European Parliament
2014-2019

TEXTS ADOPTED
Provisional edition

P8_TA-PROV(2017)0131

Adequacy of the protection afforded by the EU-US privacy Shield

European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP))

The European Parliament,

– having regard to the Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU) and Articles 6, 7, 8, 11, 16, 47 and 52 of the Charter of Fundamental Rights of the European Union,

– having regard to 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 (Data Protection Directive)[1],

– having regard to 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[2],

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[3], and to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[4],

– having regard to the judgment of the Court of Justice of the European Union of 6 October 2015 in Case C-362/14 *Maximillian Schrems* v *Data Protection*

---

1 OJ L 281, 23.11.1995, p. 31.
2 OJ L 350, 30.12.2008, p. 60.
3 OJ L 119, 4.5.2016, p. 1.
4 OJ L 119, 4.5.2016, p. 89.

Commissioner[1],

– having regard to the Commission communication to the European Parliament and the Council of 6 November 2015 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)0566),

– having regard to the Commission communication to the European Parliament and the Council of 10 January 2017 on Exchanging and Protecting Personal Data in a Globalised World (COM(2017)0007),

– having regard to the judgment of the Court of Justice of the European Union of 21 December 2016 in Cases C-203/15 *Tele2 Sverige AB* v *Post- och telestyrelsen* and C-698/15 *Secretary of State for the Home Department* v *Tom Watson and Others*[2],

– having regard to Commission Implementing Decision (EU) 2016/1250 of 12 July 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 Privacy Shield[3],

– having regard to Opinion 4/2016 of the European Data Protection Supervisor (EDPS) on the EU-US Privacy Shield draft adequacy decision[4],

– having regard to the Opinion of the Article 29 Data Protection Working Party of 13 April 2016 on the EU-US Privacy Shield draft adequacy decision[5] and the Article 29 Working Party Statement of 26 July 2016[6],

– having regard to its resolution of 26 May 2016 on transatlantic data flows[7],

– having regard to Rule 123(2) of its Rules of Procedure,

A. whereas the Court of Justice of the European Union (CJEU) in its judgment of 6 October 2015 in Case C-362/14 *Maximillian Schrems* v *Data Protection Commissioner* invalidated the Safe Harbour decision and clarified that an adequate level of protection in a third country must be understood to be 'essentially equivalent' to that guaranteed within the European Union by virtue of Directive 95/46/EC read in the light of the Charter of Fundamental Rights of the European Union (hereinafter 'the EU Charter'), prompting the need to conclude negotiations on a new arrangement so as to ensure legal certainty on how personal data should be transferred from the EU to the US;

B. whereas, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the rules applicable in that country

---

1 ECLI:EU:C:2015:650.
2 ECLI:EU:C:2016:970.
3 OJ L 207, 1.8.2016, p. 1.
4 OJ C 257, 15.7.2016, p. 8.
5 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
6 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf
7 Texts adopted, P8_TA(2016)0233.

deriving from its domestic law or its international commitments, as well as the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46/EC, take account of all the circumstances surrounding a transfer of personal data to a third country; whereas this assessment must not only refer to legislation and practices relating to the protection of personal data for commercial and private purposes, but must also cover all aspects of the framework applicable to that country or sector, in particular, but not limited to, law enforcement, national security and respect for fundamental rights;

C. whereas transfers of personal data between commercial organisations of the EU and the US are an important element for the transatlantic relationships; whereas these transfers should be carried out in full respect of the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is the protection of fundamental rights, as enshrined in the EU Charter;

D. whereas in its Opinion 4/2016 the EDPS raised several concerns on the draft Privacy Shield; whereas the EDPS welcomes in the same opinion the efforts made by all parties to find a solution for transfers of personal data from the EU to the US for commercial purposes under a system of self-certification;

E. whereas in its Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision the Article 29 Working Party welcomed the significant improvements brought about by the Privacy Shield compared with the Safe Harbour decision whilst also raising strong concerns about both the commercial aspects and access by public authorities to data transferred under the Privacy Shield;

F. whereas on 12 July 2016, after further discussions with the US administration, the Commission adopted its Implementing Decision (EU) 2016/1250, declaring the adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-US Privacy Shield;

G. whereas the EU-US Privacy Shield is accompanied by several letters and unilateral statements from the US administration explaining, inter alia, the data protection principles, the functioning of oversight, enforcement and redress and the protections and safeguards under which security agencies can access and process personal data;

