European Parliament
2014-2019

TEXTS ADOPTED

P8_TA(2018)0315

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

European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(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 (the EU Charter),

– 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)[1] (GDPR), 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[2],

– 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 Commissioner*[3],

– 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*[4];

– 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[5],

---

1 OJ L 119, 4.5.2016, p. 1.
2 OJ L 119, 4.5.2016, p. 89.
3 ECLI:EU:C:2015:650.
4 ECLI:EU:C:2016:970.
5 OJ L 207, 1.8.2016, p. 1.

– having regard to the Opinion 4/2016 of the European Data Protection Supervisor (EDPS) of 30 May 2016 on the EU-US Privacy Shield draft adequacy decision[1],

– having regard to the Opinion 01/2016 of the Article 29 Data Protection Working Party (WP29) of 13 April 2016 on the EU-US Privacy Shield draft adequacy decision[2] and the WP29 Statement of 26 July 2016[3],

– having regard to the Report from the Commission of 18 October 2017 to the European Parliament and the Council on the first annual review of the functioning of the EU-US Privacy Shield (COM(2017)0611) and the Commission Staff Working Paper accompanying the document (SWD(2017)0344),

– having regard to the WP29 document of 28 November 2017 entitled 'EU-US Privacy Shield – First Annual Joint Review'[4],

– having regard to the letter of response by the WP29 of 11 April 2018 on the reauthorisation of Section 702 of the US Foreign Intelligence Surveillance Act (FISA),

– having regard to its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield[5],

– 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 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 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 only, law enforcement, national security and

---

1 OJ C 257, 15.7.2016, p. 8.

2 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

3 http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

4 WP 255 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621

5 Text adopted, P8_TA(2017)0131.

respect for fundamental rights;

C. whereas transfers of personal data between EU and US commercial organisations are an important element of transatlantic relations in light of the ever-increasing digitisation of the global economy; 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 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;

E. whereas in its Opinion 4/2016 the EDPS raised several concerns regarding the draft Privacy Shield; whereas in this same opinion the EDPS welcomes 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;

F. whereas in its Opinion 01/2016 on the EU-US Privacy Shield draft adequacy implementing decision the WP29 welcomed the improvements brought about by the Privacy Shield compared with the Safe Harbour decision while also raising strong concerns about both the commercial aspects and access by public authorities to data transferred under the Privacy Shield;

G. 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;

H. whereas the EU-US Privacy Shield is accompanied by several unilateral commitments and assurances 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;

I. whereas in its statement of 26 July 2016, the WP29 welcomes the improvements brought by the EU-US Privacy Shield mechanism compared to the Safe Harbour and commended the Commission and the US authorities for having taken into consideration its concerns; whereas the WP29 nevertheless indicates 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, or the lack of concrete assurances of not conducting mass and indiscriminate collection of personal data (bulk collection);

J. whereas in its resolution of 6 April 2017, the Parliament, while acknowledging that the EU-US Privacy Shield contains significant improvements regarding the clarity of standards compared to the former EU-US Safe Harbour, also considers that important issues remain as regards certain commercial aspects, national security and law enforcement; whereas it calls on the Commission to conduct, during the first joint annual review, a thorough and in-depth examination of all the shortcomings and

weaknesses and to demonstrate how these 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;

K. whereas the report from the Commission to the Parliament and the Council on the first annual review on the functioning of the EU-US Privacy Shield and the Commission Staff Working Paper accompanying this document, while acknowledging that the US authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield and concluding that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield, have made ten recommendations to the US authorities in order to address issues of concern regarding not only the tasks and activities of the US Department of Commerce (DoC) as administrator responsible for the monitoring of the certification of Privacy Shield organisations and enforcement of the Principles, but also those issues related to national security, such as the re-authorisation of Section 702 of FISA, or the appointment of a permanent Ombudsperson and the fact that members of the Privacy Civil Liberties Oversight Board (PCLOB) are still not in office;

L. whereas the opinion of the WP29 of 28 November 2017 entitled 'EU-US Privacy Shield – First Annual Joint Review', following the first annual joint review, acknowledges the progress of the Privacy Shield in comparison with the invalidated Safe Harbour Decision; whereas the WP29 recognises the efforts made by the US authorities and the Commission to implement the Privacy Shield;

M. whereas the WP29 has identified a number of important unresolved issues of significant concern, regarding both the commercial issues and those relating to access by the US public authorities to data transferred to the US under the Privacy Shield (either for law enforcement or national security purposes) that need to be addressed by both the Commission and the US authorities; whereas it has requested that an action plan be set up immediately to demonstrate that all these concerns will be addressed, and at the latest at the second joint review;

