



2021/2594(RSP)

6.4.2021

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 adequate protection of personal data by the United Kingdom
(2021/2594(RSP))

Juan Fernando López Aguilar

on behalf of the Committee on Civil Liberties, Justice and Home Affairs

European Parliament resolution on the adequate protection of personal data by the United Kingdom (2021/2594(RSP))

The European Parliament,

- having regard to the Charter of Fundamental Rights of the European Union (the Charter), in particular Articles 7, 8, 47 and 52 thereof,
- having regard to the judgment of the Court of Justice of the European Union (CJEU) of 16 July 2020 in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Schrems II judgment)¹,
- having regard to the judgment of the CJEU of 6 October 2015 in case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (Schrems I judgment)²,
- having regard to the judgment of the CJEU of 6 October 2020 in case C-623/17, *Privacy International v Secretary of State of Foreign and Commonwealth affairs*³,
- having regard to 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 Affairs⁴,
- having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield⁵,
- having regard to its resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection⁶,
- having regard to its resolution of 26 November 2020 on the EU Trade Policy Review⁷,
- having regard to the Trade and Cooperation Agreement of 31 December 2020 between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part⁸,
- having regard to its resolution of XX.XX.2021 on the EU-UK Trade and Cooperation Agreement,
- having regard to Regulation (EU) 2016/679 of the European Parliament and of the

¹ ECLI:EU:C:2020:559.

² ECLI:EU:C:2015:650.

³ ECLI:EU:C:2020:790.

⁴ OJ C 378, 9.11.2017, p. 104.

⁵ OJ C 118, 8.4.2020, p. 133.

⁶ OJ C 345, 16.10.2020, p. 58.

⁷ Texts adopted, P9_TA(2020)0337.

⁸ OJ L 444, 31.12.2020, p. 14.

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 (the General Data Protection Regulation – GDPR)⁹,

- having regard 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 (the Law Enforcement Directive for Data Protection)¹⁰,
- 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 (Directive on privacy and electronic communications)¹¹,
- 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) and the European Parliament’s position thereon adopted on 20 October 2017¹²,
- having regard to the recommendations of the European Data Protection Board (EDPB), including its statement of 9 March 2021 on the ePrivacy Regulation and its recommendations 01/2020 of 10 November 2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,
- having regard to the adequacy referential adopted by the Article 29 Data Protection Working Party on 6 February 2018 and endorsed by the EDPB,
- having regard to EDPB recommendations 01/2021 of 2 February 2021 on the adequacy referential under the Law Enforcement Directive for Data Protection,
- having regard to the draft adequacy decisions published by the Commission on 19 February 2021, one pursuant to the GDPR¹³ and the other pursuant to the Law Enforcement Directive for Data Protection¹⁴,
- having regard to the EDPB opinion of XXXX on the draft adequacy decisions for the UK,
- having regard to Rule 132(2) of its Rules of Procedure,

⁹ OJ L 119, 4.5.2016, p. 1.

¹⁰ OJ L 119, 4.5.2016, p. 89.

¹¹ OJ L 201, 31.7.2002, p. 37.

¹² [A8-0324/2017](#).

¹³ Draft Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

¹⁴ Draft Commission implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

- having regard to the motion for a resolution of the Committee on Civil Liberties, Justice and Home Affairs,
- A. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness;
- B. whereas in its Schrems I judgment, the CJEU pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates Article 7 of the Charter, and that the United States do not provide sufficient legal remedies for non-US persons against mass surveillance, in violation of Article 47 of the Charter;

I. GENERAL DATA PROTECTION REGULATION

General observations

1. Notes that the UK is a signatory to the European Convention on Human Rights (ECHR) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; expects the UK to ensure the same minimum framework of data protection, despite having left the European Union;
2. Welcomes the UK's commitment to respect democracy and the rule of law, and protect and give domestic effect to fundamental rights such as those set out in the ECHR, including high levels of data protection; recalls that this is a necessary precondition for the EU's cooperation with the UK; recalls that despite Article 8 of the ECHR on the right to privacy being part of UK domestic law via the Human Rights Act 1998 and common law via the new tort of misuse of privacy information, efforts to include a fundamental right to data protection were voted down by the government;
3. Is concerned about public statements by the UK Prime Minister declaring that UK will seek to diverge from EU data protection rules and establish its own 'sovereign' controls in this field; considers that the 2020 UK National Data Strategy represents a shift from the protection of personal data towards a wider use and sharing of data that is incompatible with the principles of fairness, data minimisation and purpose limitation under the GDPR;

