European Commission - Fact Sheet

EU-U.S. Privacy Shield: Frequently Asked Questions

Brussels, 29 February 2016

What is the EU-US Privacy Shield?

After two years of negotiations, the European Commission and the U.S. Department of Commerce reached on 2 February 2016 a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (IP/16/216). This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses.

The EU-U.S. Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities. The new arrangement includes written commitments and assurance by the U.S. that any access by public authorities to personal data transferred under the new arrangement on national security grounds will be subject to clear conditions, limitations and oversight, preventing generalised access. The newly created Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in this context.

What is an adequacy decision?

An "adequacy decision" is a decision adopted by the European Commission, which establishes that a non-EU country ensures an adequate level of protection of personal data by reason of its domestic law and international commitments.

The effect of such a decision is that personal data can flow from the 28 EU Member States (and the three European Economic Area member countries: Norway, Liechtenstein and Iceland) to that third country, without any further restrictions.

The EU-U.S. Privacy Shield framework ensures an adequate level of protection for personal data transferred to the U.S. The EU-US Privacy Shield consists of Privacy Principles that companies must abide by and commitments on how the arrangement will be enforced (written commitments and assurance by the State Secretary John Kerry, Commerce Secretary Penny Pritzker, the Federal Trade Commission and the Office of the Director of National Intelligence, amongst others).

What are the main differences between the old "Safe Harbour" arrangement and the new EU-U.S. Privacy Shield?

The EU-U.S. Privacy Shield addresses both the recommendations made by the Commission in November 2013 and the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement provides **stronger obligations on companies** in the U.S. to protect the personal data of Europeans. It requires stronger monitoring and enforcement by the U.S. Department of Commerce (DoC) and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities.

The new arrangement includes commitments and assurance by the US that the competencies under US law for public authorities to access personal data transferred under the new arrangement will be subject to **clear conditions, limitations and oversight**, preventing generalised access. The newly created Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in relation to possible access by national intelligence services.

The new agreement will include:

- **Strong obligations on companies and robust enforcement:** the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply. The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the

scheme.

- **Clear safeguards and transparency obligations on U.S. government access:** for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. US Secretary of State John Kerry committed to establishing a **redress possibility** in the area of national intelligence for Europeans through an **Ombudsman mechanism** within the Department of State, who will be **independent** from national security services. The Ombudsman will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with. All the written commitments will be published in the U.S. federal register.

- **Effective protection of EU citizens' rights with several redress possibilities: Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the U.S. Department of Commerce and Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved**. If a case is not resolved by any of the other means, as a last resort there will be an enforceable arbitration mechanism. Moreover, companies can commit to comply with advice from European DPAs. This is obligatory for companies handling human resource data.

- **Annual joint review mechanism:** that will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available, including transparency reports by companies on the extent of government access requests. The Commission will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans. On the basis of the annual review, the Commission will issue a public report to the European Parliament and the Council.

How are the requirements of the ECJ ruling satisfied?

- **Regular review of adequacy decisions**

The new arrangement will be transparent and contain **effective supervision mechanisms** to ensure that companies follow the rules they submitted themselves to.

The EU and the US have now agreed to establish a new mechanism to monitor the functioning of the Safe Harbour through an **annual joint review**.

The Commission and the Department of Commerce will carry out **this review,** which will serve to **substantiate the commitments** made. The joint review would involve, as appropriate, representatives of the US intelligence community and will provide a dynamic and ongoing process to ensure that the Privacy Shield is functioning in accordance with the principles and commitments made.

The US has committed to **stronger oversight** by the Department of Commerce, **stronger cooperation** between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a self-regulating one to an oversight system that is more responsive as well as proactive.

The Department of Commerce will monitor the compliance of companies with the Privacy Shield principles on an ongoing basis of companies, including through detailed questionnaires. These reviews will take place when the Department of Commerce receives specific complaints, when a company does not provide satisfactory responses, or when there is credible evidence suggesting that a company may not be complying with the Privacy Shield Principles. If companies do not comply in practice they face sanctions and removal from the list.

- **Limitations for access to personal data for national security purposes**

The U.S. authorities set out the safeguards and limitation and oversight mechanism in place for any access to data by public authorities for national security purposes. The U.S. affirms that there is no indiscriminate or mass surveillance. For complaints on possible access by national intelligence authorities, a new Ombudsperson mechanism will be set up, independent from the intelligence services.

- **All individual complaints will be handled and resolved**

There will be a number of ways to address complaints, starting with dispute resolution by the company and free of charge alternative dispute resolution solutions. Citizens can also go to the Data protection authorities who will work together with the U.S. Department of Commerce and Federal Trade

Commission to ensure that complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Redress possibility in the area of national security for EU citizens' will be handled by an Ombudsman independent from the US intelligence services.

How will the Privacy Shield work concretely?

American companies will register to be on the Privacy Shield List and **self-certify** that they meet the requirements set out. This procedure has to be done each year.

