European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2021)0256

Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II") - Case C-311/18

European Parliament 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 (2020/2789(RSP))

The European Parliament,

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

– 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)[1],

– 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')[2],

– having regard to the judgment of the Court of Justice of 6 October 2020 in Case C-623/17 *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*[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],

---

1 Judgment of the Court of Justice 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 Court of Justice of 6 October 2015, *Maximillian Schrems* v *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
3 Judgment of the Court of Justice of 6 October 2020, *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*, C-623/17, ECLI:EU:C:2020:790.
4 OJ C 76, 28.2.2018, p. 82.
5 OJ C 298, 23.8.2018, p. 73.

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield[1],

– 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[2],

– having regard to Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)[3],

– 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-U.S. Privacy Shield (notified under document C(2016) 4176)[4],

– having regard to its resolution of 26 November 2020 on the EU Trade Policy Review[5],

– 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)[6], in particular Chapter V thereof,

– having regard to the Commission proposal for a regulation on Privacy and Electronic Communications (COM(2017)0010), having regard 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 the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, as well the EDPB statement of 19 November 2020 on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB,

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

A. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas this is even more important in the context of the current COVID-19 pandemic as such transfers are essential to ensure the continuity of business and government operations as well as social interactions; whereas they can also support exit strategies from the pandemic and contribute to economic recovery;

---

1 OJ C 118, 8.4.2020, p. 133.
2 OJ C 345, 16.10.2020, p. 58.
3 OJ L 39, 12.2.2010, p. 5.
4 OJ L 207, 1.8.2016, p. 1.
5 Texts adopted, P9_TA(2020)0337.
6 OJ L 119, 4.5.2016, p. 1.

B. whereas the Court of Justice of the European Union (CJEU) in the 'Schrems I' judgment invalidated the Commission decision on the Safe Harbour based on its findings, and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the right to confidentiality of communications provided for in Article 7 of the Charter;

C. whereas in the 'Schrems II' judgment the Court found that the United States (US) does not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the right to a legal remedy as provided for in Article 47 of the Charter;

D. whereas the General Data Protection Regulation (GDPR) applies to all companies processing personal data of data subjects in the Union, 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;

E. whereas European citizens' data stored and transferred by telecoms operators and businesses are an essential resource which contributes to the EU's strategic interests;

F. whereas dragnet mass surveillance by state actors is detrimental to the trust of European citizens, governments and businesses in digital services and by extension in the digital economy;

G. whereas consumer and other civil society organisations have limited resources, and enforcement of data protection rights and obligations cannot depend on their actions; whereas there is a patchwork of national procedures and practices, which is a challenge for the cooperation mechanism set out in the GDPR for cross-border complaints: whereas there is a lack of clear deadlines, a generally slow pace of proceedings, a lack of sufficient resources for supervisory authorities, in certain cases a lack of willingness or of efficient use of already allocated resources; whereas there is a current concentration of complaints against alleged infringements by big tech companies in the hands of a single national authority, which has led to an enforcement bottleneck;

H. whereas the proceedings leading to this CJEU ruling also show the difficulty experienced by data subjects and consumers in defending their rights, thereby creating a chilling effect on their ability to defend their rights before the Irish Data Protection Commissioner;

I. whereas in its resolution of 25 October 2018, Parliament, pointing to the failure of the US to meet the deadline of 1 September 2018 to be fully compliant with the Privacy Shield, has already called on the Commission to suspend the Privacy Shield until the US authorities comply with its terms;

J. whereas data subjects' rights guaranteed under EU data protection law should be respected regardless of the level of risk which they incur through personal data processing, including when it comes to transfer of personal data to third countries; whereas data controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, the purposes of the processing and the risks for data subjects;

K. whereas, to date and despite the significant CJEU case law developments over the past five years as well as the effective application of the GDPR since 25 May 2018, there has been no decision taken by supervisory authorities imposing corrective measures in relation to personal data transfers as per the GDPR consistency mechanism; whereas no meaningful decision imposing corrective measures or fines has been adopted by supervisory authorities at national level in relation to personal data transfer to third countries;

L. whereas on his first day in office US President Biden appointed the Deputy Assistant Secretary for Services at the US Department of Commerce, who will be the chief negotiator on commercial data transfers with the EU; whereas the President's nominee for US Secretary of Commerce, Gina Raimondo, called the swift conclusion of the negotiations on a successor agreement for the Privacy Shield a 'top priority' during a Senate confirmation hearing;