Enforcement of the GDPR

4. Expresses its concern about the lack and sometimes non-existent enforcement of the GDPR by the UK when it was still a member of the EU; points to the lack of proper enforcement by the UK Information Commissioner's Office in the past;

Data processing for immigration control

5. Is concerned that UK data protection law contains a broad derogation from aspects of the fundamental data protection principles, such as the right of access and the right of a data subject to know with whom their data has been shared, if such protection would 'prejudice effective immigration control'¹⁵; points out that this exemption is available to all data controllers in the UK; is concerned about the recently revealed information that

¹⁵ Schedule 2 of the Data Protection Act 2018.

the immigration exemption was used in over 70 % of data subject requests to the Home Office in 2020¹⁶;

6. Notes that this exception now applies to EU citizens who reside or plan to reside in the UK; is strongly concerned that the exemption removes key opportunities for accountability and remedies;
7. Points out that it has repeatedly voiced its concern about an exception for data subjects' rights in the UK's immigration policy, including in its resolution of 12 February 2020 on the new partnership with the UK¹⁷ and the opinion of the Committee on Civil Liberties, Justice and Home Affairs of February 2021, which held that the exemption for the processing of personal data for immigration purposes of the UK Data Protection Act needed to be amended before a valid adequacy decision could be reached¹⁸;

Mass surveillance

8. Recalls the revelations of mass surveillance by the US and the UK, as revealed by whistle-blower Edward Snowden; recalls that the UK 'Tempora' programme run by the Government Communications Headquarters (GCHQ) intercepts communications in real time through fibre-optical internet backbone cables, and records the data so it can be processed and searched at a later time;
9. Recalls its resolution of 12 March 2014, which found that the indiscriminate and non-suspicion-based mass surveillance programmes conducted by the UK intelligence agency GCHQ are incompatible with the principles of necessity and proportionality in a democratic society and are not adequate under EU data protection law;
10. Recalls that in September 2018, the European Court of Human Rights confirmed that the UK's mass data interception and retention programmes, including Tempora, were 'unlawful and incompatible with the conditions necessary for a democratic society'¹⁹;
11. Is concerned that the draft adequacy decisions fail to take into account either the actual use of UK bulk data powers or UK-US surveillance operations; points out that furthermore, in relation to the US, UK citizens are subject to some informal safeguards between GCHQ and the National Security Agency (NSA); expresses deep concern that these safeguards would not protect EU citizens or residents whose data may be subject to onward transfers and sharing with the NSA;

Onward Transfers

12. Takes note of the fact that the European Union (Withdrawal) Act 2018 provides that CJEU case law generated before the end of the transition period will become 'retained

¹⁶Open Rights Group press release of 3 March 2021 entitled 'Documents reveal controversial Immigration Exemption used in 70% of access requests to Home Office'.

¹⁷Texts adopted, P9_TA(2020)0033.

¹⁸Opinion of the Committee on Civil Liberties, Justice and Home Affairs on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information, LIBE_AL(2021)680848.

¹⁹Judgment of the European Court of Human Rights of 13 September 2018, *Big Brother Watch and others v the United Kingdom*, applications nos. 58170/13, 62322/14, 24960/15.

