUACY DECISION?

In light of the invalidation of the "Privacy Shield" adequacy decision, the purpose of the new agreement was to adopt a durable and reliable legal basis for transatlantic personal data flows while addressing the concerns raised by the European Court of Justice in its "Schrems II" ruling.

The European Union welcomes this new agreement and considers it to be *"an unprecedented commitment by the United States to implement appropriate measures to strengthen privacy and civil liberties protections applicable to the activities of U.S. intelligence agencies"*.[31]

It is indeed worth noting the willingness of the European Commission and the U.S. government to address the con-

27. European Commission, Commission Implementing Decision of 13 December 2022 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

28. European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.

29. Commission implementing decision of 10 July 2023, pursuant to Regulation (EU) 2016/79 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

30. See Recommendations 01/2020 of the European Data Protection Board, adopted on 18 June 2021, on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

31. United States and European Commission Joint Statement of 25 March 2022 on Trans-Atlantic Data Privacy Framework.

cerns raised by the European Court of Justice in its Schrems II ruling. Indeed, the two major issues raised by the Court of Justice concerned (i) the lack of proportionality of the collection of European personal data by American intelligence agencies and (ii) the inadequacy of the remedies available to European citizens.

The new agreement aims to respond to the remarks of the Court of Justice of the European Union by providing for an examination of the necessary and proportionate nature of the collection of European information by U.S. security authorities. It should be recalled that the Executive Order and its accompanying regulation also list the so-called legitimate national security purposes on which the U.S. security authorities may then rely to collect the personal data of European citizens. Similarly, the new framework lists purposes that are inherently non-legitimate, making the collection of European citizens' personal data prohibited.

While the European Commission and the U.S. government welcome the new agreement that will be put in place to allow transatlantic data flows, opposition to the new framework is already being heard.

This is notably the case of the Austrian NGO NOYB ("None Of Your Business"), which claims to protect personal data and whose president, Maximilian Schrems, is behind the complaints that led to the invalidation of the "Safe Harbour" and "Privacy Shield" adequacy decisions. The Austrian NGO has indeed denounced what it describes as a lack of substantial reform on the American side.

In a post published on its website,[32] NOYB explains that, in its view, the contours of the new adequacy decision do not adequately address the issues identified by the Court of Justice of the European Union in the "Schrems II" judgment, both with regard to the introduction of an assessment of the proportionality and necessity of the collection of European information by U.S. security authorities and with regard to the establishment of adequate remedies for European citizens. Moreover, NOYB considers that, despite some efforts, the new adequacy decision remains a rather similar copy of the previous "Privacy Shield" decision.

On the first point, NOYB considers that even if the new agreement is in line with article 52 of the European Charter of Fundamental Rights[33] by implementing the terms "necessary" and "proportionate", they do not specifically refer to the proportionality test mechanism defended by the European Court of Justice. The lack of agreement on the legal meaning of these terms would then allow the massive collection of European personal data by U.S. security authorities to continue.

Regarding the establishment of the Data Protection Review Court, NOYB believes that the new body does not meet the notion of "effective remedies" as provided for in Article 47 of the European Charter of Fundamental Rights.[34] In fact, according to the Austrian NGO, the Data Protection Review Court will be an integral part of the American government and proposes the same alternative as was provided for in the "Privacy Shield" Decision.[35,36]

NOYB goes further, questioning the role of the European institutions, pointing out that *"Instead of upholding the 'rule of law' the Commission simply passes an invalid decision over and over again, despite clear rulings by the CJEU. Despite large outrage after the Snowden disclosures in the EU and repeated calls by the European Parliament to take action, the Commission seems to give the diplomatic relations with the US and business pressure on both sides of the Atlantic priority over the rights of Europeans and the requirements of EU law*[37]*."* In consequence, NOYB has already pointed out the possibility of an appeal against the said adequacy decision.

In addition to the reservations expressed by NOYB, some people are already questioning the coexistence of this new adequacy decision with the positions taken by certain national data protection authorities. In particular, the recent strict stance of the French authorities, the Commission Nationale de l'Informatique et des Libertés (CNIL), has banned the use of Google Analytics on French websites after having judged that the transfer of personal data to the United States was in violation of the GDPR, as Google did not offer adequate guarantees to meet the requirements of the European Regulation.[38]

32. NOYB, "New US Executive Order unlikely to satisfy EU law", available at: https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

33. Article 52.1 of the Charter of Fundamental Rights of the European Union provides that: *"Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essential content of those rights and freedoms. In accordance with the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."*

34. Article 47 of the Charter of Fundamental Rights of the European Union states that: "Everyone whose rights and freedoms guaranteed by Union law are violated has the right to an effective remedy before a court in accordance with the conditions laid down in this article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law [...]."

