European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2021)0262

The adequate protection of personal data by the United Kingdom

European Parliament resolution of 21 May 2021 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, 16, 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 Affairs[4],

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield[5],

– having regard to its resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection[6],

---

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.

– 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[1],

– having regard to its resolution of 26 November 2020 on the EU Trade Policy Review[2],

– 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 part[3],

– having regard to its resolution of 28 April 2021 on the outcome of EU-UK negotiations[4] ,

– 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 (General Data Protection Regulation)[5] (GDPR),

– 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[6] (the Law Enforcement Directive for Data Protection),

– 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[7],

– 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 (COM(2017)0010) and the European Parliament's position thereon adopted on 20 October 2017[8],

– 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,

---

1 Texts adopted, P9_TA(2021)0256.
2 Texts adopted, P9_TA(2020)0337.
3 OJ L 444, 31.12.2020, p. 14.
4 Texts adopted, P9_TA(2021)0141.
5 OJ L 119, 4.5.2016, p. 1.
6 OJ L 119, 4.5.2016, p. 89.
7 OJ L 201, 31.7.2002, p. 37.
8 A8-0324/2017.

– having regard to the draft adequacy decisions published by the Commission on 19 February 2021, one pursuant to the GDPR[1] and the other pursuant to the Law Enforcement Directive for Data Protection[2] ,

– having regard to EDPB opinions 14/2021 and 15/2021 of 13 April 2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom,

– having regard to the European Convention on Human Rights (ECHR) and to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, as well as to its amending protocol ('Convention 108+'), to which the UK is a party,

– having regard to Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers,

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

– 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 and it is of crucial importance for effective cooperation in the fight against cross-border organised and serious crime, as well as in the fight against terrorism, which increasingly depends on the exchange of personal data;

B. whereas in its Schrems I judgment, the CJEU pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the right to confidentiality of communications as provided for in 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;

C. whereas the UK has traditionally been an important trading partner of many EU Member States, as well as a close ally in the area of security; whereas the EU and the UK should maintain this close cooperation despite the UK's withdrawal from the EU, as this will be beneficial for both sides;

D. whereas European businesses need legal clarity and certainty, as the ability to transfer personal data across borders has become increasingly important for all types of companies that deliver goods and services internationally; whereas an adequacy decision concerning the UK under the GDPR is of the utmost importance, as many European businesses conduct trade across the Channel, in particular given the fact that Brexit is still very recent

---

1 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.

2 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.

and data flows within the Union have not been subject to restrictions; whereas failing to adopt a robust adequacy framework would risk disruptions in commercial cross-border transfers of personal data between the EU and the UK, as well as high compliance costs;

E. whereas the Trade and Cooperation Agreement (TCA) includes a number of safeguards and conditions for exchanging relevant personal data in the context of law enforcement; whereas the negotiations on personal data flows were conducted in parallel to the negotiations on the TCA but were not finalised by the end of the transition period on 31 December 2020; whereas a 'bridging clause' was included in the TCA as an interim solution, conditional upon the commitment by the UK not to change its current data protection regime, in order to ensure the continuation of personal data flows between the UK and the EU until the adoption of an adequacy decision; whereas the initial four-month period has been extended and will expire at the end of June 2021;

F. whereas the assessment carried out by the Commission before it presented its draft implementing decision was incomplete and inconsistent with the CJEU requirements for adequacy assessments, which was highlighted by the EDPB in its adequacy opinions, where it advises the Commission to further assess specific aspects of UK law and practice relating to bulk collection, overseas disclosure and international agreements in the field of intelligence sharing, additional use of the information collected for law enforcement purposes and the independence of judicial commissioners;

G. whereas certain aspects of UK law and/or practice have not been considered by the Commission, which has led to draft implementing decisions which are inconsistent with EU law; whereas Article 45 of the GDPR says that 'when assessing the adequacy of the level of protection, the Commission shall, in particular, take account of... relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law', and that 'the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data', which includes international agreements in other areas involving access to data or information sharing, and therefore requires an assessment of such international agreements;

H. whereas the CJEU clearly stated in its Schrems I judgment that 'when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and 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'(paragraph 75);

I. whereas intelligence services activities and sharing with third countries are excluded from the scope of EU law as per the Treaties when it comes to Member States, as these are included in the scope of the necessary adequacy assessment of the level of personal data offered by third countries, as confirmed by the CJEU in the Schrems I and II judgments;

J. whereas data protection standards rely not only on the legislation in place, but also the application of those laws in practice, and whereas the Commission only assessed the legislation, not the actual application in practice, when preparing its decision;