N. whereas, in the event of no remedy being brought to the concerns of the WP29 within the given timeframes, the members of the WP29 will take appropriate action, including bringing the Privacy Shield adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling;

O. whereas an action for annulment (Case T-738/16 *La Quadrature du Net and Others* v *Commission*) and a referral by the Irish High Court in the case between the Data Protection Commissioner of Ireland and Facebook Ireland Limited and Maximilian Schrems (*Schrems II* case) have been brought before the CJEU; whereas the referral takes note that mass surveillance is still going on and analyses whether there is effective remedy in US law for EU citizens whose personal data is transferred to the United States;

P. whereas on 11 January 2018 the US Congress reauthorised and amended Section 702 of FISA for six years without addressing the concerns of the Commission joint review report and the opinion of the WP29;

Q. whereas, as part of the omnibus budget legislation signed into law on 23 March 2018,

the US Congress enacted the Clarifying Overseas Use of Data (CLOUD) Act, which facilitates law enforcement access to the contents of communications and other related data by allowing US law enforcement authorities to compel production of communications data even if they are stored outside the United States, and by allowing certain foreign countries to enter into executive agreements with the United States in order to permit US service providers to respond to certain foreign orders seeking access to communications data;

R. whereas Facebook Inc., Cambridge Analytica and SCL Elections Ltd are companies certified within the Privacy Shield framework and as such benefited from the adequacy decision as a legal ground for the transfer and further processing of personal data from the European Union to the United States;

S. whereas, as per Article 45(5) GDPR, where available information reveals that a third country no longer ensures an adequate level of protection, the Commission shall repeal, amend or suspend its adequacy decision;

1. Highlights the persisting weaknesses of the Privacy Shield as regards the respect of fundamental rights of data subjects; underlines the increasing risk that the CJEU may invalidate Commission Implementing Decision (EU) 2016/1250 on the Privacy Shield;

2. Takes note of the improvements compared to the Safe Harbour agreement, including the insertion of key definitions, stricter obligations related to data retention and onward transfers to third countries, the creation of an Ombudsperson to ensure individual redress and independent oversight, checks and balances ensuring the rights of data subjects (PCLOB), external and internal compliance reviews, more regular and rigorous documentation and monitoring, the availability of several ways to pursue legal remedy, and the prominent role for national data protection authorities in the investigation of claims;

3. Recalls that the WP29 set a deadline of 25 May 2018 to solve the outstanding issues, failing which it might decide to bring the Privacy Shield to national courts in order for them to refer the matter to the CJEU for preliminary ruling[1];

Institutional issues / Nominations

4. Regrets that it has taken so long to designate the two additional Members coupled with the nomination of the Chairman of the PCLOB and urges the Senate to scrutinise their profiles in order to ratify the designation so as to restore the independent agency to quorum status and enable it to fulfil its missions of preventing terrorism and ensuring the need to protect privacy and civil liberties;

5. Expresses its concern that the absence of a chair and a quorum has limited the PCLOB's ability to act and to fulfil its obligations; highlights that during a sub-quorum period the PCLOB may not initiate new advice or oversight projects, or hire staff; recalls that the PCLOB has not yet issued its long-awaited report on the conduct of surveillance under Executive Order 12333 to provide information on the concrete operation of this Executive Order and on its necessity and proportionality with regard to interferences brought to data protection in this context; notes that this report is highly desirable

---

1 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

considering the uncertainty and unforeseeability of how Executive Order 12333 is used; regrets that the PCLOB did not issue a new report on Section 702 FISA before it was reauthorised in January 2018; considers that the sub-quorum status seriously undermines the compliance and oversight guarantees and assurances made by the US authorities; urges the US authorities, therefore, to nominate and confirm new Board Members without delay;

6. In light of the fact that Presidential Policy Directive 28 (PPD 28) is one of the central elements on which the Privacy Shield is built, calls for the release of the PCLOB report on PPD 28, which is still subject to Presidential privilege and has thus not yet been published;

7. Reiterates its position 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 carry out its tasks and provide effective redress to EU citizens; stresses that the exact powers of the Ombudsperson mechanism need to be clarified, especially with regard to his/her powers vis-à-vis the intelligence community and the level of effective remedy of his/her decisions; regrets that the Ombudsperson can only request action by and information from US governmental bodies, and cannot order the authorities to cease and discontinue unlawful surveillance, or to permanently destroy information; points out that, while there is an acting Ombudsperson, to date the US administration has still not appointed a new permanent Ombudsman, which does not contribute to mutual trust; takes the view that in the absence of an appointed independent, experienced and sufficiently empowered Ombudsperson, the US assurances with regard to the provision of effective redress to EU citizens would be null and void;