35. The "Privacy Shield" adequacy decision had then set up a mediation mechanism, called "Ombudsperson mechanism" providing for the intervention of a mediator ensuring mediation between the European citizen and the U.S. security authority in question.

36. U.S. Department of State, "Privacy Shield Ombudsperson", available at: https://www.state.gov/e/privacyshield/ombud/.

37. NOYB, "European Commission gives EU-US transfers third round at CJEU", available at: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

38. Formal notice from the CNIL of February 10, 2022, to stop using Google Analytics available at the following link: https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf.

A. Will the new adequacy decision suffer the same fate as its predecessors?

Given the previous announcements, including by Maximilien Schrems, president of the Austrian NGO NOYB, the future adequacy decision will be the target of several complaints.

The validity of the aforementioned decision concerning the GDPR will most likely be discussed before the Court of Justice of the European Union.

It will then be necessary to wait to determine whether the improvements made by the latter concerning the evaluation of the proportionate and necessary character of the collection of information by the U.S. security authorities as well as the establishment of the Data Protection Review Court meet the expectations of the European Court in terms of respect for fundamental rights.

The differences are profound since they concern the role attributed to the State, the relationship between individuals and the State, the extent of the sphere attributed to the notion of private life, the conception of the importance of an economic market, the role that companies can or should play in it, in fact, the scale of values concerning innovation and therefore economic progress. The very conception of personal privacy rights differs in the EU and other nations, such as the United States. As long as this fundamental difference in perspective prevails, strenuous efforts and difficult negotiations will be required to bridge the gap between the realities of cross-border data transfer and the expectations of citizens on either side of the divide.

However, the common points that constitute the starting point for any discussion are just as numerous. We can note:

- agreement on the principle of privacy;
- agreement that the data collector is subject to various obligations to the user;
- agreement that the collector cannot deceive (in bad faith) the user;
- agreement on the minimal fact that the collector cannot deceive the user by a behavior that is evaluated from the point of view of the behavior of a reasonable collector or that does not correspond to the legitimate-objectifiable expectations of the user;
- substantial and formal agreement in important economic sectors;
- agreement on exceptions due to public authority; But is there a right to state surveillance for reasons of national security?
- agreement on the necessary balance between two freedoms considered essential: privacy and freedom of trade (freedom of enterprise);
- understanding and recognition of common interest (despite the current blockage) of the need for an international legal agreement due to the type of economic activity on the one hand and its expansion beyond borders on the other hand (except latent protectionism, shared conception of free trade);
- the forum of judges: increasingly frequent exchanges between the highest courts of the two states to define the content of essential legal concepts.

While the GDPR is a homogeneous, comprehensive, and mandatory text, much more restrictive than the US federal or state provisions, we have noted that the Americans have themselves legislated in several sectors of vital importance, such as banking, insurance, and health, with special protection for minors, etc.

The GDPR itself contains (many) exceptions to its application in connection with collective security and or to the extent of certain needs deemed necessary by states can easily be agreed upon.

The issue of consent in the form of a prior contract in the GDPR and the lack of such a contract in America for unresolved issues is at first glance intractable. However, without having definitive solutions in this regard, we can identify avenues by looking not at the superficiality of the distinct legal terms but rather at the meaning behind them by establishing a lexicon with common content and meaning of the terms. This common lexicon is usual in the drafting of all international conventions or treaties.

Also, the absence or presence of a contract (in cases where it is not mandatory) divides U.S. jurisprudence.

Secondly, even if the GDPR clearly expresses such a qualification, part of the doctrine in Europe is particularly dubious on this issue considering that the required consent is not consent in the legal sense of the term, since the material and psychological conditions in which the "click-okay-approve" takes place cannot, in the legal sense of the term, be considered as a valid consent.

More generally, it should be borne in mind that the GDPR, in terms of political will and despite the way it is presented, has as its essential common economic (and cultural) objective, equivalent to privacy protection, the circulation of data.

It now seems essential to find an adequate mechanism for transferring personal data to the United States, particularly in view of the recent fine imposed on Meta Platforms Ireland Limited ("Meta IE"). Indeed, Meta IE was issued a 1.2 billon euro fine following an inquiry into its Facebook service, by the Irish Data Protection Authority. This fine,

the largest GDPR fine ever, was imposed for Meta's transfer of personal data to the United States, on the basis of standard contractual clauses since 2020.

Meta IE was then asked to stop transferring data to the United States on the basis of standard contractual clauses and has been ordered to bring its data transfers into compliance with the GDPR.

The Irish authority's decision appears, in Meta IE's view, unjustified since, as things stand, there is no mechanism allowing them to continue transferring personal data to the U.S. in compliance with the GDPR.