Thursday, March 25, 2021

P9_TA(2021)0111

Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application

European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP))

(2021/C 494/11)

The European Parliament,

— having regard to Article 8 of the Charter of Fundamental Rights,

— having regard to Article 16 of the Treaty on the Functioning of the European Union,

— 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) (GDPR) ([1]),

— having regard to the statement by the Commission of 24 June 2020 on the Commission Communication to the European Parliament and the Council on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — two years of application of the General Data Protection Regulation,

— having regard to the Commission Communication of 24 June 2020 to the European Parliament and the Council on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — two years of application of the General Data Protection Regulation (COM(2020)0264),

— having regard to the Commission Communication of 24 July 2019 entitled 'Data protection rules as a trust-enabler in the EU and beyond — taking stock' (COM(2019)0374),

— having regard to the contribution of the European Data Protection Board (EDPB) to the evaluation of the GDPR under Article 97, adopted on 18 February 2020 ([2]),

— having regard to the EDPB's 'First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities' of 26 February 2019 ([3]),

— having regard to the guidelines adopted by the EDPB pursuant to Article 70(1)(e) of the GDPR,

— 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 GDPR has been applicable since 25 May 2018; whereas, with the exception of Slovenia, all Member States have adopted new legislation or adapted their national data protection law;

B. whereas according to the Fundamental Rights Survey carried out by the Fundamental Rights Agency, individuals are increasingly aware of their rights under the GDPR; whereas despite the fact that organisations have put in place measures to facilitate the exercise of data subject's rights, individuals continue to face difficulties when trying to exercise these rights, particularly the right of access, portability, and enhanced transparency;

C. whereas, since the start of application of the GDPR, supervisory authorities have received a massive increase in complaints; whereas this illustrates that data subjects are more aware of their rights and want to protect their personal data in line with the GDPR; whereas this also illustrates that large volumes of illegal data processing operations continue to take place;

([1]) OJ L 119, 4.5.2016, p. 1.
([2]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf
([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

D. whereas many businesses have used the transition period between the GDPR entering into force and becoming applicable for a data 'spring cleaning' to assess what data processing is actually taking place and which data processing might not be any longer needed or justified;

E. whereas many data protection authorities (DPAs) are not able to cope with the number of complaints; whereas many DPAs are understaffed, under-resourced and lack a sufficient number of information technology experts;

F. whereas the GDPR recognises that Member State law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression, with the right to personal data protection; whereas according to Article 85 Member State legislation should provide for exemptions for processing of data carried out for journalistic purposes or academic artistic or literary expression, if they are necessary to reconcile the right to the protection of personal data with the freedoms of expression and information;

G. whereas, as also emphasised by the EDPB, the protection of journalistic sources is the cornerstone of freedom of the press; whereas the GDPR should not be abused against journalists and to limit access to information: whereas it should under no circumstances be used by national authorities to stifle media freedom;

General Observations

1. Welcomes the fact that the GDPR has become a global standard for the protection of personal data and is a factor for convergence in the development of norms; welcomes the fact that the GDPR has placed the EU at the forefront of international discussions about data protection, and a number of third countries have aligned their data protection laws with the GDPR; points out that Council of Europe Convention 108 on Data Protection has been aligned with the GDPR ('Convention 108+') and has already been signed by 42 countries; urges the Commission and the Member States to use this momentum to push at UN, OECD, G8 and at G20 level for the creation of international standards that are shaped on European values and principles without undermining the GDPR; underlines that a dominant European position in this field would help our continent to better defend the rights of our citizens, safeguard our values and principles, promote trustworthy digital innovation, and to accelerate the economic growth by avoiding fragmentation;

2. Concludes that, two years after its entry into application, the GDPR has been an overall success, and agrees with the Commission that it is not necessary at this stage to update or review the legislation;

3. Acknowledges that until the Commission's next evaluation, the focus must continue to be on the improvement of implementation and on actions to strengthen the enforcement of the GDPR;

4. Acknowledges the need for strong and effective enforcement of the GDPR in large digital platforms, integrated companies and other digital services, especially in the areas of online advertising, micro-targeting, algorithmic profiling, and the ranking, dissemination and amplification of content;

