EUROPEAN
COMMISSION

Brussels, 29.2.2016
COM(2016) 117 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

## Transatlantic Data Flows: Restoring Trust through Strong Safeguards

## 1. INTRODUCTION: THE ROLE OF PERSONAL DATA EXCHANGES IN THE EU-U.S. RELATIONSHIP

A solid transatlantic partnership between the European Union and the United States is as vital today as it has ever been. We share common values, pursue shared political and economic objectives, and cooperate closely in the fight against common threats to our security. The enduring strength of our relationship is evidenced by the extent of our commercial exchanges and our close cooperation in global affairs.

The transfer and exchange of personal data is an essential component underpinning the close links between the European Union (EU) and the United States (U.S.) in the commercial area as well as in the law enforcement sector. These data exchanges require a high level of data protection and corresponding safeguards.

In June 2013, reports concerning large-scale intelligence collection programmes in the U.S. raised serious concerns at both EU and Member State level about the impact on the fundamental rights of Europeans of large-scale processing of personal data by both public authorities and private companies in the United States.

In response, on 27 November 2013 the Commission issued a Communication on Rebuilding Trust in EU-U.S. Data Flows[1] setting out an action plan to restore trust in data transfers for the benefit of the digital economy, the protection of European individuals' rights, and the broader transatlantic relationship. The Communication set out the following key actions to achieve this objective:

(i) adopting the data protection reform package proposed by the Commission in 2012[2];

(ii) making the Safe Harbour safer on the basis of the 13 recommendations laid out in the Communication on the Safe Harbour[3]; and

(iii) strengthening data protection safeguards for law enforcement cooperation, notably by concluding negotiations on the EU-U.S. Data Protection Umbrella Agreement. The latter also included the objective of obtaining commitments from the U.S. on enforceable

---

1 Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, 27.11.2013 (hereafter "the 2013 Communication" or "the Communication"), available at: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

2 Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012, and Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012, available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

3 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013, pp. 18-19 (hereafter "the Safe Harbour Communication"), available at: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

individual rights, including avenues for obtaining judicial redress, in particular through the enactment of a Judicial Redress Act extending certain rights enshrined in the 1974 U.S. Privacy Act to EU citizens that at the time were only available to U.S. citizens and permanent residents.

These objectives were reaffirmed in the political guidelines[4] of the Juncker Commission: "*Data protection is a fundamental right of particular importance in the digital age. In addition to swiftly finalising the legislative work on common data protection rules within the European Union, we also need to uphold this right in our external relations. In view of recent mass surveillance revelations, close partners such as the United States must convince us that the current safe harbour arrangements really are safe if they want them to continue. The U.S. must also guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil. This will be essential for restoring trust in transatlantic relations.*"

Since then, the Commission has worked to achieve these objectives. The Commission stepped up negotiations on the Umbrella Agreement which was initialled by the parties on 8 September 2015. The inter-institutional discussions on the data protection reform package were intensified, resulting in a political agreement between the Council and the European Parliament on 15 December 2015. As for transatlantic data transfers in the commercial sphere, the Commission began discussions with the U.S. to strengthen the Safe Harbour in January 2014. The invalidation of the Safe Harbour Decision by the Court of Justice in the *Schrems* ruling on 6 October 2015[5] confirmed the need for a renewed framework and provided further guidance on the conditions that the framework should fulfil. Following the ruling, on 6 November 2015 the Commission issued guidance for companies setting out the alternative tools that allow the continued transfer of personal data to the United States[6]. On 2 February 2016, a political agreement was reached on a new framework for transatlantic data flows, the EU-U.S. Privacy Shield[7], to replace the previous arrangement.

These achievements will benefit the transatlantic relationship and should restore Europeans' trust in the digital economy while strengthening their fundamental rights. They will also equip the EU and its Member States with a stronger data protection legal framework that will lead to closer integration of the internal market, in particular the Digital Single Market, as well as enable the EU to step up its efforts to promote and develop international privacy and personal data protection standards.

---

[4] A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change Political Guidelines for the next European Commission.

[5] Judgment of 6 October 2015 in Case C-362/14 Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650.