8. Acknowledges the recent confirmation by the Senate of a new Federal Trade Commission (FTC) Chairman and four FTC Commissioners; deplores that until said confirmation four of the five FTC seats had remained vacant, considering that the FTC is the competent agency for enforcement of the Privacy Shield principles by US organisations;

9. Stresses 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; calls on the competent EU data protection authorities to take appropriate action and suspend transfers in cases of non-compliance;

Commercial issues

10. Considers that in order to ensure transparency and avoid false certification claims, the DoC should not tolerate US companies making public representations about their Privacy Shield certification before it has finalised the certification process and has included them on the Privacy Shield list; is concerned by the fact that the DoC has not made use of the possibility provided in the Privacy Shield to request copies of the contractual terms used by certified companies in their contracts with third parties to ensure compliance; considers therefore that there is no effective control over whether certified companies actually comply with the Privacy Shield provisions; calls on the DoC to undertake proactively and on a regular basis *ex officio* compliance reviews to monitor the effective compliance of companies with the Privacy Shield rules and

requirements;

11. Considers that the various recourse procedures for EU citizens may prove to be too complex, difficult to use, and therefore less effective; notes that, as underlined by the companies providing independent recourse mechanisms (IRMs), most of the complaints are brought directly to the companies by individuals seeking general information on the Privacy Shield and the processing of their data; recommends therefore that the US authorities offer more concrete information on the Privacy Shield website in an accessible and easily understandable form to individuals regarding their rights and available recourses and remedies;

12. In view of the recent revelations of misuse of personal data by companies certified under the Privacy Shield, such as Facebook and Cambridge Analytica, calls on the US authorities responsible for enforcing the Privacy Shield to act upon such revelations without delay in full compliance with the assurances and commitments given to uphold the current Privacy Shield arrangement and, if needed, to remove such companies from the Privacy Shield list; calls also on the competent EU data protection authorities to investigate such revelations and, if appropriate, suspend or prohibit data transfers under the Privacy Shield; considers that the revelations clearly show that the Privacy Shield mechanism does not provide adequate protection of the right to data protection;

13. Is seriously concerned about the change in the terms of service of Facebook for non-EU users outside the United States and Canada who have so far enjoyed rights under EU data protection law, and who now have to accept Facebook US instead of Facebook Ireland as the data controller; considers that this constitutes a transfer of personal data of approximately 1,5 billion users to a third country; seriously doubts that such an unprecedented large-scale limitation of the fundamental rights of users of a de-facto monopoly platform is what was intended with the Privacy Shield; calls on EU data protection authorities to investigate this matter;

14. Expresses its strong concern that, if the issue is not tackled, such misuses of personal data by various entities that aim to manipulate political opinion or voting behaviour can pose a threat to the democratic process and its underlying idea that voters are able to make informed, fact-based decisions for themselves;

15. Welcomes and supports calls for the US legislator to move towards an omnibus privacy and data protection act;

16. Recalls its 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; acknowledges the intention of the Commission to order a study to collect factual evidence and further assess the relevance of automated decision-making for data transfers under the Privacy Shield; calls on the Commission to provide for specific rules concerning automated decision-making to provide sufficient safeguards if the study recommends this; takes note in this regard of the information provided from the joint review that automated decision-making may not take place on the basis of personal data that have been transferred under the Privacy Shield; deplores that, according to the WP29, ‘the feedback from the companies remained very general, leaving unclear whether these assertions correspond to the reality of all companies adhering to the Privacy Shield’; further stresses the applicability of the GDPR under the conditions of Article 3(2) GDPR;

17. Stresses that further improvements should be made with regard to the interpretation and handling of HR data due to the different reading of the notion 'HR data' by the US Government on the one hand and the Commission and the WP29 on the other; agrees fully with the WP29's call on the Commission to engage in negotiations with the US authorities in order to amend the Privacy Shield mechanism on this issue;

18. Reiterates its concern that the 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; urges therefore, in the light of the joint review, that the DoC work with European Data Protection Authorities to provide more precise guidance as regards essential principles of the Privacy Shield such as the Choice Principle, the Notice Principle, onward transfers, the controller-processor relationship and access, which are much more aligned with the rights of the data subject under Regulation (EU) 2016/679;

19. Reiterates its concerns about 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; considers that this is yet another threat to privacy safeguards in the United States;

