European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

2023/2501(RSP)

14.2.2023

DRAFT MOTION FOR A RESOLUTION

to wind up the debate on the statement by the Commission

pursuant to Rule 132(2) of the Rules of Procedure

on the adequacy of the protection afforded by the EU-US Data Privacy Framework
(2023/2501(RSP))

Juan Fernando López Aguilar
on behalf of the Committee on Civil Liberties, Justice and Home Affairs

B9-0000/2023

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

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 6 October 2015 in Case C-362/14 *Maximillian Schrems* v *Data Protection Commissioner* ('Schrems I')[1],

– having regard to the judgment of the Court of Justice 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 enquiry 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 President of the United States' Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence

[1] Judgment of 6 October 2015, *Maximilian Schrems* v *Data Protection Commissioner*, C-362/14, EU:C:2015:650.
[2] Judgment of 16 July 2020, *Data Protection Commissioner* v *Facebook Ireland Limited and Maximilian Schrems*, C-311/18, 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.

Activities,

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

– 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 ('GDPR')[8], in particular Chapter V thereof,

– having regard to the Commission proposal of 10 January 2017 for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010), to the decision to enter into interinstitutional negotiations confirmed by Parliament's plenary on 25 October 2017, and to the Council's general approach adopted on 10 February 2021 (6087/21),

– having regard to the European Data Protection Board (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 the EDPB Opinion of [to be added],

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

A. whereas in the 'Schrems I' judgment, the Court of Justice of the European Union (CJEU) invalidated the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 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[9], and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7 of the Charter;

B. whereas in the 'Schrems II' judgment, the CJEU invalidated 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-U.S. Privacy Shield[10] 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

[8] OJ L 119, 4.5.2016, p. 1.
[9] OJ L 215, 25.8.2000, p. 7.
[10] OJ L 207, 1.8.2016, p. 1.

Activities (‘EO’);

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;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas these transfers should be carried out in full respect for 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 Charter;

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, including the bulk collection of data, by state actors is detrimental to the trust of European 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 (US); whereas the EU and the US have differing definitions of key data protection concepts such as principles of necessity and proportionality;

1. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the 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 can be balanced only against other fundamental rights and not against commercial or political interests;

2. Acknowledges the efforts made in the EO to lay down limits on US Signals Intelligence Activities, by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in the EO 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 will be interpreted solely in the light of US law and legal traditions; points out that the EO requires that signals intelligence must be conducted in a manner proportionate to the ‘validated intelligence priority’, which appears to be a broad interpretation of proportionality;

3. Regrets the fact that the EO does not prohibit the bulk collection of data by signals

intelligence, including the content of communications; notes that the list of legitimate national security objectives can be expanded by the US President, who can determine not to make the relevant updates public;

4. Points out that the EO 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;

5. Points out that the decisions of the Data Protection Review Court ('DPRC') will be classified and not made public or available to the complainant; points out that the DPRC is part of the executive branch and not the judiciary; points out that a complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence; points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; 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; concludes that the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter;

6. Notes that, while the US has provided for a new mechanism for remedy for issues related to public authorities' access to data, the remedies available for commercial matters under the adequacy decision are insufficient; notes that 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;

7. Notes that European businesses need and deserve legal certainty; stresses that successive data transfer mechanisms, which were subsequently repealed by the CJEU, created additional costs for European businesses; notes that continuing uncertainty and the need to adapt to new legal solutions is particularly burdensome for micro, small and medium-sized enterprises;

8. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law; points out that the EO is not clear, precise or foreseeable in its application, as it can be amended at any time by the US President; is therefore concerned about the absence of a sunset clause which could provide that the decision would automatically expire four years after its entry into force;

9. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof and that EU citizens' fundamental right to data protection is guaranteed;

Conclusions

10. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms were introduced, in particular for national security and intelligence purposes;

11. Concludes that the EU-US Data Privacy Framework fails to create actual 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; urges the Commission not to adopt the adequacy finding;

°

° °

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