[6] See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015. See also the Statement of the Article 29 Working Party on the Consequences of the *Schrems* Judgment of 3 February 2016, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[7] See http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en

In parallel, important initiatives were launched that led to significant changes in the U.S. legal order. On 17 January 2014, President Obama announced[8] reforms of U.S. signals intelligence activities which were subsequently laid down in Presidential Policy Directive 28 (PPD-28)[9]. Importantly, these reforms provided for the extension of certain privacy protections to non-Americans as well as a refocussing of data collection away from bulk collection towards an approach that prioritises targeted collection and access. The Commission welcomed those new orientations as an important step in the right direction[10]. This reform process was also instrumental in informing the discussions with the U.S. on the EU-U.S. Privacy Shield. Further changes have been introduced since then. For instance, in June 2015 the U.S. passed the USA Freedom Act[11] which modified certain U.S. surveillance programmes, strengthened judicial oversight and increased public transparency about their use. Finally, on 10 February 2016, the U.S. Congress passed the Judicial Redress Act which was signed into law by President Obama on 24 February 2016.[12]

It is against this background that the present Communication takes stock of how far we have come in realising the objectives formulated in the 2013 Communication. It will also highlight areas where more work is still required to cement and fully restore trust in transatlantic data flows.

## 2. THE EU DATA PROTECTION REFORM

### 2.1 The context

In order to seize the opportunities and address the challenges of an increasingly digital inter-connected world, the European Commission put forward its Data Protection Reform package ("the reform") in January 2012. By strengthening EU-internal rules and by providing individuals with more control over their personal data, the reform aims at fostering trust in the digital economy whether personal data is processed within one Member State, in the EU or in third countries, such as United States.

The reform package comprises two legal instruments, a General Data Protection Regulation[13] ("the Regulation") setting out a common EU framework for data protection, and a Data Protection Directive in the area of police and judicial cooperation ("the Police Directive")[14]. By proposing a regulation that will be directly applicable in the Member States, the Commission's aim was to establish one common data protection standard for all, thereby eliminating differences in the level of protection amongst Member States. Likewise, the Police Directive will for the first time lay down a common set of rules at EU level, while

[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm
[11] USA FREEDOM Act of 2015, Pub. L., No. 114-23, § 401, 129 Stat. 268.
[12] H.R.1428 - Judicial Redress Act of 2015. It will enter into force 90 days after enactment.
[13] COM(2012) 11 final, 25.1.2012: see footnote 2.
[14] COM(2012) 10 final, 25.1.2012: see footnote 2.

taking account of the specificities of the judicial and law enforcement traditions in the Member States.

On 15 December 2015 the European Parliament and the Council reached a political agreement on the reform package, thereby fulfilling one of the key actions set out in the 2013 Communication.

## 2.2 What has changed?

The Regulation updates, modernises and in some cases strengthens the data protection principles enshrined in the 1995 Data Protection Directive[15] to guarantee privacy rights. It focuses on reinforcing individuals' rights, deepening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The rules are designed to make sure that EU individuals' personal data are protected – no matter where they are sent, processed or stored – even outside the EU, as may often be the case in the digital world. A number of features in the reform are particularly relevant to highlight.

First, **territorial scope:** the Regulation makes clear that it also applies to companies established in a third country if they are offering goods and services, or monitoring the behaviour of individuals, in the EU. Companies based outside of the EU will have to apply the same rules as companies based in the EU. This ensures the comprehensive protection of EU individuals' rights. It also creates a level-playing field between EU and foreign companies, thereby avoiding competitive imbalances between EU and foreign companies when operating in the EU or targeting consumers in the EU.

Second, **stronger enforcement** of data protection rules: the Regulation provides for an effective sanctions regime by harmonising the powers of national data protection supervisory authorities (DPAs). They will be empowered to impose fines reaching up to EUR 20 million or up to 4% of the total worldwide annual turnover of a company. This power to impose dissuasive sanctions for non-compliance with the data protection rules in conjunction with the territorial scope mentioned above will ensure that companies doing business in the EU will have every incentive to comply with EU law. The new rules also introduce a clearer and stricter liability regime for controllers and processors.

