C/2023/1073

15.12.2023

P9_TA(2023)0204

Adequacy of the protection afforded by the EU-U.S. Data Privacy Framework

European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))

(C/2023/1073)

The European Parliament,

— having regard to the Charter of Fundamental Rights of the European Union ('the Charter'), in particular Articles 7, 8, 16, 47 and 52 thereof,

— having regard to the judgment of the Court of Justice of the European Union (CJEU) of 6 October 2015 in Case C-362/14 *Maximillian Schrems* v *Data Protection Commissioner* (Schrems I) ([1]),

— having regard to the judgment of the CJEU of 16 July 2020 in Case C-311/18 *Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems* (Schrems II) ([2]),

— having regard to its inquiry into the revelations made by Edward Snowden on the electronic mass surveillance of EU citizens, including the findings in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs ([3]),

— having regard to its resolution of 26 May 2016 on transatlantic data flows ([4]),

— 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 its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield ([6]),

— having regard to its resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — *Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems* (Schrems II), Case C-311/18 ([7]),

— having regard to the Commission draft implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework,

— having regard to the President of the United States' Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence Activities,

— having regard to the President of the United States' Executive Order 12333 of 4 December 1981 on United States intelligence activities,

— having regard to the Regulation on the Data Protection Review Court issued by the US Attorney General (AG Regulation),

([1]) Judgment of 6 October 2015, *Maximilian Schrems* v *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
([2]) Judgment of 16 July 2020, *Data Protection Commissioner* v *Facebook Ireland Limited and Maximilian Schrems*, C-311/18, ECLI:EU:C:2020:559.
([3]) OJ C 378, 9.11.2017, p. 104.
([4]) OJ C 76, 28.2.2018, p. 82.
([5]) OJ C 298, 23.8.2018, p. 73.
([6]) OJ C 118, 8.4.2020, p. 133.
([7]) OJ C 15, 12.1.2022, p. 176.

— 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) ([8]), in particular Chapter V thereof,

— having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ([9]),

— having regard to the Adequacy Referential of the Article 29 Working Party (WP 254 rev.01) as endorsed by the European Data Protection Board (EDPB), having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and to the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,

— having regard to European Data Protection Board opinion 5/2023 of 28 February 2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework,

— having regard to Rule 132(2) of its Rules of Procedure,

A. whereas in the 'Schrems I' judgment, the CJEU overturned the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce ([10]), and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to the confidentiality of communications provided for in Article 7 of the Charter; whereas the Court pointed out that, for the purposes of an adequacy decision, a third country does not have to ensure an identical, but rather an 'essentially equivalent' level of protection to that guaranteed in EU law, which may be ensured through different means;

B. whereas in the 'Schrems II' judgment, the CJEU overturned Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-US Privacy Shield ([11]) and concluded that it did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter;

C. whereas on 7 October 2022, the President of the United States of America signed Executive Order 14086 on Enhancing Safeguards For United States Signals Intelligence Activities (EO 14086);

D. whereas on 13 December 2022 the Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework;

E. 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; whereas, if such an assessment were to be found unsatisfactory in terms of adequacy and equivalence, the Commission should refrain from adopting an adequacy decision since it is conditional upon implementation of relevant guarantees; whereas the Commission is obliged to suspend the adequacy when there is no longer equivalence; whereas the General Data Protection Regulation (GDPR) requires that relevant assessment should be a continuous process taking into account changes to applicable rules and practices;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness as long as adequate safeguards are provided; whereas these transfers should be carried out with full respect for the right to the protection of personal data and the right to privacy; whereas one of the aims of the EU is the protection of fundamental rights, as enshrined in the Charter;

([8]) OJ L 119, 4.5.2016, p. 1.
([9]) OJ L 201, 31.7.2002, p. 37.
([10]) OJ L 215, 25.8.2000, p. 7.
([11]) OJ L 207, 1.8.2016, p. 1.

G. whereas the GDPR applies to all companies processing the personal data of data subjects in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as their behaviour takes place within the Union;

H. whereas mass surveillance, i.e., the indiscriminate collection of data without any safeguards to limit intrusions on individuals' privacy, by state actors is detrimental to the trust of European citizens' and businesses' trust in digital services and, by extension, in the digital economy; whereas while US agencies are prohibited from collecting the bulk data of US citizens living in the United States, this prohibition does not apply to EU citizens; whereas mass surveillance by state actors is illegal and impacts negatively affects the trust of EU citizens and businesses in digital services and, by extension, in the digital economy;

I. whereas controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, purposes and risks for data subjects;

J. whereas there is no federal privacy and data protection legislation in the United States; whereas EO 14086 introduces definitions of key data protection concepts such as principles of necessity and proportionality, constituting a significant step forward in comparison with previous transfer mechanisms; whereas the way these principles are interpreted requires close monitoring; whereas a comprehensive assessment of how these principles are implemented in the US legal order might not be possible due to a lack of transparency in Data Protection Review Court (DPRC) procedures;