K. whereas the Commission currently recognises 12 third countries as providing adequate protection under the GDPR and has recently concluded talks with the Republic of Korea in this regard; whereas the UK is the first country to which the Commission has proposed to grant adequacy under the Law Enforcement Directive;

L. whereas the case of the UK is distinct from all previous adequacy assessments as it concerns a former EU Member State which has incorporated the provisions of the GDPR into its national law and has moreover provided that all 'EU-derived domestic legislation', including the legislation transposing the LED, will continue to apply after the end of the transition period;

I. GENERAL DATA PROTECTION REGULATION

General observations

1. Notes that the UK is a signatory to the 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. Points out that the EU has opted for a human-rights-centric approach to data governance in developing robust data protection rules under the GDPR, and is therefore deeply 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; notes that in its adequacy opinions, the EDPB highlighted that this might lead to possible risks in relation to the protection of personal data transferred from the EU;

4. Points out that valid adequacy decisions greatly contribute to the protection of the fundamental rights of individuals and legal certainty for companies; stresses, however, that adequacy decisions based on incomplete assessments and without proper enforcement by the Commission may have the opposite effect if challenged in court;

5. Points out that the assessment carried out by the Commission before it presented its draft implementing decision was incomplete and inconsistent with the CJEU requirements for adequacy assessments, which was highlighted by the EDPB in its adequacy opinions, where it advises the Commission to further assess specific aspects of UK law and practice

relating to bulk collection, overseas disclosure and international agreements in the field of intelligence sharing, additional use of the information collected for law enforcement purposes and the independence of judicial commissioners;

Enforcement of the GDPR

6. Expresses its concern about the lack and often non-existent enforcement of the GDPR by the UK when it was still a member of the EU; points, in particular, to the lack of proper enforcement by the UK Information Commissioner's (ICO's) Office in the past; points to the example of the ICO closing a complaint about ad tech after holding two stakeholder events, writing a report (the 'Update Report on Adtech') and stating that 'the adtech industry appears immature in its understanding of data protection requirements', having used none of its enforcement powers[1]; is concerned that non-enforcement is a structural problem, as laid out in the ICO's regulatory action policy', which explicitly states that 'in the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations. These will typically involve wilful, deliberate or negligent acts, or repeated breaches of information rights obligations, causing harm or damage to individuals'; underlines that in practice, this has meant that a large number of data protection law breaches in the UK have therefore not been remedied;

7. Takes note of the UK's national data strategy, as updated on 9 December 2020, which suggests that there will be a switch from the protection of personal data towards increased and wider use and sharing of data; points out that a position that 'withholding data can negatively impact society', as indicated in the strategy, is not compatible with the principles of data minimisation and purpose limitation under the GDPR and primary law;

8. Takes note that the Constitutional Affairs Committee in 2004[2] and the Public Affairs Committee of the UK Parliament in 2014[3] recommended securing the independence of the ICO by making them an officer of parliament who would report to the parliament rather than continuing to be appointed by the Minister for Digital Media and Sport; regrets that this recommendation has not been followed through;

Data processing for immigration control

9. Notes that UK data protection law contains a derogation from certain aspects of the fundamental data protection rights and principles, such as the right of access and the right

---

1 Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it*, TechCrunch, San Francisco, 2020.

2 Seventh Report of the Select Committee on Constitutional Affairs published by the House of Commons on 13 June 2006. Paragraph 108 reads: 'We see considerable merit in the Information Commissioner becoming directly responsible to, and funded by, Parliament, and recommend that such a change be considered when an opportunity arises to amend the legislation'.

3 Report of the Public Administration Committee entitled 'Who's accountable? Relationships between Government and arm's-length bodies' published by the House of Commons on 4 November 2014. Paragraph 64 reads: 'The Information Commissioner and HM Inspectorate of Prisons should be more fully independent of Government and should report to Parliament. The Information Commissioner, Commissioner for Public Appointments and the Chair of the Committee on Standards in Public Life should become Officers of Parliament, as the Parliamentary and Health Service Ombudsman and the Comptroller and Auditor General already are.'

of a data subject to know with whom their data has been shared, if such protection would 'prejudice effective immigration control'; underlines that the monitoring and compliance of the use of the exemption must be carried out in line with standards required in the adequacy referential which require consideration of practice as well as principle by pointing out that 'it is necessary to consider not only the content of the rules applicable to personal data transferred to a third country … but also the system in place to ensure the effectiveness of such rules'; recognises that this exemption, which is available to all data controllers in the UK, has been endorsed by the ICO and a court, and can only be invoked on a case-by-case basis and applied in a necessary and proportionate way; recalls recently revealed information according to which 17 780 access requests were made in relation to data processed by the Home Office between 1 April 2018 and 31 March 2019 concerning 146.75 million data subjects and that the immigration exemption was used in over 70 % of data subject requests to the Home Office in 2020[1]; stresses that even in those cases where the Home Office made use of the derogation, access to information was not completely denied but restricted to redacted documents;