Legal Basis For Processing

5. Underlines that all six legal bases laid down in Article 6 of the GDPR are equally valid for the processing of personal data, and that the same processing activity may fall under more than one basis; urges data supervisory authorities to specify that data controllers must rely on only one legal ground for each purpose of the processing activities, and specify how each legal ground is relied upon for their processing operations; is concerned that controllers often mention all the legal grounds of the GDPR in their privacy policy without further explanation and without referring to the specific processing operation concerned; understands that this practice hinders the ability of the data subjects and the supervisory authorities to assess whether these legal grounds are appropriate; recalls that in order to process special categories of personal data a lawful ground under Article 6 and a separate condition for processing under Article 9 must be identified; reminds controllers of their legal obligation to conduct a data protection impact assessment (DPIA) when the processing of data is likely to result in a high risk to the rights and freedoms of natural persons;

6. Recalls that since the start of the application of the GDPR, 'consent' means any freely, given, specific, informed and unambiguous indication of the data subject's wishes; underlines that this also applies to the e-Privacy Directive; notes that the implementation of valid consent continues to be compromised by the use of dark patterns, pervasive tracking and other unethical practices; is concerned that individuals are often put under financial pressure to give consent in return for discounts or other commercial offers, or are forced to give consent by conditioning access to a service through tying provisions, in breach of Article 7 of the GDPR; recalls the EDPB harmonised rules on what constitutes valid consent, replacing the different interpretations by many national DPAs, and avoiding fragmentation within the Digital Single Market; recalls also the EDPB and Commission guidelines establishing that for cases in which the data subject has initially given consent but where the personal data is further processed for a different purpose than the purpose to which the data subject gave consent to, the initial consent cannot legitimise further processing, as consent needs to be informed and specific to be valid; takes note of the EDPB's upcoming guidelines on processing personal data for scientific research, which will provide clarity on the meaning of Recital 50 of the GDPR;

7. Is concerned that 'legitimate interest' is very often abusively mentioned as a legal ground for processing; points out that controllers continue to rely on legitimate interest without conducting the required test of the balance of interests, which includes a fundamental rights assessment; is particularly concerned by the fact that some Member States are adopting national legislation to determine conditions for processing based on legitimate interest by providing for the balancing of the respective interests of the controller and of the individuals concerned, while the GDPR obliges each and every controller to undertake this balancing test individually, and to avail themselves of that legal ground; is concerned that some national interpretations of legitimate interest do not respect Recital 47, and effectively prohibit processing on the basis of legitimate interest; welcomes the fact that the EDPB has already started the work to update the Article 29 Working Party (WP29) opinion on the application of legitimate interest as a legal ground for processing in order to address the issues highlighted in the Commission's report;

Data Subject Rights

8. Stresses that there is a need to facilitate the exercise of individual rights provided for by the GDPR, such as data portability or rights in the context of automated processing, including profiling; welcomes the EDPB guidelines on automated decision-making and on data portability; notes that the right to data portability has not been fully implemented in several sectors; calls on the EDPB to encourage online platforms to create a single point of contact for all their underlying digital platforms from which user requests can be forwarded to the correct recipient; points out that in line with the principle of data minimisation, the implementation of the right to anonymity effectively prevents unauthorised disclosure, identity theft and other forms of abuse of personal data;

9. Highlights that compliance with the right to be informed requires companies to provide information in a concise, transparent, intelligible and easily accessible manner, and to avoid taking a legalistic approach when drafting data protection notices; is concerned that some companies continue to breach their obligations under Article 12(1) of the GDPR and fail to provide all the relevant information recommended by the EDPB, including listing the names of the entities with whom they share data; recalls that the obligation to provide information that is simple and accessible is particularly strict when it comes to children; is concerned about the widespread lack of properly functioning data subject access mechanisms; points out that individuals are often not able to force internet platforms to reveal their behavioural profiles to them; is concerned that too often companies ignore the fact that inferred data is also personal data, subject to all safeguards under the GDPR;

Small Businesses and Organisations

10. Observes that some stakeholders report that the application of the GDPR has been particularly challenging, especially for small and medium sized enterprises (SMEs), start-ups, organisations and associations, including schools, and clubs as well as societies; notes, however, that many of the rights and obligations in the GDPR are not new, but were already

in force under Directive 95/46/EC ([4]), although rarely enforced; finds that the GDPR and its enforcement must not lead to unintended consequences of compliance for smaller companies that big companies would not experience; believes that more support, information and training should be made available by national authorities and Commission information campaigns in order to help increase knowledge, the quality of implementation and awareness of the requirements and purpose of the GDPR;