General observations

1. Takes note of the CJEU ruling of 16 July 2020, in which the Court upheld, in principle, the validity of Decision 2010/87/EU on standard contractual clauses (SCCs), which are the most widely used mechanism for international data transfers; notes further that the Court invalidated Commission Decision (EU) 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield; notes that to date no sustainable single mechanism to guarantee the legal transfer of commercial personal data between the EU and the US has withstood a legal challenge at the CJEU;

2. Takes note that the CJEU found SCCs an effective mechanism to ensure compliance with the level of protection provided in the EU, but required that a controller/processor established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned; recalls that this includes assessing the legal regime concerning public authorities' access to personal data, in order to ensure that the data subjects and their transferred data are not at risk of being subject to US surveillance programmes allowing bulk collection of personal data; recalls that where the recipient is unable to comply with the SCCs, the CJEU ruled that the controllers or processors are obliged to suspend the transfers of data and/or to terminate the contract; notes however, that many companies, especially SMEs, do not possess the necessary knowledge or capacity to conduct such verification, which can lead to result business disruptions;

3. Believes that the CJEU ruling, while focusing on the level of data protection afforded to data subjects in the EU whose data were transferred to the US under the Privacy Shield mechanism, also has implications for adequacy decisions concerning other third countries, including the United Kingdom; reaffirms the need for legal clarity and certainty, as the ability to safely transfer personal data across borders has become increasingly important for individuals for their personal data protection and rights, as well as for all types of organisations that deliver goods and services internationally and for businesses regarding the legal regime under which they operate; underlines, however, that until revoked, replaced or declared invalid by the CJEU, existing adequacy decisions remain in force;

4. Is disappointed that the Irish Data Protection Commissioner (DPC) brought proceedings against Maximilian Schrems and Facebook at the Irish High Court, rather than taking a

decision within its powers pursuant to Article 4 of Decision 2010/87/EU and Article 58 of the GDPR; recalls, however, that the DPC made use of the legal avenue that allows data protection authorities (DPAs) to bring concerns about the validity of a Commission implementing decision to the attention of a national judge in view of triggering a reference for preliminary ruling to the CJEU; expresses deep concern that several complaints against breaches of the GDPR filed on 25 May 2018, the day the GDPR became applicable, and other complaints from privacy organisations and consumer groups, have not yet been decided by the DPC, which is the lead authority for these cases; is concerned that the DPC interprets 'without delay' in Article 60(3) of the GDPR – contrary to the legislators' intention – as longer than a matter of months; is worried that supervisory authorities have not taken proactive steps under Article 61 and 66 of the GDPR to force the DPC to comply with its obligations under the GDPR; is also concerned about the lack of tech specialists working for the DPC and their use of outdated systems; deplores the implications of the unsuccessful attempt by the DPC to shift the costs of the judicial procedure on to the defendant, which would have created a massive chilling effect; calls on the Commission to start infringement procedures against Ireland for not properly enforcing the GDPR;

5. Is concerned about the insufficient level of enforcement of the GDPR, particularly in the area of international transfers; expresses concerns at the lack of prioritisation and overall scrutiny by national supervisory authorities with regard to personal data transfers to third countries, despite the significant CJEU case law developments over the past five years; deplores the absence of meaningful decisions and corrective measures in this regard, and urges the EDPB and national supervisory authorities to include personal data transfers as part of their audit, compliance and enforcement strategies; points out that harmonised binding administrative procedures on the representation of data subjects and admissibility are needed to provide legal certainty and deal with cross-border complaints;

6. Takes note of the Commission's draft implementing decision on standard contractual clauses for the transfer of personal data to third countries; urges the EDPB to publish further guidance on international data transfers for companies, in particular for SMEs, including a checklist for the assessment of transfers, tools to evaluate whether governments are allowed to or can access data, and information on the supplementary measures required for transfers using SCCs; invites the EDPB to also seek input from independent academics regarding potentially conflicting national law in major trading partners;

7. Recalls that in line with EDPB Guidelines 2/2018[1] on derogations of Article 49 under Regulation (EU) 2016/679, when transfers take place outside the framework of adequacy decisions or other instruments providing appropriate safeguards but are relying on derogations for specific situations pursuant to Article 49 GDPR, they must be interpreted strictly so that the exception does not become the rule; notes however, that since the invalidation of the EU-US Privacy Shield, transatlantic data flows have been maintained for digital advertising purposes in spite of doubts as to their legal basis for transfers for advertising purposes; calls on the EDPB and DPAs to ensure consistent