1. Recalls that respect for private and family life and the protection of personal data are legally enforceable fundamental rights enshrined in the Treaties, the Charter and the European Convention on Human Rights, as well as in laws and case-law; emphasises that adequacy decisions under the GDPR are legal decisions, not political choices and that the rights to privacy and data protection cannot be balanced against commercial or political interests but only against other fundamental rights;

2. Takes note of the efforts made in the EO 14086 to lay down limits on US signals intelligence activities by making the principles of proportionality and necessity apply to the US legal framework on signals intelligence, and providing a list of legitimate objectives for such activities; notes that these principles would be binding on the entire US intelligence community and could be invoked by data subjects within the procedure envisaged in EO 14086; stresses that this executive order provides for significant improvements aimed at ensuring that these principles are essentially equivalent under EU law; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in EO 14086 are not in line with their definition under EU law and their interpretation by the CJEU; points out, furthermore, that for the purposes of the EU-US Data Privacy Framework, these principles would be interpreted solely in the light of US law and legal traditions and not those of the EU; notes that EO 14086 lists 12 legitimate objectives that may be pursued when conducting signals intelligence collection and five objectives for which signals intelligence collection is prohibited; notes that the list of legitimate national security objectives can be amended and expanded by the US President with no obligation to make the relevant updates public nor to inform the EU; points out that EO 14086 requires that signals intelligence must be conducted in a manner necessary and proportionate to the 'validated intelligence priority', which appears to be a broad interpretation of these concepts; stresses that for a comprehensive assessment of principles of proportionality and necessity in the context of EO 14086 , they would have to be operationalised and implemented in the policies and procedures of US intelligence agencies; is concerned, however, that it is not a requirement that analysts conduct a proportionality assessment for each surveillance decision;

3. Notes that EO 14086 allows the bulk collection of data by signals intelligence in certain cases, including the content of communications; at the same time takes note that EO 14086 provides that targeted collection should be prioritised over bulk collection; recalls that, while EO 14086 contains several safeguards in case of bulk collection, it does not provide for independent prior authorisation for bulk collection, which is also not envisaged under Executive Order 12333; recalls that in Schrems II, the CJEU explained that US surveillance failed to satisfy EU law because it failed to require an 'objective criterion' 'capable of justifying' the government interference with privacy; points out that this would undermine the

purpose of the objectives as a safeguard to limit US intelligence activities; recalls that after Presidential Policy Directive 28 (PPD-28), which formed the basis for the 'Privacy Shield' adequacy decision, the Privacy and Civil Liberties Oversight Board (PCLOB) issued a review report ([12]) and concluded that PPD-28 had essentially maintained the existing practices of the intelligence community; is convinced that PPD-28 will not stop electronic mass surveillance of EU citizens by US authorities;

4. Shares the EDPB's concerns over EO 14086'sfailure to provide sufficient safeguards in the case of bulk data collection, namely the lack of independent prior authorisation, lack of clear and strict data retention rules, 'temporary' bulk collection, and lack of stricter safeguards concerning dissemination of data collected in bulk; points particularly to the specific concern that without further restrictions on dissemination to US authorities, law enforcement authorities would be able to access data they would otherwise have been prohibited from accessing; recalls that onward transfers effectively multiply the risks to the protection of data; notes that the EDPB has called for the inclusion of a legally binding obligation to analyse and determine whether a third country offers an acceptable minimum level of safeguards;

5. Points out that EO 14086 does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements;

6. Points out that the underlying problem is the surveillance of non-US persons under US law, and the inability of European citizens to seek effective judicial redress in this regard; requests that EU citizens should have the same rights and privileges as US citizens, when it comes to the activities of the US intelligence community and access to US courts;

7. Notes that, in line with the US interpretation, 'signals intelligence' covers all data access methods provided for in the Foreign Intelligence Surveillance Act (FISA), including from 'remote computing service' providers added with the FISA amendment Act S1881a in 2008; calls on the Commission to clarify in future negotiations the definition and scope of 'signals intelligence' in EO 14086; recalls that under FISA Section 702, the US Government still claims the power to target any non-US person abroad to obtain foreign intelligence, broadly defined;

8. Points out that a new redress mechanism has been created allowing EU data subjects to lodge a complaint; at the same time stresses that the decisions of the DPRC would be classified and not made public or available to the complainant, who would only be informed that the review either did not identify any covered violations or that the DPRC had issued a determination requiring appropriate action, thereby undermining their right to access or rectify their data; is concerned that this means that a person bringing a case would have no chance of being informed about the substantive outcome of the case and the decision would be final; notes that the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any possibility for the complainant to claim damages; calls on the Commission to continue negotiations with the United States to achieve the necessary changes to address these concerns;

9. Notes that EO 14086 introduces some guarantees to ensure the independence of DPRC judges, as recognised by the EDPB in its opinion; points out that the DPRC is part of the executive branch and not the judiciary and its judges are appointed for a fixed term of four years; highlights that the US President can overrule DPRC decisions even in secret; points out that although the new redress mechanism does not allow for the US Attorney General to dismiss and supervise the DPRC judges, it does not affect the relevant powers of the US President; stresses that as long as the US President can remove DPRC judges during their term, the independence of these judges is not guaranteed; notes that if adopted, the Commission would have to closely monitor the application of safeguards to ensure independence in practice; points out that a complainant would be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence; calls on the Commission to ensure an independence requirement is introduced in the event an adequacy decision is adopted; concludes that, as it stands, the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter; notes that while PCLOB would independently review the functioning of the new redress process, the scope of this review would be limited;

([12]) PCLOB, *Report to the President on the Implementation of Presidential Directive 28: Signals Intelligence Activities*.