11. Points out that there are no derogations for SMEs, start-ups, organisations and associations, including schools, clubs as well as societies, and that they are subject to the scope of the GDPR; calls on the EDPB, therefore, to provide clear information to avoid any confusion about the interpretation of the GDPR, and to create a practical GDPR tool to facilitate the implementation of the GDPR by SMEs, start-ups, organisations and associations, including schools, clubs as well as societies with low risk processing activities; calls on the Member States to make available sufficient means for the DPAs to disseminate knowledge about these practical tools; encourages the EDPB to develop privacy policy templates that organisations may use to assist them to demonstrate actual compliance with GDPR in practice without having to rely on costly third party services;

Enforcement

12. Expresses its concern about the uneven and sometimes non-existent enforcement of the GDPR by national DPAs more than two years after the start of its application, and therefore regrets that the enforcement situation has not substantially improved compared to the situation under Directive 95/46/EC;

13. Takes note that around 275 000 complaints were introduced and 785 administrative fines were imposed for different infringements during the first 18 months of the application of the GDPR, but points out that only a very small share of submitted complaints has been so far been followed up; is aware of the problems caused by personal data breaches, and recalls current EDPB guidance providing clarity on the timeline for notification, communication to data subjects and remedies among others; points out that a European standard data breach notification form could be beneficial for harmonising diverse national approaches; regrets, however, that the amount of the fines varies significantly across Member States, and that some fines issued to large companies are too low to have the intended deterrent effect for data protection violations; calls on the DPAs to strengthen the enforcement, prosecution and penalties for data protection violations, and to make full use of the possibilities in the GDPR to impose fines and use other corrective measures; stresses that bans on processing, or the obligation to delete personal data acquired in a manner that is not compliant with the GDPR, may have an equally if not higher deterrent effect than fines; calls on the Commission and the EDPB to harmonise penalties by means of guidelines and clear criteria, as has been done by the conference of German supervisory authorities, in order to increase legal certainty and to prevent companies settling in the locations that impose the lowest penalties;

14. Is concerned about the length of case investigations by some DPAs, and about its adverse effect on effective enforcement and on citizens' trust; urges DPAs to speed up the resolution of cases, and to use the full range of possibilities under the GDPR, particularly if there are systematic and persistent breaches, including with gainful interest and a large number of affected data subjects;

15. Is concerned about the fact that the supervisory authorities of 21 Member States out of the combined 31 states applying the GDPR, namely all Member States of the European Union, the European Economic Area, and the United Kingdom, have explicitly stated that they do not have sufficient human, technical and financial resources, premises and infrastructure to effectively perform their tasks and exercise their powers; is concerned by the lack of dedicated technical staff in most supervisory authorities across the EU, which makes investigations and enforcement difficult; notes with concern that supervisory authorities are under strain given the growing mismatch between their responsibilities to protect personal data and their resources to do so; notes that digital services will become increasingly complex due to the increased use of innovations like artificial intelligence (i.e. worsening the problem of limited transparency on data processing, especially for algorithmic training); points therefore to the importance of EU supervisory authorities as well as the EDPB

([4]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

having sufficient financial, technical and human resources in order to be able to deal swiftly but thoroughly with an increasing number of resource-intensive and complex cases, and to coordinate and facilitate cooperation between national DPAs, to properly monitor the application of the GDPR, and protect fundamental rights and freedoms; expresses its concern that insufficient resources for DPAs, in particular when their resources are compared with the revenue of large information technology companies, may result in agreements on settlements, as this would limit the cost of lengthy and cumbersome proceedings;

16. Calls on the Commission to evaluate the possibility of obliging large multinational technology companies to pay for their own oversight through the introduction of an EU digital tax;

17. Notes with concern that the lack of enforcement by DPAs and the inaction on the part of the Commission to address the lack of resources of the DPAs leaves the burden of enforcement on individual citizens to bring data protection claims to court; is concerned that courts sometimes order individual claimants to be compensated without ordering the organisation or company to solve structural problems; considers that private enforcement can trigger important case law, but does not constitute a replacement for enforcement by the DPAs or action by the Commission to address the lack of resources; deplores the fact that these Members States are in breach of Article 52(4) of the GDPR; calls on Member States, therefore, to comply with their legal obligation under Article 52(4) to allocate sufficient funds to their DPAs to allow them to carry out their work in the best way possible and to ensure a European level playing field for the enforcement of the GDPR; regrets the fact that the Commission has not yet started infringement procedures against those Member States that have failed to fulfil their obligations under the GDPR, and urges the Commission to do so without delay; calls on the Commission and the EDPB to organise a follow-up of the Commission communication of 24 June 2020, assessing the functioning of the GDPR as well as its enforcement;