Third, **harmonised rules for law enforcement cooperation:** the Police Directive will apply general data protection principles and rules to the processing of personal data by police and judicial authorities in the Member States for criminal law enforcement matters. This includes harmonised rules for international transfers of personal data in the context of criminal law enforcement cooperation[16]. The new Directive will raise the level of protection for individuals

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.95, p. 31 ("the Data Protection Directive").

[16] Unlike under the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which only covers cross-border exchanges of data between Member States' competent authorities, the application of such rules under the Police Directive will no longer depend on whether those data have previously been exchanged between the criminal law enforcement authorities of the Member States.

while ensuring that the data of victims, witnesses, and suspects of crimes are duly protected in the context of a criminal investigation or a law enforcement action. Supervision is ensured by independent national data protection authorities and individuals must be afforded effective judicial remedies. At the same time, more harmonised laws will enable the police and judicial authorities to cooperate more effectively, amongst Member States as well as between Member States and their international partners, to combat crime and terrorism more effectively. This is a crucial part of the European Agenda on Security.[17]

Fourth, **strong rules for safer international transfers**: both the Regulation and the Police Directive provide transparent, detailed and comprehensive rules for personal data transfers to third countries. They cover all forms of international transfers, be they for commercial or law enforcement purposes, between private parties or public authorities, or between private entities and public authorities. While the architecture of the rules on international transfers remains essentially the same as under the current Data Protection Directive (i.e., adequacy decisions, standard contractual clauses and binding corporate rules, as well as certain derogations from the general prohibition to transfer personal data outside the EU), the reform clarifies and simplifies those rules in a number of ways while reducing red tape. It also introduces some new tools for international transfers.

The Regulation furthermore strengthens the **powers of EU data protection authorities**, including with respect to international transfers. Compared to the current Data Protection Directive, the provisions on the independence, functions and powers of EU DPAs are spelled out in more detail and substantially enhanced. This expressly includes the power to suspend data flows to a recipient in a third country or to an international organisation. The Police Directive contains similar provisions with regard to international transfers and the powers of DPAs over the law enforcement sector.

More specifically, as regards the rules on Commission **adequacy decisions**, the Regulation provides for a precise and detailed catalogue of elements that the Commission must take into account when assessing the level of data protection provided in the legal order of a third country. This process consists of a comprehensive assessment that the Commission must undertake and which should cover – an element that is also in line with the *Schrems* ruling – rules governing the access by the public authorities of a third country to personal data. Another crucial feature of this assessment is that individuals are provided with effective and enforceable data protection rights and may obtain effective administrative and judicial redress.

Furthermore, the Regulation expressly requires the Commission to **periodically review**, at least every four years, all of its adequacy decisions in order to keep abreast of all relevant developments in a third country that may have a direct, or indeed adverse, impact on the level of protection in its legal order. This continuous monitoring of adequacy will be a more

[17] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM(2015) 185 final, 28.4.2015.

dynamic process as it will also entail a dialogue with the authorities of the third country in question.

As regards transfers to third countries for which there is no adequacy decision, the Regulation provides the conditions governing the use of **alternative transfer tools** such as standard contractual clauses and binding corporate rules. It also adds other instruments for transfers, such as approved codes of conduct and approved certification mechanisms. Finally, it clarifies the situation when **derogations** can be used.

### 2.3 The way forward

The data protection reform is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. Consumer trust in EU and third country operators will fuel and thus benefit the European and global digital economy. It will impact positively on our commercial relations with the U.S., our biggest trading partner. It will bring clarity and a stable environment for EU and foreign businesses to operate in. For their part, U.S. businesses will benefit from the legal certainty that comes from doing business with an integrated economic area that applies a uniform set of data protection rules.

Common rules in the law enforcement sector will ensure that individuals' data are better protected and that they are entitled to effective judicial remedies. Facilitating cross-border cooperation amongst police and judicial authorities in the Member States will increase the efficiency of criminal law enforcement and thus create conditions for more effective crime prevention in the EU. At the same time this will enable smoother cooperation with their counterparts in third countries.

The formal adoption of the reform package by the European Parliament and Council is expected to take place during the first semester of 2016. The Regulation will apply two years after adoption while the Police Directive provides for a two-year implementation period. The two-year transition period should be used by all concerned stakeholders both inside and outside the EU to prepare for the new rules. The Commission will play its part. During this transition period, the Commission will work closely with Member States, DPAs and other interested parties to ensure a uniform application of the rules and promote a compliance-ready environment.