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

interpretation in the application and control of such derogations in line with the EDPB Guidelines;

8. Welcomes international discussions on GDPR and Law Enforcement Directive (LED)[1] compliant cross-border personal data flows; stresses that the GDPR, the LED, the e-Privacy rules and other current and future measures protecting the fundamental rights to privacy and personal data protection must not be undermined by or incorporated into international trade agreements; urges the Commission to follow and not deviate from the EU's 2018 horizontal position[2] and to take into account the relevant commitments of third countries under trade law when assessing their adequacy, including for onward transfers of data;

Standard contractual clauses

9. Takes note of the Commission draft implementing decision and draft SCCs; welcomes the fact that the Commission has sought feedback from stakeholders by organising a public consultation on this draft; notes that the EDPB and the EDPS, by means of a joint opinion issued on 15 January 2021[3], commented positively on the draft SCCs but proposed some further improvements; expects the Commission to take the input received into account before launching the comitology procedure;

10. Recalls that a large number of SMEs make use of SCCs; stresses that all types of companies urgently need clear guidelines and assistance in order to ensure legal certainty in the application and interpretation of the Court ruling;

11. Takes note of the EDPB Recommendations 01/2020[4] on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data; welcomes the fact that the EDPB organised a public consultation on its recommendations; is concerned about potential conflicts between these recommendations and the Commission proposal for SCCs; invites the Commission and the EDPB to cooperate on the finalisation of their respective documents to ensure legal certainty following the CJEU ruling; considers that the Commission should follow the guidance of the EDPB;

12. Welcomes in particular the EDPB recommendations concerning the necessity for controllers to rely on objective factors when assessing whether anything in the law or

---

1 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 (OJ L 119, 4.5.2016, p. 89).

2 EU proposal for provisions on cross-border data flows and protection of personal data and privacy, http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

3 EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries of 14 January 2021: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

4 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 11 November 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

practice of the third country may impinge on the effectiveness of the appropriate safeguards in the transfer tools for the transfers in question, rather than on subjective factors, such as the likelihood of public authorities' obtaining access to the data in a manner not in line with EU standards, which have been repeatedly rejected by the CJEU; calls on the Commission, in this regard, to ensure full alignment of its proposal for SCCs with the applicable CJEU case law;

13. Underlines that it is crucial for EU companies transferring personal data out of the EU to be able to rely on solid mechanisms compliant with the CJEU judgement; believes, in this regard, that the current Commission proposal for a SCC template should duly take into account all the relevant recommendations of the EDPB; supports the creation of a tool box of supplementary measures to choose from, e.g. security and data protection certification, encryption safeguards and pseudonymisation, that are accepted by regulators, and publicly available resources on the relevant legislation of the EU's main trading partners;

14. Points out that for data controllers that fall within the scope of the US Foreign Intelligence Surveillance Act (FISA), a transfer of personal data from the Union is not possible under these SCCs, due to the high risk of mass surveillance; expects, if no arrangement with the US is swiftly found which guarantees an essentially equivalent and therefore adequate level of protection to that provided by the GDPR and the Charter, that these transfers will be suspended until the situation is resolved; underlines the CJEU finding that neither Section 702 of the FISA, nor Executive Order 12333 (E.O. 12333), read in conjunction with Presidential Policy Directive 28 (PPD-28), correlate to the minimum safeguards resulting under EU law from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary; stresses the need to address the problems identified by the Court ruling in a sustainable manner in order to provide adequate protection of personal data for data subjects; recalls that no contract between companies can provide protection from indiscriminate access by intelligence authorities to the content of electronic communications, nor can any contract between companies provide sufficient legal remedies against mass surveillance; emphasises that this requires a reform of US surveillance laws and practices with a view to ensuring that access of US security authorities to data transferred from the EU is limited to what is necessary and proportionate, and that European data subjects have access to effective judicial redress before US courts;

15. Highlights the limited bargaining power and legal and financial capacity of European SMEs as well as of not-for-profit organisations and associations, which, through the mandated third country self-adequacy assessments, are expected to navigate the complex legal frameworks of different third countries; urges the Commission and the EDPB to provide guidance on the practical use of reliable supplementary measures, especially for SMEs;