10. Notes that the United States has provided for a new remedy mechanism for issues related to public authorities' access to data, but that questions remain about the effectiveness of the remedies available for commercial matters, which are unchanged under the adequacy decision; notes that the mechanisms aimed at resolving these issues are largely left to the discretion of companies, which can select alternative remedy avenues such as dispute resolution mechanisms or the use of companies' privacy programmes; calls on the Commission, if an adequacy decision is adopted, to closely analyse the effectiveness of these redress mechanisms;

11. Notes that European businesses need and deserve legal certainty; stresses that the succession of data transfer mechanisms, which have subsequently been repealed by the CJEU, has created additional costs for European businesses; acknowledges, therefore, the need to ensure legal certainty and avoid a situation where businesses constantly need to adapt to new legal solutions, which might be particularly burdensome for micro, small and medium-sized enterprises; is concerned that the adequacy decision, if adopted, could (like its predecessors) be invalidated by the CJEU, leading to a continuing lack of legal certainty, further costs and disruption for European citizens and businesses;

12. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the United States still lacks a federal data protection law; points out that the application of EO 14086 is not clear, precise or foreseeable in its application, as it can be amended or revoked at any time by the US President, who is also empowered to issue secret executive orders; notes that the review of the adequacy finding would take place after one year from the date of the notification of the adequacy decision to the Member States and subsequently at least every four years; calls on the Commission, in the event that any future adequacy decision is adopted, to carry out subsequent reviews at least every three years, as requested by the EDPB opinion; is concerned about the absence of a sunset clause such that the decision would automatically expire four years after its entry into force, after which the Commission would have to make a new determination; is concerned that this lack of a sunset clause in this adequacy decision represents a more lenient approach to the United States, even though the US privacy framework is based on an executive order that allows for secret amendments, and which can be amended without either the approval of Congress or informing EU counterparts; therefore calls on the Commission to introduce such a clause;

13. Shares the concerns expressed by the EDPB regarding the rights of data subjects, the absence of key definitions and specific rules on automated decision-making and profiling, the lack of clarity about the application of the Data Privacy Framework principles to processors and the need to avoid onward transfers undermining the level of protection;

14. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof or repealed or amended as necessary, and that EU citizens' fundamental right to data protection is guaranteed at all times; underlines that any future adequacy decision should be subject to continuous review, taking into account legal and practical developments in the US;

Conclusions

15. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt a new adequacy decision in relation to the United States unless meaningful reforms were introduced, in particular for national security and intelligence purposes; does not consider the EO 14086 to be sufficiently meaningful; reiterates that the Commission should not leave the task of protecting the fundamental rights of EU citizens to the Court of Justice of the European Union following complaints from such individual citizens;

16. Recalls that the Commission must assess the adequacy of a third country based on legislation and practices in place not only in substance but also in practice as established under Schrems I, Schrems II cases and the GDPR (recital 104);

17. Notes that the Data Privacy Framework principles issued by the US Department of Commerce have not been sufficiently amended, in comparison to those under the Privacy Shield, to provide essentially equivalent protection to that provided under the GDPR;

18. Notes that while the United States is making an important commitment to improve access to remedies and rules on data processing by public authorities, the US Intelligence Community has until October 2023 to update its policies and practices in line with the commitment of the EO 14086 and that the US Advocate General has yet to name the EU and its Member States as qualifying countries to be eligible to access the remedy avenue available under the DPRC; underlines that

this means that the Commission was not in position to assess the effectiveness of the proposed remedies and proposed measures on access to data 'in practice'; concludes, therefore, that the Commission can only proceed with the next step of an adequacy decision once these deadlines and milestones have first been completed by the United States to ensure that the commitments have been delivered in practice;

19. Concludes that the EU-US Data Privacy Framework fails to create essential equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; calls on the Commission not to adopt the adequacy finding until all the recommendations made in this resolution and the EDPB opinion are fully implemented;

20. Calls on the Commission to act in the interest of EU businesses and citizens by ensuring that the proposed framework provides a solid, sufficient and future-oriented legal basis for EU-US data transfers; expects any adequacy decision, if adopted, to be challenged before the CJEU; highlights the Commission's responsibility for failure to protect EU citizens rights in the scenario where the adequacy decision is again invalidated by the CJEU;

o

o o

21. Instructs its President to forward this resolution to the Council, the Commission and the President and Congress of the United States of America.