10. Notes that this exemption 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, and underlines that this is not an adequate level of protection;

11. Reiterates its serious concern about an exception to data subjects' rights in the UK's immigration policy; reiterates its position that the exemption for the processing of personal data for immigration purposes in the UK Data Protection Act needs to be amended before a valid adequacy decision can be issued, as repeatedly voiced, including in its resolution of 12 February 2020 on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland[2] and the opinion of the Committee on Civil Liberties, Justice and Home Affairs of 5 February 2021[3]; calls on the Commission to seek the removal of the immigration exemption, or to ensure that it is reformed so that the exemption and its use provide sufficient safeguards for data subjects and do not breach the standards expected of a third country;

Mass surveillance

12. 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; recalls that this mass surveillance of

---

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

2 Texts adopted, P9_TA(2020)0033.

3 Opinion 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.

communications content and metadata takes place regardless of whether there are any specific suspicions or any target data;

13. Recalls that in the Schrems I and Schrems II judgments, the CJEU held that mass access to the content of private communications touches upon the essence of the right to privacy, and that in such cases, a necessity and proportionality test is no longer required; underlines that these principles apply to data transfers to third countries other than the US, including the United Kingdom;

14. 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; recognises that the UK has since significantly reformed its surveillance laws and introduced safeguards which go beyond the conditions defined by the Court of Justice of the European Union (CJEU) in its 'Schrems II' ruling[1] and the safeguards provided in the surveillance laws of most Member States; welcomes in particular the provision of full access to effective judicial redress; recalls that the UN Special Rapporteur on the Right to Privacy has welcomed the strong safeguards introduced with the Investigatory Powers Act (IPA) 2016 in terms of necessity, proportionality and independent authorisation by a judicial body;

15. 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'[2];

16. Considers it unacceptable that the draft adequacy decisions fail to take into account the lack of limitations on the use of UK bulk data powers, or the actual use of UK-US surveillance operations as exposed by Edward Snowden, including the facts that:

    (a) there is no effective substantive oversight by the ICO or the courts over the use of the national security exemption in UK data protection law;

    (b) the limitations on the use of UK 'bulk powers' are not set out in the law itself, as required by the CJEU (but rather are left to executive discretion subject to 'respectful' judicial control);

    (c) the description of 'secondary data' (metadata) in the draft decisions is seriously misleading and fails to note that such data can be highly revealing and intrusive and are subject to sophisticated automated analyses (as the CJEU found in *Digital Rights Ireland*[3]), yet under UK law metadata are not meaningfully protected against undue access, bulk collection and AI-based analysis by the UK intelligence agencies;

---

1 Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

2 Judgment 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.

3 Judgment of the Court of Justice of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

(d) the Five Eyes agencies, in particular GCHQ and the National Security Agency (NSA), in practice share all intelligence data;

points out that furthermore, in relation to the US, UK citizens are subject to some informal safeguards between GCHQ and the 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;

17. Calls on the Member States to enter into no-spying agreements with the UK and calls on the Commission to use its exchanges with its UK counterparts to convey the message that, if UK surveillance laws and practices are not amended, the only feasible option to facilitate the adequacy decisions would be the conclusion of 'no-spying' agreements with the Member States;

Onward transfers

18. Strongly underlines 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 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 I and Schrems II judgments of the CJEU when assessing the adequacy of other third countries; is concerned that UK courts will nevertheless no longer apply the Charter; points out that the UK is not under the jurisdiction of the CJEU anymore, which is the highest instance that can interpret the Charter;

19. 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;

20. Is concerned that the UK has granted itself the right to declare that other third countries or territories provide adequate data protection, irrespective of whether the third country or territory in question has been held to provide such protection by the EU; recalls that the UK has already declared that Gibraltar provides such protection even though the EU has not done so; 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;

21. 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 11 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 decision[1];

22. Regrets that the Commission did not assess the impact and potential risks of the Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan

---

[1] UK Department for International Trade press release of 30 January 2021 entitled 'UK applies to join huge Pacific free trade area CPTPP'.

for a Comprehensive Economic Partnership, which includes provisions on personal data and on the level of data protection;

23. 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

24. Highlights that the UK is the first country for which the Commission has suggested adopting an adequacy decision under Directive (EU) 2016/680;