16. Urges DPAs to comply with their obligations, underlined by the CJEU ruling, to ensure a proper and swift enforcement of the GDPR by closely monitoring the use of SCCs; calls on the DPAs to assist companies in complying with the case law of the Court; urges the DPAs to also use the full range of their investigatory and corrective powers pursuant to Article 58 of the GDPR in cases where data exporters transfer personal data despite the existence of laws in the third country of destination preventing the data importer from complying with the SCCs and the lack of effective supplementary

measures; recalls that the CJEU's found that every supervisory authority is 'required to execute its responsibility for ensuring that the GDPR is fully enforced';

Privacy shield

17. Notes that the CJEU found that the EU-US Privacy Shield does not guarantee an essentially equivalent, and therefore adequate, level of protection compared to that provided by the GDPR and the Charter, particularly because of the bulk access by US public authorities to personal data transferred under the Privacy Shield, which fails to comply with the principles of necessity and proportionality, and because of the absence of actionable rights for EU data subjects before US courts or any other independent authority acting as a tribunal against the US authorities; expects the current US administration to be more engaged in complying with its obligations under possible future transfer mechanisms than previous administrations, which showed a lack of political commitment to compliance with and enforcement of the Safe Harbour rules and enforcement of the Privacy Shield rules;

18. Points out that some companies, in reaction to the Schrems II ruling, have hastily revised their privacy notices and third-party contracts referring to their commitments under the Privacy Shield without assessing the best measures to transfer data lawfully;

19. Deplores the fact that despite Parliament's numerous calls on the Commission in its resolutions of 2016, 2017 and 2018 to take all the necessary measures to ensure that the Privacy Shield fully complied with the GDPR and the Charter, the Commission has failed to act in accordance with Article 45(5) of the GDPR; regrets that the Commission has ignored Parliament's calls to suspend the Privacy Shield until the US authorities comply with its terms, which underlined the risk of the invalidation of the Privacy Shield by the CJEU; recalls that problems with the functioning of the Privacy Shield were repeatedly raised by the Article 29 Working Party and EDPB;

20. Deplores that the Commission put the relations with the US before the interests of EU citizens, and that the Commission thereby left the task of defending EU law to individual citizens;

Mass surveillance and the legal framework

21. Encourages the Commission to proactively monitor the use of mass surveillance technologies in the United States as well as in other third countries that are or could be the subject of an adequacy finding, such as the United Kingdom; urges the Commission not to adopt adequacy decisions concerning countries where mass surveillance laws and programmes do not meet the criteria of the CJEU, either in letter or spirit;

22. Takes note of the recent entry into force in the US of the California Consumer Privacy Act (CCPA); takes note of related discussions and legislative proposals at the federal level; points out that, although they are steps in the right direction, neither CCPA nor any of the federal proposals so far meet the requirements of the GDPR for an adequacy finding; strongly encourages the US legislator to enact legislation that meets those requirements, and to thereby contribute to ensuring that US law provides an essentially equivalent level of protection to that currently guaranteed in the EU;

23. Points out that such consumer data protection and privacy legislation will not by itself suffice to remedy the fundamental issues found by the Court on mass surveillance by US intelligence services and the insufficient access to remedies; encourages the US legislator to amend section 702 of the FISA, and the US President to amend EO 12333 and PPD-28, particularly with regard to mass surveillance and granting the same level of protection to EU and US citizens; encourages the US to provide mechanisms to ensure that individuals receive (delayed) notifications and are able to challenge improper surveillance under Section 702 and EO 12333, and establish a legally enshrined mechanism to ensure that non-US citizens have enforceable rights beyond the Judicial Redress Act;

24. Recalls that the Member States continue to exchange personal data with the United States under the Terrorist Financing Tracking Program (TFTP), the EU-US Passenger Name Record (PNR) Agreement, the automatic exchange of tax information via the intergovernmental agreements implementing the US Foreign Tax Compliance Act (FATCA),which adversely affects 'accidental Americans', as referred to in Parliament's resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans'[1]; recalls that the US continues to have access to Member States' law enforcement databases containing EU citizens' fingerprints and DNA data; requests the Commission to analyse the impact of the Schrems I and II judgments on these data exchanges, and to present its analysis and how it intends to bring them in line with the judgments in public and in writing to the Committee on Civil Liberties, Justice and Home Affairs by 30 September 2021;