18. Regrets that, the majority of Member States decided not to implement Article 80(2) of GDPR; calls on all Member States to make use of Article 80(2), and to implement the right to lodge complaints and go to court without being mandated by a data subject; calls on Member States to clarify the position of complainants during proceedings in national administrative procedures legislation applicable to supervisory authorities; points out that this should clarify that complainants are not limited to a passive role during the procedure, but should be able to intervene at different stages;

Cooperation and consistency

19. Points out that weak enforcement is particularly evident in cross-border complaints, and deplores the fact that the DPAs in 14 Member States do not have the right resources to contribute to the cooperation and consistency mechanisms; calls on the EDPB to increase its efforts to ensure the correct application of Article 60 and Article 63 of the GDPR and reminds the supervisory authorities that they can make use, in exceptional circumstances, of the urgency procedure provided for in Article 66 of the GDPR, in particular provisional measures;

20. Underlines the importance of the one-stop-shop mechanism in providing legal certainty and reducing the administrative burden for companies and citizens alike; expresses, however, great concern over the functioning of the mechanism, particularly regarding the role of the Irish and Luxembourg DPAs; notes that these DPAs are responsible for handling a large number of cases, since many tech companies have registered their EU headquarters in Ireland or Luxembourg; is particularly concerned that the Irish data protection authority generally closes most cases with a settlement instead of a sanction and that cases referred to Ireland in 2018 have not even reached the stage of a draft decision pursuant to Article 60(3) of the GDPR; calls on these DPAs to speed up their ongoing investigations into major cases in order to show EU citizens that data protection is an enforceable right in the EU; points out that the success of the 'one-stop shop-mechanism' is contingent on the time and effort that DPAs can dedicate to the handling of and cooperation on individual cross-border cases in the EDPB, and that the lack of political will and resources has immediate consequences on the extent to which this mechanism can function properly;

21. Observes inconsistencies between the Member States' guidelines and the EDPB guidelines; points out that national DPAs may come to different interpretations of the GDPR, resulting in different applications among the Member States; notes that this situation is creating geographical advantages as well as disadvantages for companies; urges the Commission to assess whether national administrative procedures hinder the full effectiveness of cooperation as per Article 60 of the

GDPR as well as its effective implementation; calls on DPAs to strive for consistent interpretation and guidance facilitated through the EDPB; calls specifically on the EDPB to establish basic elements of a common administrative procedure to handle complaints in cross-border cases under the cooperation established under Article 60; urges that this should be done by following guidance on common timelines for carrying out investigations and adopting decisions; calls on the EDPB to strengthen the consistency mechanism and make it mandatory for any matter of general application or for any case with cross-border effects in order to avoid inconsistent approaches and decisions from individual DPAs, as this would jeopardise the uniform interpretation and application of the GDPR; considers that this common interpretation, application and guidance will contribute to the creation and the success of the digital single market;

22. Calls on the EDPB to publish its meeting agenda ahead of its meetings and to provide more detailed summaries of its meetings to the public and to Parliament;

Fragmentation of GDPR implementation

23. Deplores the fact that the Member States' use of the facultative specification clauses (e.g. processing in the public interest or by public authorities on the basis of the Member State's law and age of children to consent) has been detrimental to the achievement of full data protection harmonisation and to the elimination of diverging market conditions for companies throughout the EU, and expresses concern that this may drive up the cost of GDPR-compliance; calls on the EDPB to bring forward guidance on how to deal with the different implementation of facultative specification clauses between the Member States; calls on the Commission to use its powers to intervene in Member States where national measures, actions and decisions undermine the spirit, objective, and text of the GDPR, with a view to preventing unequal protection for citizens and market distortions; highlights in this juncture that the Member States have adopted a different age range for parental consent; calls, therefore, on the Commission and the Member States to assess the impact of this fragmentation on children's activities and on their protection online; stresses that in the case of conflict of laws between a national law of a Member State and the GDPR, the provisions of the GDPR should prevail;

24. Expresses strong concerns over abuse of the GDPR by some Member States' public authorities to curtail journalists and non-governmental organisations; strongly agrees with the Commission that data protection rules should not affect the exercise of freedom of expression and information, especially by creating a chilling effect or by being interpreted as a way to put pressure on journalists to disclose their sources; expresses, however, its disappointment over the fact that the Commission has still not finished its assessment of the balancing between the right to the protection of personal data with freedom of expression and information, as outlined in Article 85 of the GDPR; calls on the Commission to finish its assessment of national legislation in this respect without undue delay and to use all available tools, including infringement procedures, to ensure that the Member States comply with the GDPR and to limit any fragmentation of the data protection framework;