The US Department of Commerce will have **to monitor and actively verify** that companies' privacy policies are presented in line with the relevant Privacy Shield principles and are readily available.

The US has committed to maintaining an **updated list of current Privacy Shield members** and removing those companies that have left the arrangement. The Department of Commerce will ensure that companies that are no longer members of Privacy Shield must still **continue to apply** its principles to personal data received when they were in the Privacy Shield, for as long as they continue to retain them.

How can Europeans obtain redress in the US if their data is misused by commercial companies?

Any citizen who considers that their data has been misused will have several redress possibilities, under the new arrangement:

- **Lodge a complaint with the company itself:**Companies commit to reply to complaints within 45 days. In addition, any company handling human resources data from Europeans has to commit to comply with advice by the competent EU Data Protection Authority (DPA), while other companies may voluntarily make such a commitment. The Commission encourages companies to do so.
- **Take their complaint to their 'home' DPA:** The DPA will refer the complaint to the Department of Commerce, who will respond within 90 days, or the Federal Trade Commission, if the Department of Commerce is unable to resolve the matter.
- **Use the Alternative Dispute Resolution,** a free of charge tool to which US companies must sign up if they want to be Privacy Shield-certified. The companies will be required to include information in their published privacy policies about the independent dispute resolution body where consumers can address their complaints. They must provide a link to the website of their chosen dispute resolution provider and the Department of Commerce will verify that companies have implemented this obligation.
- If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Individuals will be able to have recourse to the **Privacy Shield Panel**, a dispute resolution mechanism that can take binding decisions against U.S. self-certified companies. It ensures that every single complaint is being dealt with and that the individual obtains a remedy.

What changes have been made in the U.S. since the Snowden revelations?

The U.S. Government and Congress launched important surveillance reforms in response to the Snowden revelations.

In January 2014, President Obama issued Presidential Policy Directive 28 (PPD-28), which imposes important limitations for intelligence operations. It specifies that data collection by the intelligence services should be targeted. Additionally, the PPD-28 limits the use of bulk collection of data to six national security purposes (detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to the Armed Forces,or transnational criminal threats) to better protect privacy of all persons, including non-U.S citizens.

Since 2015, the USA Freedom Act also limits bulk collection of data and allows companies to issue transparency reports on the approximate number of government access requests.

The Commission will follow with interest the upcoming reports of the Privacy and Civil Liberties Oversight Board assessing the implementation of the PPD-28, as well as the review of the Section 702 FISA Programme relating to foreign surveillance due in 2017.

What are the guarantees regarding the national security access to data transferred to the US?

For the first time, the US has given the EU written assurance, to be published in the federal register, that the access of public authorities for law enforcement and national security purposes will be subject to **clear limitations, safeguards and oversight mechanisms**. The US assures there is no **indiscriminate or mass surveillance** on the personal data transferred to the US under the new arrangement. To regularly monitor the functioning of the arrangement and the commitments made, there will be an **annual joint review**, which will also include the issue of national security access. The

European Commission and the US Department of Commerce will conduct the review and invite national intelligence experts from the US and European Data Protection Authorities to it.

What will be the role of the Ombudsperson mechanism?

The possibility for redress in the area of national security for EU citizens' will be handled by an **Ombudsperson,** independent from the US intelligence services. This is a new mechanism introduced by the Privacy Shield arrangement.

The Ombudsperson mechanism will deal with individual complaints from Europeans if they fear that their personal information has been used in an unlawful way by US authorities in the area of national security. This redress mechanism will inform the complainant whether the matter has been properly investigated and that either US law has been complied with or, in case of non-compliance, this has been remedied.

What is the role of Judicial Redress Act?

The **Judicial Redress Act** was signed by President Obama on 24 February. Once in force, it will give EU citizens access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes. The Judicial Redress Act will extend the rights US citizens and residents enjoy under the 1974 Privacy Act also to EU citizens. This is a long-standing demand of the EU.

What is the EU-US data protection "Umbrella Agreement"?

The EU-US data protection "Umbrella Agreement" puts in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation. The Agreement covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the U.S. for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.

The Umbrella Agreement is not in itself a legal basis for data transfer nor an adequacy decision. It will provide safeguards and guarantees of lawfulness for data transfers made under different agreements. This will ensure that fundamental rights are fully respected, while facilitating EU-U.S. law enforcement cooperation and restoring trust.

With the signature of the Judicial Redress Act by President Obama on 24 February, EU citizens will soon benefit from equal treatment: they will have the same judicial redress rights as US citizens in case of privacy breaches. This point was outlined by President Juncker in his political guidelines, when he stated: " *The United States must [...] 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. Removing such discrimination will be essential for restoring trust in transatlantic relations*"

For more information

See IP/16/433

MEMO/16/434

Press contacts:

Melanie VOIN (+ 32 2 295 86 59)
Christian WIGAND (+32 2 296 22 53)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email