Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield

2018/2645(RSP) - 05/07/2018 - Text adopted by Parliament, single reading

The European Parliament adopted by 303 votes to 223 with 29 abstentions a resolution tabled by the Committee on Civil Liberties, Justice and Home Affairs on the adequacy of the protection afforded by the EU-US Privacy Shield.

Taking note of the improvements compared to the Safe Harbour agreement, Parliament nevertheless highlighted the **persistent weaknesses of the Privacy Shield** as regards the respect of fundamental rights of data subjects. It took the view that the current Privacy Shield arrangement **does not provide the adequate level of protection** required by Union data protection law and the EU Charter as interpreted by the European Court of Justice. It underlined the increasing risk that the Court may invalidate Commission Implementing Decision (EU) 2016/1250 on the Privacy Shield.

Accordingly, it considered that, unless the US is fully compliant by 1 September 2018, the Commission must **suspend the Privacy Shield until the US authorities comply with its terms**.

In its resolution, Parliament raised the following points:

Institutional issues: Members stressed that the recent revelations regarding the practices of Facebook and Cambridge Analytica highlight the need for **proactive oversight and enforcement actions** which are not only based on complaints but which include systematic checks of the practical compliance of privacy policies with the Privacy Shield principles throughout the certification lifecycle. Facebook, a signatory to the Privacy Shield, has confirmed that the data of 2.7 million EU citizens were among those improperly used by political consultancy Cambridge Analytica.

Members added that the **Ombudsperson mechanism** set up by the US Department of State is **not sufficiently independent** and is not endowed with sufficient effective powers to provide effective redress to EU citizens.

Commercial issues: Parliament felt that there is **no effective control** over whether certified companies actually comply with the Privacy Shield provisions. It called on the US Department of Commerce to undertake proactively *ex officio* compliance reviews to monitor compliance of companies with the Privacy Shield rules. It added that, in view of the recent revelations of **misuse of personal data** by companies certified under the Privacy Shield, such as Facebook and Cambridge Analytica, the US authorities responsible for enforcing the Privacy Shield must act upon such revelations without delay and, if needed, **remove** such companies from the Privacy Shield list. The competent EU data protection authorities must also investigate such revelations and, if appropriate, **suspend or prohibit** data transfers under the Privacy Shield.

Parliament also raised concerns about

- the lack of specific rules and guarantees in the Privacy Shield for **decisions based on automated processing/profiling**, which produce legal effect or significantly affect the individual;
- the fact that Privacy Shield principles do not follow the EU model of **consent-based processing**, but allow for opt-out / right to object only in very specific circumstances.
- the rejection by Congress in March 2017 of the rule submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other

Telecommunications Services', which in practice **eliminates broadband privacy rules** that would have required Internet Service Providers to get consumers' explicit consent before selling or sharing web browsing data and other private information with advertisers and other companies.

Law Enforcement and National Security issues: Members called for a **clear definition of 'national security'** in the Privacy Shield mechanism, stating that the term is not specifically circumscribed in order to ensure that data protection breaches can be effectively reviewed in courts to ensure compliance with a strict test of what is necessary and proportionate. In addition, Parliament made the following points:

- **Cloud Act**: Members expressed strong concerns regarding the Clarifying Lawful Overseas Use of Data Act or CLOUD Act, which expands the abilities of American and foreign law enforcement to target and access people's data across international borders. It considered that the Act could have **serious implications for the EU** as it is far-reaching and creates a potential conflict with the EU data protection laws. A more balanced solution would have been to strengthen the existing international system of Mutual Legal Assistance Treaties with a view to encouraging international and judicial cooperation.
- **Executive Order 12333**: Members were concerned that this Order allows the National Security Agency to **share vast amounts of private data** gathered without warrants, court orders or congressional authorisation with 16 other agencies, including the FBI, the Drug Enforcement Agency and the Department of Homeland Security. They regretted the **lack of any judicial review of surveillance activities** conducted on the basis of Executive Order 12333.
- **Section 702 of the US Foreign Intelligence Surveillance Act (FISA)**: Parliament called for evidence and legally binding commitments ensuring that data collection under FISA Section 702 is not indiscriminate and access is not conducted on a generalised basis (bulk collection) in contrast with the EU Charter. It deplored the fact that EU individuals are excluded from the additional protection provided by the reauthorisation of FISA Section 702.
- **Executive Order 13768**: Parliament considered that this Order indicates the intention of the US executive to reverse the data protection guarantees previously granted to EU citizens and to override the commitments made towards the EU during the Obama Presidency.

Parliament called on the Commission to take all the necessary measures to ensure that the Privacy Shield will fully comply with Regulation (EU) 2016/679, to be applied as from 25 May 2018, and with the EU Charter, so that adequacy does not lead to loopholes or competitive advantage for US companies.