Data protection by design

25. Calls on the supervisory authorities to evaluate the implementation of Article 25 on data protection by design and by default, in particular with a view to ensuring the technical and operational measures needed to implement the principles of data minimisation and purpose limitation, and to determine the effect this provision has had on manufacturers of processing technologies; welcomes the fact that the EDPB adopted in October 2020 Guidelines 04/2019 on Article 25 data protection by design and by default in order to contribute to the legal clarity of the concepts; calls on the supervisory authorities to also assess the proper use of default settings as provided for in Article 25(2), including by major online service providers; recommends that the EDPB adopt guidelines to determine under which specific conditions and in which (classes of) cases, ICT manufacturers are to be considered controllers pursuant to Article 4(7), in the sense that they determine the means of processing; points out that data protection practices still largely depend on manual tasks and arbitrary formats, and are riddled with incompatible systems; calls on the EDPB to develop guidelines that help to implement data protection requirements into practice, including guidelines for data protection impact assessments (Article 35), data protection by design and by default (Article 25), information directed at data subjects (Articles 12–14), the exercise of data subjects' rights (Articles 15–18, 20–21), and records of processing activities (Article 30); calls on the EDPB to ensure that such guidelines are easy to apply and also allow for machine-to-machine communication between data

subjects, controllers and DPAs (automating data protection); calls on the Commission to develop the machine-readable icons pursuant to Article 12(8) for informing data subjects, in close coordination with the EDPB; encourages the EDPB and the supervisory authorities to leverage the full potential of Article 21 (5) on automated ways to object to the processing of personal data;

Guidelines

26. Calls on the EDPB to harmonise the implementation of data protection requirements into practice through the development of guidelines, inter alia, the need to assess risks related to data processing information to data subjects (Articles 12–14), to the exercise of data subjects' rights (Articles 15–18, 20–21) and to the implementation of the accountability principle; calls on the EDPB to issue guidelines that classify different legitimate use cases of profiling according to their risks for the rights and freedoms of data subjects, along with recommendations for appropriate technical and organisational measures, and with a clear delineation of illegal-use cases; invites the EDPB to review WP29 05/2014 of 10 April 2014 on Anonymisation Techniques and to establish a list of unambiguous criteria to achieve anonymisation; encourages the EDPB to clarify data processing for human resources purposes; takes note of the EDPB's conclusion that the need to assess risks related to data processing, as provided in the GDPR, should be maintained, as risks for data subjects are not related to the size of data controllers; calls for a better use of the mechanism under which the Commission can request advice from the EDPB on the matters covered by the GDPR;

27. Notes that the COVID-19 pandemic has highlighted the need for clear guidance from DPAs and the EDPB on the adequate implementation and enforcement of the GDPR in public health policies; recalls, in this regard, the Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak and Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak; calls on the Commission to ensure full compliance with the GDPR when creating the common European health data space;

International personal data flows and cooperation

28. Stresses the importance of allowing free personal data flows at international level without lowering the level of protection guaranteed under the GPDR; supports the Commission's practice of addressing data protection and personal data flows separately from trade agreements; believes that international cooperation in the field of data protection and the convergence of relevant rules towards the GDPR will improve mutual trust, foster understanding of technological and legal challenges, and eventually facilitate cross-border data flows, which are of key importance for international trade; acknowledges the reality of conflicting legal requirements for companies conducting data processing activities in the EU, as well as in third-country jurisdictions, notably the US;

29. Stresses that adequacy decisions should not be political but legal decisions; encourages continued efforts to promote global legal frameworks to enable data transfers on the basis of the GDPR and the Council of Europe Convention 108+; Notes, further, that stakeholders consider adequacy decisions an essential instrument for such data flows since they do not attach them to additional conditions or authorisations; highlights, however, that so far adequacy decisions have only been adopted for nine countries, even though many additional third countries have recently adopted new data protection laws with similar rules and principles as the GDPR; notes that, to date, no single mechanism guaranteeing the legal transfer of commercial personal data between the EU and the US has stood a legal challenge at the Court of Justice of the European Union (CJEU);