## 3. THE EU-U.S. PRIVACY SHIELD: A NEW TRANSATLANTIC FRAMEWORK FOR PERSONAL DATA FLOWS

### 3.1 The context

In order to facilitate personal data flows between the EU and the U.S. for commercial exchanges while ensuring the protection of those data, the Commission had, back in 2000, recognised the Safe Harbour framework as providing an adequate level of protection[18]. As a

[18] Commission Decision 2000/520/EC of 20 July 2000. In this decision, based on Article 25(6) of the Data Protection Directive, the Commission had recognised the Safe Harbour Privacy Principles and accompanying

result, despite the absence of a general data protection law in the U.S., personal data could be freely transferred from EU Member States to companies in the U.S. that had signed up to the privacy principles underpinning the framework.

In the 2013 Safe Harbour Communication[19], the Commission pointed to a number of weaknesses in the functioning of the arrangement over time, notably a lack of transparency by companies concerning their adherence to the scheme and a lack of effective enforcement by U.S. authorities of those companies' compliance with the scheme's privacy principles. Moreover, the surveillance revelations earlier that year raised concerns as regards the scale and scope of certain U.S. intelligence programmes and the level of access by U.S. public authorities to Europeans' personal data transferred under the Safe Harbour. Taking these and other elements[20] into consideration, the Commission concluded that the Safe Harbour had to be reviewed. Against this background, the Commission formulated 13 recommendations[21] to strengthen and update the data protection guarantees built into the framework. These recommendations focused on: (i) strengthening the substantive privacy principles and increasing the transparency of U.S. self-certified companies' privacy policies incorporating these principles; (ii) better and effective supervision, monitoring and enforcement by the U.S. authorities of companies' compliance with the principles; (iii) the availability of affordable dispute resolution mechanisms for individual complaints; and (iv) the need to ensure that the use of the national security and law enforcement exception provided in the 2000 Safe Harbour Decision would be limited to what is strictly necessary and proportionate.

On the basis of these 13 recommendations, the Commission entered into discussions with the U.S. authorities in January 2014. The subsequent invalidation of the Safe Harbour Decision on 6 October 2015 by the Court of Justice confirmed the need for a stronger and new framework for transatlantic commercial data flows. While the Court's ruling draws on the Commission's 2013 recommendations, it further underscores the need to have limitations, safeguards and judicial control mechanisms in place in order to ensure the continued protection of the personal data of EU individuals, including when the data are accessed and used by public authorities for national security, public interest or law enforcement purposes.

On 2 February 2016, after two years of intensive discussions, the EU and the U.S. reached a political agreement on the new framework, the EU-U.S. Privacy Shield. This new arrangement comprises important new safeguards and will guarantee a high level of protection of the fundamental rights of EU individuals. It will provide the necessary legal certainty for companies on both sides of the Atlantic that want to do business together. And it will inject a new momentum into the transatlantic partnership.

---

Frequently Asked Questions issued by the U.S. Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU. The functioning of the Safe Harbour arrangement relied on commitments and self-certification of adhering companies. The rules were binding under U.S. law for those entities and enforceable by the U.S. Federal Trade Commission.

[19] See footnote 3.

[20] These elements included the exponential increase in data flows and their critical importance for the transatlantic economy as well as the rapid growth of the number of U.S. companies adhering to the Safe Harbour scheme. See the Safe Harbour Communication, p. 37.

[21] Safe Harbour Communication, pp. 18-19.

Following conclusion of the negotiations with the U.S., the Commission will submit the new arrangement to the "Article 29 Working Party" (comprising the EU DPAs) for an opinion on the level of protection provided. Furthermore, the adequacy decision will go through the comitology procedure before it can be adopted. The European Data Protection Supervisor will also be consulted.