H. whereas in its statement of 26 July 2016, the Article 29 Working Party welcomes the improvements brought by the EU-US Privacy Shield mechanism compared with Safe Harbour and commended the Commission and the US authorities for having taken into consideration its concerns; whereas the Article 29 Working Party indicates, nevertheless, that a number of its concerns remain, regarding both the commercial aspects and the access by US public authorities to data transferred from the EU, such as the lack of specific rules on automated decisions and of a general right to object, the need for stricter guarantees on the independence and powers of the Ombudsperson mechanism, and the lack of concrete assurances of not conducting mass and indiscriminate collection of personal data (bulk collection);

1. Welcomes the efforts made by both the Commission and the US administration to address the concerns raised by the CJEU, the Member States, the European Parliament, data protection authorities (DPAs) and stakeholders, so as to enable the Commission to adopt the implementing decision declaring the adequacy of the EU-US Privacy Shield;

2. Acknowledges that the EU-US Privacy Shield contains significant improvements regarding the clarity of standards compared with the former EU-US Safe Harbour and that US organisations self-certifying adherence to the EU-US Privacy Shield will have to comply with clearer data protection standards than under Safe Harbour;

3. Takes note that as at 23 March 2017, 1 893 US organisations have joined the EU-US Privacy Shield; regrets that the Privacy Shield is based on voluntary self-certification and therefore applies only to US organisations which have voluntarily signed up to it, which means that many companies are not covered by the scheme;

4. Acknowledges that the EU-US Privacy Shield facilitates data transfers from SMEs and businesses in the Union to the US;

5. Notes that, in line with the ruling of the CJEU in the Schrems case, the powers of the European DPAs remain unaffected by the adequacy decision and they can, therefore, exercise them, including the suspension or the ban of data transfers to an organisation registered with the EU-US Privacy Shield; welcomes in this regard the prominent role given by the Privacy Shield Framework to Member State DPAs to examine and investigate claims related to the protection of the rights to privacy and family life under the EU Charter and to suspend transfers of data, as well as the obligation placed upon the US Department of Commerce to resolve such complaints;

6. Notes that under the Privacy Shield Framework, EU data subjects have several means available to them to pursue legal remedies in the US: first, complaints can be lodged either directly with the company or through the Department of Commerce following a referral by a DPA, or with an independent dispute resolution body, secondly, with regard to interferences with fundamental rights for the purpose of national security, a civil claim can be brought before the US court and similar complaints can also be addressed by the newly created independent Ombudsperson, and finally, complaints about interferences with fundamental rights for the purposes of law enforcement and the public interest can be dealt with by motions challenging subpoenas; encourages further guidance from the Commission and DPAs to make those legal remedies all the more easily accessible and available;

7. Acknowledges the clear commitment of the US Department of Commerce to closely monitor the compliance of US organisations with the EU-US Privacy Shield Principles and their intention to take enforcement actions against entities failing to comply;

8. Reiterates its call on the Commission to seek clarification on the legal status of the 'written assurances' provided by the US and to ensure that any commitment or arrangement foreseen under the Privacy Shield is maintained following the taking up of office of a new administration in the United States;

9. Considers that, despite the commitments and assurances made by the US Government by means of the letters attached to the Privacy Shield arrangement, important remain as regards certain commercial aspects, national security and law enforcement;

10. Specifically notes the significant difference between the protection provided by Article 7 of Directive 95/46/EC and the 'notice and choice' principle of the Privacy Shield arrangement, as well as the considerable differences between Article 6 of Directive 95/46/EC and the 'data integrity and purpose limitation' principle of the Privacy Shield

arrangement; points out that instead of the need for a legal basis (such as consent or contract) that applies to all processing operations, the data subject rights under the Privacy Shield Principles only apply to two narrow processing operations (disclosure and change of purpose) and only provide for a right to object ('opt-out');

11. Takes the view that these numerous concerns could lead to a fresh challenge to the decision on the adequacy of the protection being brought before the courts in the future; emphasises the harmful consequences as regards both respect for fundamental rights and the necessary legal certainty for stakeholders;

12. Notes, amongst other things, the lack of specific rules on automated decision-making and on a general right to object, and the lack of clear principles on how the Privacy Shield Principles apply to processors (agents);