25. Notes the UK's cross-border data access agreement with the US[1] under the US CLOUD Act, which facilitates transfers for law enforcement purposes; is deeply concerned that this will allow undue access to the personal data of EU citizens and residents by US authorities; shares the concern of the EDPB that the safeguards provided under the EU-US Umbrella Agreement[2] applied on a *mutatis mutandis* basis might not meet the criteria of clear, precise and accessible rules when it comes to access to personal data, or might not sufficiently enshrine such safeguards so as to be effective and actionable under UK law;

26. 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;

27. 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 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;

28. 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;

29. Recalls that in its resolution of 12 February 2020, the European Parliament stressed that 'the UK cannot have direct access to EU information systems data or participate in the management structures of the EU agencies in the area of Freedom, Security and Justice, while any sharing of information including personal data with the UK should be subject to strict safeguards, audit and oversight conditions, including an equivalent level of protection of personal data to that provided by EU law'; takes note of the shortcomings 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 a copy of the Schengen

---

1 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.

2 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (OJ L 336, 10.12.2016, p. 3.)

Information System (SIS); expects the UK law enforcement agencies to fully comply with the applicable rules when exchanging personal data in the future; recalls that the UK maintains access to some EU law enforcement databases only on a hit/no hit basis and is legally excluded from accessing the SIS;

30. Expresses its concern over the January 2021 revelation that 400 000 criminal records were accidentally deleted from the UK Police National Computer; stresses that this does not inspire trust in the UK's efforts to protect data for law enforcement purposes;

31. Notes that the draft adequacy decision thoroughly assesses the rights of each UK authority empowered by national law to intercept and retain personal data for national security reasons; welcomes, furthermore, the fact that detailed oversight reports about the authorities in charge of the intelligence community provide information regarding the UK's current surveillance practices; calls on the Commission to further assess and monitor the types of communications data that fall under UK data retention and lawful interception powers;

32. Points out that the EU-UK Trade and Cooperation Agreement (TCA) includes titles on the exchange of DNA, fingerprints and vehicle registration data, the transfer and processing of passenger name record (PNR) data, 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; recalls the right to bring an action before the CJEU in order to seek verification of the legality of the proposed international agreement and, in particular, the compatibility thereof with the protection of a fundamental right[1];

Conclusions

33. 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;

34. Welcomes the fact that the adequacy decisions will only apply for four years, as the UK might choose to amend the legislation subject to the Commission's adequacy assessment now that it is no longer an EU Member State; calls on the Commission to keep monitoring the level of data protection in the UK in law and practice in the meantime and to conduct a thorough assessment before renewing the adequacy decision in 2025;

35. Takes the view that by adopting the two implementing decisions, which are not consistent with EU law, without having addressed all the concerns expressed in the present resolution, the Commission is going beyond the implementing powers conferred upon it

---

[1] European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (OJ C 103 E, 29.4.2004, p. 665).

by Regulation (EU) 2016/679 and Directive (EU) 2016/680; therefore objects to the two implementing acts on the basis that the draft implementing decisions are not consistent with EU law;

36. Calls on the Commission to amend the two draft implementing decisions with a view to making them fully consistent with EU law and case law;

37. Requests that national data protection authorities suspend the transfer of personal data, which might be subject to indiscriminate access by UK intelligence authorities if the Commission were to adopt its adequacy decisions in relation to the UK before the UK solves the issues mentioned above;

38. Calls on the Commission and the UK competent authorities to set up an action plan in order to address as soon as possible the deficiencies identified in the EDPB opinions and other outstanding issues in UK data protection, which must be a precondition for the final adequacy decision;

39. Calls on the Commission to keep closely monitoring the level of data protection as well as laws and practices on mass surveillance in the UK; points out that there are other legal possibilities for transfers of personal data to the UK in Chapter V of the GDPR; recalls that in line with EDPB guidelines, transfers relying on derogations for specific situations pursuant to Article 49 of the GDPR must be exceptional;

40. Regrets that the Commission has ignored Parliament's calls to suspend the Privacy Shield until the US authorities comply with its terms, but has instead always preferred to 'monitor the situation' without any concrete result in terms of data protection for individuals and legal certainty for businesses; urges the Commission to learn from its past failures to heed calls from Parliament and experts with regard to the conclusion and monitoring of past adequacy decisions, and not to leave the proper enforcement of EU data protection law to the CJEU following complaints by individuals;

41. Calls on the Commission to closely monitor data protection law and practices in the UK, to immediately inform and consult Parliament on any future changes to the UK data protection regime, and to give Parliament a scrutiny role in the new institutional framework, including for relevant bodies such as the Specialised Committee on Law Enforcement and Judicial Cooperation;

°

° °

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