## 3.2 What has changed?

The EU-U.S. Privacy Shield provides a robust and effective response to both the Commission's 13 recommendations and the *Schrems* ruling. It contains a number of important improvements, compared to the previous framework, with respect to the commitments that must be undertaken by U.S. companies. It also contains important new commitments and detailed explanations of relevant U.S. laws and practice by U.S. authorities. Unlike its predecessor, the Privacy Shield covers not only commitments in the commercial sector but also, significantly and for the first time in EU-U.S. relations, in the area of access to personal data by public authorities including for national security purposes. This is a crucial and necessary element in light of the Court jurisprudence to restore trust in transatlantic relations following the surveillance revelations.

The most important achievements of this new arrangement can be grouped into four main categories:

First, **strong obligations on companies and robust enforcement**: the new arrangement will be more transparent and contain effective supervision mechanisms to ensure that companies follow the rules they have legally committed to uphold. U.S. companies wishing to import personal data from Europe under the Privacy Shield will need to accept robust obligations on how personal data is processed and individual rights are guaranteed. This includes tightened conditions and stricter liability provisions for Privacy Shield companies that transfer EU data, for instance for sub-processing activities, to third parties outside the framework, whether in the U.S. or in other third countries ("onward transfers"). As for supervision, the U.S. Department of Commerce has committed to a regular and rigorous monitoring of how companies comply with their commitments and to weed out "free-riders", i.e. companies that falsely claim adherence to the scheme. Companies' commitments are legally binding and enforceable under U.S. law by the Federal Trade Commission and companies that do not comply will be faced with severe sanctions.

Second, **clear limits and safeguards with respect to U.S. government access**: for the first time, the U.S. government, through the Department of Justice and the Office of the Director of National Intelligence as the body overseeing the entire U.S. intelligence community, has provided the EU with written representations and assurances that access by public authorities for law enforcement, national security and other public interest purposes will be subject to clear limitations, safeguards and oversight mechanisms. The U.S. will also establish a new redress mechanism for EU data subjects in the area of national security through an Ombudsperson who will be independent from the national security authorities. The Ombudsperson will be tasked with following-up complaints and enquiries by EU individuals into national security access and will have to confirm to the individual that the relevant laws

have been complied with or that any non-compliance has been remedied. This is a significant development that will apply not only to Privacy Shield transfers but to *all* personal data transferred to the U.S. for commercial purposes, irrespective of the basis used to transfer those data.

Third, **effective protection of EU individuals' privacy rights with several redress possibilities**: anyone in Europe who considers that his or her data have been misused under the new arrangement will benefit from several accessible and affordable avenues to obtain individual redress, including cost-free alternative dispute resolution bodies. Companies commit to reply to complaints within a fixed deadline. In addition, any company handling human resources data from Europe has to commit to comply with the decisions of the competent EU DPA while other companies may voluntarily make such a commitment. Individuals can also take their complaint to their 'home' DPA that will be offered a formalized procedure to refer complaints to the Department of Commerce and the Federal Trade Commission to facilitate the investigation and resolution of the respective claim within a reasonable timeframe. If a case is nevertheless not resolved by any of these avenues, individuals will be able to have recourse, as a last resort, to the Privacy Shield Panel, a dispute resolution mechanism that can take binding and enforceable decisions against U.S. Privacy Shield companies. Additionally, EU DPAs will be able to provide assistance to individuals to prepare their case. As mentioned above, for complaints on possible access by national intelligence authorities a new Ombudsperson will be created, providing a further avenue for redress.

Fourth and finally, an **annual joint review mechanism:** this will allow the Commission to regularly monitor the functioning of all aspects of the Privacy Shield, including the limitations and safeguards relating to national security access. The Commission and the U.S. Department of Commerce will carry out the review and involve EU data protection authorities and U.S. national security authorities and the Ombudsperson. In this way, the U.S. will be held accountable to its commitments. But the Commission will not stop there: it will also draw on all other sources of information available, including voluntary transparency reports by companies on the degree of government access requests[22]. The annual review goes beyond the new Regulation, which requires such reviews only at least every four years, thus demonstrating the resolve of both the EU and the U.S. to rigorously ensure full compliance.

This review will not be a formalistic exercise without consequences. In cases where the U.S. companies or public authorities are not abiding by their commitments, the Commission will activate the process to suspend the Privacy Shield. As the Court of Justice has stressed in the *Schrems* ruling, an adequacy decision must not be a dead letter; rather, U.S. companies and authorities have to breathe life into the framework and continuously sustain it by living up to their commitments. Where they fail to do so, the particular benefit for data transfers deriving from an adequacy finding is no longer justified and will be withdrawn.