13. Notes that, while individuals have the possibility to object vis-à-vis the EU controller to any transfer of their personal data to the US, and to the further processing of those data in the US where the Privacy Shield company acts as a processor on behalf of the EU controller, the Privacy Shield lacks specific rules on a general right to object vis-à-vis the US self-certified company;

14. Notes that only a fraction of the US organisations that have joined the Privacy Shield have chosen to use an EU DPA for the dispute resolution mechanism; is concerned that this constitutes a disadvantage for EU citizens when trying to enforce their rights;

15. Notes the lack of explicit principles on how the Privacy Shield Principles apply to processors (agents), while recognising that all principles apply to the processing of personal data by any US self-certified company '[u]nless otherwise stated' and that the transfer for processing purposes always requires a contract with the EU controller which will determine the purposes and means of processing, including whether the processor is authorised to carry out onward transfers (e.g. for sub-processing);

16. Stresses that, as regards national security and surveillance, notwithstanding the clarifications brought by the Office of the Director of National Intelligence (ODNI) in the letters attached to the Privacy Shield framework, 'bulk surveillance', despite the different terminology used by the US authorities, remains possible; regrets the lack of a uniform definition of the concept of bulk surveillance and the adoption of the American terminology, and therefore calls for a uniform definition of bulk surveillance linked to the European understanding of the term, where evaluation is not made dependent on selection; stresses that any kind of mass surveillance is in breach of the EU Charter;

17. Recalls that Annex VI (letter from Robert S. Litt, ODNI) clarifies that under Presidential Policy Directive 28 (hereinafter 'PPD-28'), bulk collection of personal data and communications of non-US persons is still permitted in six cases; points out that such bulk collection only has to be 'as tailored as feasible' and 'reasonable', which does not meet the stricter criteria of necessity and proportionality as laid down in the EU Charter;

18. Notes with great concern that the Privacy and Civil Liberties Oversight Board (PCLOB) referred to in Annex VI (letter from Robert S. Litt, ODNI) as an independent body established by statute, charged with analysing and reviewing counter-terrorism programmes and policies, including the use of signals intelligence, to ensure that they

adequately protect privacy and civil liberties, lost its quorum on 7 January 2017 and will be in a sub-quorum status until new Board Members are nominated by the US President and confirmed by the US Senate; highlights that in a sub-quorum status the PCLOB is more limited in its authority and cannot undertake certain actions that require approval of the Board such as initiating oversight projects or making oversight recommendations, thus seriously undermining the compliance and oversight guarantees and assurances made by US authorities in this field;

19. Deplores the fact that the EU-US Privacy Shield does not prohibit the collection of bulk data for law enforcement purposes;

20. Stresses that in its judgment of 21 December 2016, the CJEU clarified that the EU Charter 'must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'; points out that the bulk surveillance in the US therefore does not provide for an essentially equivalent level of the protection of personal data and communications;

21. Is alarmed by the recent revelations about surveillance activities conducted by a US electronic communications service provider on all emails reaching its servers, upon request of the National Security Agency (NSA) and the FBI, as late as 2015, i.e. one year after Presidential Policy Directive 28 was adopted and during the negotiation of the EU-US Privacy Shield; insists that the Commission seek full clarification from the US authorities and make the answers provided available to the Council, Parliament and national DPAs; sees this as a reason to strongly doubt the assurances brought by the ODNI; is aware that the EU-US Privacy Shield rests on PPD-28, which was issued by the President and can also be repealed by any future President without Congress's consent;

22. Notes with concern that, on 23 and 28 March 2017 respectively, both the US Senate and the House of Representatives voted in favour of rejecting 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; considers that this is yet another threat to privacy safeguards in the United States;

23. Expresses great concerns at the issuance of the 'Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333', approved by the Attorney General on 3 January 2017, allowing the NSA 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; calls on the Commission to immediately assess the compatibility of these new rules with the commitments made by the US authorities under the Privacy Shield, as well as their impact on the level of personal data protection in the United States;

24. Recalls that while individuals, including EU data subjects, have a number of avenues of

redress when they have been the subject of unlawful (electronic) surveillance for national security purposes in the US, it is equally clear that at least some legal bases that US intelligence authorities may use (e.g. Executive Order 12333) are not covered; highlights moreover that, even where judicial redress possibilities in principle do exist for non-US persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including US persons) will be declared inadmissible where they cannot show 'standing', which restricts access to ordinary courts;