Law Enforcement and National Security issues

20. Considers that the term 'national security' in the Privacy Shield mechanism 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; calls therefore for a clear definition of 'national security';

21. Takes note that the number of targets under Section 702 of FISA has increased due to changes in technology and communication patterns as well as an evolving threat environment;

22. Regrets that the US did not seize the opportunity of the recent reauthorisation of FISA Section 702 to include the safeguards provided in PPD 28; calls 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; takes note of the Commission's explanation in its Staff Working Document that surveillance under Section 702 FISA is always based on selectors and does not therefore allow for bulk collection; adds its voice therefore to the call made by the WP29 for an updated report from the PCLOB on the definition of 'targets', on the 'tasking of selectors' and on the concrete process of applying the selectors in the context of the UPSTREAM programme to clarify and assess whether bulk access to personal data occurs in that context; deplores that EU individuals are excluded from the additional protection provided by the reauthorisation of FISA Section 702; regrets that the reauthorisation of Section 702 contains several amendments that are merely procedural and do not address the most problematic issues, as also raised by the WP29; calls on the Commission to take the forthcoming WP29 analysis on FISA Section 702 seriously and to act accordingly;

23. Affirms that the reauthorisation of section 702 of the FISA act for six more years calls

into question the legality of the Privacy Shield;

24. Reiterates its concerns about Executive Order 12333, which allows 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; regrets the lack of any judicial review of surveillance activities conducted on the basis of Executive Order 12333;

25. Highlight the persisting obstacles concerning redress for non-US citizens subject to a surveillance measure based on section 702 FISA or Executive Order 12333 due to the procedural requirements of 'standing' as currently interpreted by the US courts, in order to enable non-US citizens to bring legal actions before US courts against decisions affecting them;

26. Expresses its concern about the consequences of Executive Order 13768 on 'Enhancing Public Safety in the Interior of the United States' for judicial and administrative remedies available to individuals in the US, because the protections of the Privacy Act no longer apply to non-US citizens; takes note of the Commission's position that the adequacy assessment does not rely on the protections of the Privacy Act and that therefore this Executive Order does not affect the Privacy Shield; considers that Executive Order 13768 does however indicate 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;

27. Expresses its strong concerns regarding the recent adoption of the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943), which expands the abilities of American and foreign law enforcement to target and access people's data across international borders without making use of the mutual legal assistance treaty (MLAT) instruments, which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located; highlights that the CLOUD Act could have serious implications for the EU as it is far-reaching and creates a potential conflict with the EU data protection laws;

28. Considers that a more balanced solution would have been to strengthen the existing international system of MLATs with a view to encouraging international and judicial cooperation; reiterates that, as set out in Article 48 GDPR, mutual legal assistance and other international agreements are the preferred mechanism to enable access to personal data overseas;

29. Deplores that the US authorities have failed to proactively fulfil their commitment to provide the Commission with timely and comprehensive information about any developments that could be of relevance for the Privacy Shield, including the failure to notify the Commission of changes in the US legal framework, for example with respect to President Trump's Executive Order 13768 'Enhancing Public Safety in the Interior of the United States' or the repeal of the privacy rules for internet service providers;

30. Recalls that, as indicated in its resolution of 6 April 2017, neither the Privacy Shield Principles nor the letters from the US administration provide clarifications and assurances demonstrating the existence of effective judicial redress rights for individuals in the EU in respect of use of their personal data by US 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;

Conclusions

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 25 May 2018, and with the EU Charter, so that adequacy should not lead to loopholes or competitive advantage for US companies;

32. Deplores that the Commission and the competent US authorities did not restart discussions on the Privacy Shield arrangement and did not set up any action plan in order to address as soon as possible the deficiencies identified, as called for by the WP29 in its December report on the joint review; calls on the Commission and the competent US authorities to do so without any further delay;

33. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the EU Charter and the European Convention of Human Rights, as well as in laws and case law; emphasises that they must be applied in a manner that does not unnecessarily hamper trade or international relations, but cannot be 'balanced' against commercial or political interests;

34. Takes 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 CJEU;

35. Considers that, unless the US is fully compliant by 1 September 2018, the Commission has failed to act in accordance with Article 45(5) GDPR; calls therefore on the Commission to suspend the Privacy Shield until the US authorities comply with its terms;

36. Instructs its Committee on Civil Liberties, Justice and Home Affairs to continue to monitor developments in this field, including on cases brought before the CJEU, and to monitor the follow-up to the recommendations made in the resolution;

o

o o

37. Instruct its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States and the Council of Europe.