EU law’ and thus legally binding for the UK; points out that the UK is bound by the principles and conditions defined in the Schrems II judgment of the CJEU when assessing the adequacy of other non-EU countries; considers this an important safeguard to ensure the legality of onward transfers;

13. Points out that the UK rules on the sharing of personal data under the Digital Economy Act 2017 and on onward transfers of research data are clearly not ‘essentially equivalent’ to the rules set out in the GDPR, as interpreted by the CJEU;
14. Is strongly concerned that a UK adequacy status would therefore lead to the bypassing of the EU rules on transfers to countries or territories not deemed adequate under EU law;
15. Takes note that on 1 February 2021, the UK sent a request to join the Comprehensive and Progressive Trans-Pacific Partnership (CPTTP), in particular to ‘benefit from modern digital trade rules that allow data to flow freely between members, remove unnecessary barriers for businesses [etc.]’; notes with concern that there are eleven members of the CPTTP, eight of which do not have an adequacy decision from the EU; is strongly concerned about potential onward transfers of personal data from EU citizens and residents to these countries if the UK is granted an adequacy decision²⁰;
16. Is concerned that if the UK includes provisions on data transfers in any future trade agreements, inter alia US-UK trade agreements, the level of protection offered by the GDPR would be undermined;

II. Law Enforcement Directive for Data Protection

17. Highlights that the UK is the first country for which the Commission has suggested adopting an adequacy decision under Directive (EU) 2016/680; underlines that this is particularly important given the close partnership with the UK in the area of security and law enforcement;
18. Notes the UK’s cross-border data access agreement with the US²¹, under the US CLOUD Act, which facilitates transfers for law enforcement purposes; is concerned that this will allow undue access to the personal data of EU citizens and residents by US authorities;
19. Recalls that CJEU judgment C-623/17 must be interpreted as precluding national legislation enabling a state authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the state’s security and intelligence agencies for the purpose of safeguarding national security;
20. Notes that in this case, the CJEU ruled that the bulk data collection carried out in the UK under the Regulation of Investigatory Powers Act 2000 was illegal; points out that the regulation has since been replaced by the Investigatory Powers Act (the IPA 2016) in order to strengthen the principles of necessity and proportionality; underlines that the

²⁰ Source: <https://www.gov.uk/government/news/uk-applies-to-join-huge-pacific-free-trade-area-cpttp>

²¹ Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America of 3 October 2019 on Access to Electronic Data for the Purpose of Countering Serious Crime.

IPA 2016 makes interception subject to judicial oversight and empowers individuals to access their data and lodge complaints before the investigatory powers tribunal; deplores, however, the fact that the IPA 2016 continues to enable the practice of bulk data retention;

21. Is concerned about recent reports that a mass data collection and retention scheme is part of a trial by the UK Home Office conducted under the IPA 2016;
22. Is concerned about the shortcomings and violations identified in the way the UK implemented data protection law while it was still a member of the EU; recalls that the UK was recording and maintaining an illegal copy of the Schengen Information System; is therefore concerned about data being exchanged with UK law enforcement agencies, and about the UK maintaining access to EU law enforcement databases;
23. Notes that the draft adequacy decision fails to take account of the UK's actual surveillance practices and reflects an inaccurate and limited understanding of the types of communications data that fall under UK data retention and lawful interception powers;
24. Points out that the EU-UK Trade and Cooperation Agreement (TCA) includes titles regarding the exchange of DNA, fingerprints and vehicle registration data, the transfer and processing of passenger name record data (PNR), cooperation on operational information and cooperation with Europol and Eurojust, which will apply regardless of the adequacy decision; recalls, however, the concerns expressed in the opinion of the Committee on Civil Liberties, Justice and Home Affairs of February 2021 on the TCA regarding the special use and longer retention of personal data granted to the UK under the Prüm and PNR titles of the TCA, which are not in line with the uses and retentions by the Member States;

Conclusions

25. Calls on the Commission to assure EU businesses that the adequacy decision will provide a solid, sufficient and future-oriented legal basis for data transfers; underlines the importance of making sure that this adequacy decision will be deemed acceptable if reviewed by the CJEU and stresses that all recommendations made in the EDPB opinion should therefore be taken on board;
26. Welcomes the fact that the adequacy decision will be reviewed every four years and will include a sunset clause, and calls on the Commission to keep monitoring the level of data protection in the UK in law and practice in the meantime;
27. Calls for the Commission to consult with Parliament on any future changes to the UK data protection regime, and for a scrutiny role for Parliament in the new institutional framework, including for relevant bodies such as the Specialised Committee on Law Enforcement and Judicial Cooperation;

o

o o

28. Instructs its president to forward this resolution to the Commission, the Member States, and the Government of the UK.