25. Calls on the Commission to assess the impact of the Executive Order on 'Enhancing Public Safety in the Interior of the United States' of 25 January 2017, and in particular its Section 14 on the exclusion of foreign citizens from the protections of the Privacy Act regarding personally identifiable information, contradicting the written assurances that judicial redress mechanisms exist for individuals in cases where data was accessed by the US authorities; asks the Commission to communicate a detailed legal analysis of the consequence of the Executive Order measures on avenues for remedies and the right to judicial redress for Europeans in the US;

26. Deplores the fact that neither the Privacy Shield Principles nor the letters of the US administration providing clarifications and assurances demonstrate the existence of effective judicial redress rights for individuals in the EU whose personal data are transferred to a US organisation under the Privacy Shield Principles and further accessed and processed by US public authorities for law enforcement and public interest purposes, which were emphasised by the CJEU in its judgment of 6 October 2015 as the essence of the fundamental right in Article 47 of the EU Charter;

27. Recalls its resolution of 26 May 2016 stating that the Ombudsperson mechanism set up by the US Department of State is not sufficiently independent and is not vested with sufficient effective powers to carry out its duties and provide effective redress to EU individuals; points out that to date the incoming US administration has not appointed a new Ombudsperson following the end of term of the Under Secretary for Economic Growth, Energy, and the Environment appointed to this role in July 2016; considers that in the absence of an appointed independent and sufficiently empowered Ombudsperson, the US assurances with regard to the provision of effective redress to EU individuals would be null and void; is generally concerned that an individual affected by a breach of the rules can apply only for information and for the data to be deleted and/or for a stop to further processing, but has no right to compensation;

28. Notes with concern that, as of 30 March 2017, the Federal Trade Commission (FTC), which enforces the Privacy Shield, has three of its five seats vacant;

29. Regrets that the procedure of adoption of an adequacy decision does not provide for a formal consultation of relevant stakeholders such as companies, and in particular SMEs' representation organisations;

30. Regrets that the Commission followed the procedure for adoption of the Commission implementing decision in a practical manner that de facto has not enabled Parliament to exercise its right of scrutiny on the draft implementing act in an effective manner;

31. Calls 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 16 May

2018, and with the EU Charter;

32. Calls on the Commission to ensure, in particular, that personal data that has been transferred to the US under the Privacy Shield can only be transferred to another third country if that transfer is compatible with the purpose for which the data was originally collected, and if the same rules of specific and targeted access for law enforcement apply in the third country;

33. Calls on the Commission to monitor whether personal data which is no longer necessary for the purpose for which it had been originally collected is deleted, including by law enforcement agencies;

34. Calls on the Commission to closely monitor whether the Privacy Shield allows for the DPAs to fully exercise all their powers, and if not, to identify the provisions that result in a hindrance to the DPAs' exercise of powers;

35. Calls on the Commission to conduct, during the first joint annual review, a thorough and in-depth examination of all the shortcomings and weaknesses referred to in this resolution and in its resolution of 26 May 2016 on transatlantic data flows, and those identified by the Article 29 Working Party, the EDPS and the stakeholders, and to demonstrate how they have been addressed so as to ensure compliance with the EU Charter and Union law, and to evaluate meticulously whether the mechanisms and safeguards indicated in the assurances and clarifications by the US administration are effective and feasible;

36. Calls on the Commission to ensure that when conducting the joint annual review, all the members of the team have full and unrestricted access to all documents and premises necessary for the performance of their tasks, including elements allowing a proper evaluation of the necessity and proportionality of the collection and access to data transferred by public authorities, for either law enforcement or national security purposes;

37 .Stresses that all members of the joint review team must be ensured independence in the performance of their tasks and must be entitled to express their own dissenting opinions in the final report of the joint review, which will be public and annexed to the joint report;

38. Calls on the Union DPAs to monitor the functioning of the EU-US Privacy Shield and to exercise their powers, including the suspension or definitive ban of personal data transfers to an organisation in the EU-US Privacy Shield if they consider that the fundamental rights to privacy and the protection of personal data of the Union's data subjects are not ensured;

39. Stresses that Parliament should have full access to any relevant document related to the joint annual review;

40. Instructs its President to forward this resolution to the Commission, the Council, the governments and national parliaments of the Member States and the US Government and Congress.