[22] Major U.S. internet companies already produce such reports in order to regain the trust of their customers. The 2015 USA FREEDOM Act allows the publication of voluntary reports on access requests, at least within certain bands to protect national security interests.

## 3.3 The way forward

The commitments agreed by the U.S. under the Privacy Shield will provide the basis for, and be reflected in, a new Commission adequacy decision. Companies are encouraged to already begin their preparations so as to be in a position to join the new framework as soon as possible after it is in place following the adoption of the Commission decision. For its part, the U.S. government will publish its representations in the U.S. Federal Register, thereby publicly attesting to uphold its commitments.

The EU-U.S. Privacy Shield requires action from many actors:

- the participating U.S. companies that must fulfil their obligations under the framework in the full knowledge that it will be strictly enforced and they will be sanctioned if they are non-compliant. To strengthen trust with their consumers, companies are also encouraged to opt for EU DPAs as their chosen avenue to resolve complaints under the Privacy Shield, as European individuals are most likely to turn to these authorities. Similarly, the extent to which companies are prepared to utilise the possibility provided under U.S. law to publish transparency reports on national security and law enforcement access requests concerning EU data they receive will contribute to maintaining confidence that such access is limited to what is necessary and proportionate[23];

- the various U.S. authorities entrusted with overseeing and enforcing the framework, respecting the limitations and safeguards as far as access to data for law enforcement and national security purposes is concerned, and those entrusted with responding in a timely and meaningful manner to complaints by EU individuals about the possible misuse of their personal data;

- the EU DPAs that have an important role to play in ensuring that individuals can effectively exercise their rights under the Privacy Shield, including by channelling their complaints to the appropriate U.S. authorities and cooperate with the latter, triggering the Ombudsperson mechanism, assisting complainants in bringing their case to the Privacy Shield Panel, as well as exercising oversight over human resources data transfers; and

- the Commission that is responsible for making a finding of adequacy and reviewing it on a regular basis: these regular reviews mark a significant departure from the previous static situation by transforming the Privacy Shield adequacy finding into a closely monitored, living framework.

The annual joint review and the ensuing Commission report – as well as the prospect of suspending the arrangement in case of non-compliance – will thus play a central role in ensuring that the Privacy Shield will endure the test of time. Our mutual transatlantic ambition

[23] Such reporting would be made in accordance with the provisions in the 2015 USA FREEDOM Act. See footnote 22.

should be to develop together a strong culture of privacy compliance and protection of individual rights that restores and maintains trust.

# 4. THE UMBRELLA AGREEMENT: STRENGTHENING DATA PROTECTION SAFEGUARDS FOR LAW ENFORCEMENT COOPERATION

## 4.1 The context

An important dimension of our transatlantic relationship is the capacity for the EU, the Member States and the U.S. to respond effectively to common security threats and challenges in a cooperative and coordinated way. This collective response significantly relies on our ability to exchange personal data in the framework of police and judicial cooperation in criminal matters. A number of bilateral agreements between the Member States and the U.S. as well as between the EU and the U.S.[24] were concluded over time in pursuit of this aim. At the same time, it is equally important for these law enforcement agreements to provide effective data protection safeguards. The two-fold objective of working successfully with our U.S. partners to combat serious crime and terrorism while advancing the level of protection of Europeans in line with their fundamental rights and the EU data protection rules when transfers are made for those purposes, triggered the negotiations, launched in March 2011, on an international data protection agreement in the area of law enforcement, the EU-U.S. Data Protection "Umbrella Agreement"[25].

The EU and the U.S. finalised their negotiations in the summer of 2015. The two parties initialled the Umbrella Agreement on 8 September 2015 in Luxembourg[26], and the agreement is now waiting for its ratification on both sides of the Atlantic. The signing of the Umbrella Agreement was, however, conditional on the passage of the Judicial Redress Act by the U.S. Congress to provide, for the first time, equal treatment of EU citizens with US citizens under the 1974 U.S. Privacy Act[27]. The bill was approved by Congress on 10 February 2016 and was signed into law on 24 February 2016.

