European Commission

February 2016

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield imposes **stronger obligations on U.S. companies** to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbour framework invalid. The Privacy Shield requires the U.S. to **monitor and enforce more robustly**, and cooperate more with European Data Protection Authorities.

It includes, for the first time, written commitments and assurance regarding **access to data by public authorities**.

The new arrangement will include the following elements:

Commercial sector

Strong obligations on companies and robust enforcement:

> Greater transparency.

> Oversight mechanisms to ensure companies abide by the rules.

> Sanctions or exclusion of companies if they do not comply.

> Tightened conditions for onward transfers.

Redress

Several redress possibilities:

> **Directly with the company:** Companies must reply to complaints from individuals within 45 days.

> **Alternative Dispute Resolution:** free of charge.

> **With the Data Protection Authority:** they will work with U.S. Department of Commerce and Federal Trade Commission to ensure unresolved complaints by EU citizens are investigated and swiftly resolved.

> **Privacy Shield Panel:** As a last resort, there will be an arbitration mechanism to ensure an enforceable decision.

U.S. Government access

Clear safeguards and transparency obligations:

> For the first time, written assurance from the U.S. that any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms.

> U.S authorities affirm absence of indiscriminate or mass surveillance.

> Companies will be able to report approximate number of access requests.

> New redress possibility through EU-U.S. Privacy Shield Ombudsperson mechanism, independent from the intelligence community, handling and solving complaints from individuals.

Monitoring

Annual joint review mechanism:

> Monitoring the functioning of the Privacy Shield and U.S. commitments, including as regards access to data for law enforcement and national security purposes.

> Conducted by the European Commission and the U.S. Department of Commerce, associating national intelligence experts from the U.S. and European Data Protection Authorities.

> Annual privacy summit with NGOs and stakeholders on developments in the area of U.S. privacy law and its impact on Europeans.

> Public report by the European Commission to the European Parliament and the Council, based on the annual joint review and other relevant sources of information (e.g. transparency reports by companies).

What will it mean in practice?

For American companies

> Self-certify annually that they meet the requirements.

> Display privacy policy on their website.

> Reply promptly to any complaints.

> (If handling human resources data) Cooperate and comply with European Data Protection Authorities.

For European individuals

> More transparency about transfers of personal data to the U.S. and stronger protection of personal data.

> Easier and cheaper redress possibilities in case of complaints —directly or with the help of their local Data Protection Authority.