25. Calls also on the Commission to analyse the situation of cloud providers falling under section 702 of the FISA who transfers data using SCCs; calls also on the Commission to analyse the effect on the rights granted under the EU-US Umbrella Agreement, including the right to judicial redress, considering that the US explicitly only grants this right to citizens of designated countries that permit data transfers to the US for commercial purposes; finds it unacceptable that the Commission has still not published its findings of the first joint review of the Umbrella Agreement, a year after the deadline, and calls on the Commission, if necessary, to without delay bring the agreement into line with the standards set by the CJEU judgments;

26. Deems it necessary, in view of the marked gaps in the protection of data of European citizens transferred to the United States, to support investment in European data storage tools (e.g. cloud service) to reduce the dependence of the Union in storage capacities vis-à-vis third countries and to strengthen the Union's strategic autonomy in terms of data management and protection;

Adequacy decisions

27. Calls on the Commission to take all the measures necessary to ensure that any new adequacy decision with regard to the US fully complies with Regulation (EU) 2016/679, with the Charter, and every aspect of the CJEU judgements; recalls that adequacy frameworks significantly facilitate economic activity, in particular for SMEs and start-ups, which, unlike large companies, often do not possess the necessary financial, legal and technical capacity to make use of other transfer tools; calls on Member States to

[1] OJ C 118, 8.4.2020, p. 141.

enter into no-spying agreements with the US; calls on the Commission to use its contacts with its US counterparts to convey the message that, if there is no modification of US surveillance laws and practices, the only feasible option to facilitate a future adequacy decision would be the conclusion of no-spying agreements with the Member States;

28. Considers that any future adequacy decision by the Commission should not rely on a system of self-certification, as was the case with both Safe Harbour and the Privacy Shield; calls on the Commission to fully involve the EDPB in the assessment of compliance and enforcement of any new adequacy decision in relation to the US; calls on the Commission, in this regard, to agree with the US administration the measures necessary to allow the EDPB to fulfil this role effectively; expects the Commission to consider more seriously the European Parliament's position on any new adequacy decision in relation to the US before adopting such a decision;

29. Recalls that the Commission is currently reviewing all the adequacy decisions adopted under Directive EC 95/46/EC; stresses that the Commission should apply the stricter standards set by the GDPR and by the CJEU's Schrems I and II judgments to assess whether an essentially equivalent level of protection to that provided by the GDPR, including in terms of access to an effective remedy and protection against undue access to personal data by the third country's authorities is afforded; urges the Commission to finalise these reviews as a matter of urgency and to revoke or suspend any of pre-GDPR decisions if it finds that the third country in question does not provide an essentially equivalent level of protection and if the situation cannot be remedied;

30. Considers that the Biden administration, through the appointment of an experienced privacy expert as chief negotiator on the successor to the Privacy Shield, showed commitment to finding a solution for commercial data transfers between the EU and the US as a matter of priority; expects the dialogue between the Commission and its US counterparts which began right after the CJEU ruling to be stepped up over the coming months;

31. Calls on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms are introduced, in particular for national security and intelligence purposes, which can be achieved through clear, legally sustainable, enforceable and non-discriminatory reform of US laws and practices; reiterates, in this regard, the importance of robust safeguards in the area of access to personal data by public authorities; calls on the Commission to put into practice its 'geopolitical ambitions' to enforce essentially equivalent data protection in the US and other third countries as in the EU;

32. Recommends national data protection authorities suspend the transfer of personal data which may be subject to access by public authorities in the US if the Commission were to adopt any new adequacy decision in relation to the US in the absence of such meaningful reforms;

33. Welcomes the fact that the Commission follows the criteria set out in the Article 29 Working Party Adequacy Referential under the GDPR[1] (as endorsed by the EDPB) and in EDPB Recommendation 01/2021 on the Adequacy Referential under the Law

[1] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

Enforcement Directive[1]; considers that the Commission should not go below these criteria when evaluating whether a third country qualifies for an adequacy decision; takes note that the EDPB has recently updated its Recommendations on the European Essential Guarantees for surveillance measures in light of CJEU case law[2];

°

° °

34. Instructs its President to forward this resolution to the Commission, the European Council, the Council of the European Union, the European Data Protection Board, the national parliaments of the Member States, the Congress and Government of the United States of America and the Parliament and Government of the United Kingdom.

---

1 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en

2 https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en