## 4.2 What has changed?

The Umbrella Agreement will enshrine, for the very first time, a harmonised and comprehensive set of data protection safeguards that will apply to all transatlantic exchanges between the relevant authorities in the area of criminal law enforcement. It is in effect a

[24] Notably, the EU-US Passenger Name Record (PNR) Agreement and the EU-US Terrorist Financing and Tracking Programme (TFTP).

[25] An agreement between the EU and the U.S. on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

[27] The Judicial Redress Act grants rights to citizens of "covered countries"', designated by the U.S. Government. This is in turn conditional on the following criteria: (a) the country [or regional organisation] has an agreement with the United States on privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses: (b) the country or [regional organization] permits the transfer of personal data for commercial purposes between it and the United States; and (c) the policies regarding the transfer of personal data for commercial purposes and related actions of the country or regional organization, do not materially impede the national security interests of the United States.

fundamental rights agreement setting a high-level standard of protection against which all data exchanges in existing and future agreements must be measured.

First, **the protections and safeguards provided by the Umbrella Agreement will horizontally apply to all data exchanges taking place in the context of transatlantic law enforcement co-operation in criminal matters**. This includes transfers on the basis of domestic laws, EU-US agreements, Member States-U.S. agreements (e.g. Mutual Legal Assistance Treaties) as well as specific agreements providing for the transfer of personal data by private entities for law enforcement purposes. The agreed provisions will thus immediately increase the level of protection guaranteed to EU data subjects when data is transferred to the U.S. It will also increase legal certainty for transatlantic law enforcement cooperation by ensuring that exiting agreements contain all necessary protections and can thus withstand possible legal challenges.

Second, the provisions cover all the core EU data protection rules in terms of **processing standards** (e.g. data quality and integrity, data security, accountability and oversight), **safeguards and limitations** (e.g. purpose and use limitations, data retention, onward transfers, processing of sensitive data) as well as **individual rights** (access, rectification, administrative and judicial redress).

Third, the agreement will ensure the availability of **judicial redress rights for denial of access, denial of rectification and unlawful disclosure**. This constitutes a major improvement and will significantly contribute to restoring trust in transatlantic exchanges. This key and long-sought for EU demand, which had remained unanswered for many years, has already been reflected in the Judicial Redress Act introduced in the U.S. Congress in March 2015 and passed on 10 February 2016. This Act will extend to EU citizens[28] three core judicial redress avenues under the 1974 U.S. Privacy Act that are currently reserved only to U.S. citizens and permanent residents. Thus, for the first time, EU citizens will be able to avail themselves of rights of general application for any transatlantic transfer of data in the criminal law enforcement sector. This removes a critical difference in treatment between EU and U.S. citizens.

Fourth, the Umbrella Agreement generalises and expands to the whole law enforcement sector the principle of **independent oversight** as a core data protection requirement, one that is not present in many of the existing bilateral agreements. This includes effective powers to investigate and resolve individual complaints as regards compliance with the Agreement.

Fifth, the effective implementation of the Umbrella Agreement will be subject to **periodic joint reviews**. Particular attention will be given in these reviews to the provisions relating to individuals' rights (access, rectification, administrative and judicial redress).

The Umbrella Agreement does not in itself authorise data transfers, nor does it constitute an adequacy decision.

[28] According to the Judicial Redress Act, other non-EU countries or "regional economic integration organisations" may equally be designated as "covered countries" with the effect that judicial redress rights would benefit their citizens.

## 4.3 The way forward

The entry into force of the Judicial Redress Act[29] will pave the way to the signing of the Umbrella Agreement. The Commission will shortly submit to the Council a proposal for a decision authorising the signing of the Umbrella Agreement. After signature, the decision concluding the Agreement will have to be adopted by the Council after obtaining the consent of the European Parliament. The Umbrella Agreement will significantly improve the present day situation which is characterised by fragmented, non-harmonised and often weak data protection rules in a patchwork of multilateral, bilateral, national and sectorial instruments. The Umbrella Agreement has a retrospective function in that it will supplement the data protection guarantees in current agreements when and to the extent these lack the requisite level of safeguards. In this respect, it will bring significant added value by essentially "filling in the gaps" of existing agreements which contain lower data protection standards than those found in the Umbrella Agreement. This will enable continuity in law enforcement cooperation while ensuring greater legal certainty when transfers are made. As regards future agreements, the Umbrella Agreement will represent a safety net below which the level of protection cannot fall. This is a very important guarantee for the future and a major shift from the present situation where safeguards, protections and rights have to be negotiated afresh for each individual new agreement. The Umbrella Agreement is thus a template containing the standard safeguards which cannot be negotiated downwards. This is a very important precedent not only for EU-U.S. relations but, more generally, for any future data protection or data exchange arrangement at international level.

Negotiated in parallel with the reform, the Umbrella Agreement is aligned with the EU's data protection acquis. The interaction between the Umbrella Agreement and the Police Directive is particularly relevant given the importance of having a high and common level of data protection, regardless of whether the personal data is processed at national level or exchanged across borders within the EU or with third countries. In this respect, the Umbrella Agreement will help to substantiate the general requirements of the reform in the transatlantic context.

Concluding negotiations on the Umbrella Agreement which sets common standards in a complex area of law and policy is a significant achievement. The future Umbrella Agreement will restore and reinforce trust, provide guarantees of lawfulness for data transfers and facilitate EU-U.S. cooperation in this field.

Going forward, there is a need to jointly address common challenges in the area of police and judicial cooperation. One important open issue is the question of direct access by law enforcement authorities to personal data held by private companies abroad. Such access should, in principle, take place in the framework of formal channels of co-operation, such as Mutual Legal Assistance (MLA) agreements or other sectorial agreements. Private companies currently risk facing legal uncertainty which could impact on their capacity to operate across different jurisdictions when asked to provide access to electronic evidence under the laws of one country for personal data subject to the laws of another. In parallel to the upcoming

[29] The Judicial Redress Act enters into force 90 days after its enactment.

review of the EU-U.S. MLA Agreement[30], the EU would welcome further exchanges with the U.S. on this matter, including addressing the development of common and more effective rules to collect electronic evidence.

## 5. CONCLUSION

The successful conclusion of the key actions outlined in the 2013 Communication demonstrates the EU's capacity to solve problems in a pragmatic and focused manner without sacrificing its strong fundamental rights values and traditions. It also demonstrates that the EU and the U.S. are able to resolve their differences and take difficult decisions in order to preserve a strategic relationship that has withstood the test of time. At the same time, as we turn a new chapter in our bilateral relations, the time for vigilance is not over as we continue to face common threats and challenges in an uncertain world.

Once the Privacy Shield and the Umbrella Agreement are in place, it is incumbent on both parties to ensure that these two important data transfer frameworks work effectively and in an enduring manner. Their success depends in large part on effective enforcement and the respect of the rights accorded to individuals. It also depends on the continual assessment of their functioning; this requires a shift in mind-set from a static to a more dynamic process.

Against this background, an important element of this process relates to the ongoing reform of U.S. intelligence programmes. In this respect, the Commission will follow closely the upcoming reports prepared by the Privacy and Civil Liberties Oversight Board (PCLOB) and the review of the Section 702 FISA programme relating to foreign surveillance due in 2017. In particular further reforms relating to transparency, oversight, and the extension of safeguards to non-U.S. persons will be followed closely.

More generally, given the significance of cross border data flows for transatlantic trade, the EU will follow closely further legislative progress on the U.S. side in the area of privacy. Now that Europe has equipped itself with a single, coherent and robust set of rules, we hope that the U.S. will also continue to pursue efforts towards a comprehensive system of privacy and data protection. It is through such a comprehensive approach that convergence between the two systems could be achieved in the longer term. In this respect, the Commission will hold an annual privacy summit with interested NGOs and other concerned stakeholders on both sides of the Atlantic.

The EU-U.S. partnership can be a driving force to develop and promote international legal standards for the protection of privacy and personal data. Initiatives at UN level, including the work of the Special Rapporteur on the Right to Privacy, can also play an important role in this regard. In the coming years, given the increasing centrality of these issues on the global stage, the EU and the U.S. should seize this opportunity to advance their common values of individual freedoms and rights in the globalised digital world.

[30] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11.2009, p. 40-41.