30. Welcomes the adoption of the first mutual adequacy decision between the EU and Japan, which has created the largest area of free and safe data flows in the world; calls, however, on the Commission to take all issues raised by Parliament into account in the first review on this instrument and make the results publicly available as soon as possible, since the review should have been adopted by January 2021;

31. Calls on the Commission to publish the set of criteria used in determining whether a third country is deemed to provide an 'essentially equivalent' level of protection to that afforded in the EU, especially with regard to access to remedies, and government access to data; insists on the need to ensure the effective application of and compliance with the provisions

related to transfers or disclosures not authorised by Union law as per Article 48 of the GDPR, in particular regarding requests by third-country authorities for access to personal data in the Union, and calls on the EDPB and DPAs to provide guidance and enforce these provisions, including in the assessment and development of personal data transfer mechanisms;

32. Calls on the Commission to adopt delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanism as per Article 42(1), to boost the use of the latter, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, as a means for international transfers, as provided for by Article 46(2)(f);

33. Reiterates the fact that mass surveillance programmes encompassing bulk data collection prevent adequacy findings; urges the Commission to apply the conclusions of the CJEU in the cases Schrems I ([5]), II ([6]) and Privacy International & al (2020) ([7]) to all reviews of adequacy decisions as well as ongoing and future negotiations; recalls that transfers relying on derogations for specific situations as per Article 49 of the GPDR should remain exceptional; welcomes the guidelines from the EDPB and the DPAs in this regard and calls on them to ensure consistent interpretation in the application and control of such derogations in line with the EDPB Guidelines 02/2018;

34. Calls on the DPAs and the Commission to systematically assess whether data protection rules are applied in practice in third countries, in line with CJEU case law;

35. Urges the Commission to publish its review of the adequacy decisions adopted under the 1995 Directive without undue delay; highlights that, in the absence of an adequacy decision, standard contractual clauses (SCC) are the most widely used tool for international data transfers; notes that the CJEU upheld the validity of Decision 2010/87/EU on SCC ([8]) while requiring an assessment of the level of protection afforded for data transferred to a third country and of the relevant aspects of the legal system of that third country as regards public authorities' access to the personal data transferred; urges the Commission to accelerate its work on modernised SCC for international data transfers to ensure a level-playing field for small and medium-sized enterprises (SMEs) at international level; welcomes the Commission's publication of draft SCC and the objective to make SCC more user-friendly and to address identified shortcomings of the current standards;

36. Recalls the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation (EU) 2016/679; acknowledges that this instrument is currently underused despite ensuring GDPR compliance when used together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards; highlights the potential of this instrument to better support SMEs and provide more legal certainty in the context of international data transfers across different sectors;

Future Union legislation

37. Takes the view that by being technology-neutral, the GDPR provides a solid regulatory framework for emerging technologies; considers, nonetheless, that further efforts are needed to address broader issues of digitisation, such as monopoly situations and power imbalances through specific regulation, and to carefully consider the correlation of the

([5]) Judgment of the Court of Justice of 6 October 2015, *Maximillian Schrems* v *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

([6]) Judgement 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.

([7]) Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.

([8]) 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, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ L 39, 12.2.2010, p. 5).

GDPR with each new legislative initiative in order to ensure consistency and address legal gaps; reminds the Commission of its obligation to ensure legislative proposals, such as the data governance, data act, digital services act or on artificial intelligence, must always fully comply with the GDPR and the Law Enforcement Directive ([9]); considers that the final texts adopted by the co-legislators through interinstitutional negotiations need to fully respect the data protection acquis; regrets, however, that the Commission itself does not always have a consistent approach to data protection in legislative proposals; stresses that a reference to the application of the GDPR, or 'without prejudice to the GDPR', does not automatically make a proposal GDPR compliant; calls on the Commission to consult the European Data Protection Supervisor (EDPS) and the EDPB where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data following the adoption of proposals for a legislative act; calls further on the Commission, when preparing proposals or recommendations, to endeavour to consult the EDPS, in order to ensure consistency of data protection rules throughout the Union, and to always conduct an impact assessment;

38. Notes that profiling, although only allowed by Article 22 GDPR under strict and narrow conditions, is increasingly used as the online activities of individuals allow for deep insights into their psychology and private life; notes that since profiling makes it possible to manipulate users' behaviour, the collection and processing of personal data concerning the use of digital services should be limited to the extent strictly necessary in order to provide the service and bill users; calls on the Commission to propose strict sector-specific data protection legislation for sensitive categories of personal data where it has not yet done so; demands the strict enforcement of the GDPR in the processing of personal data;

39. Calls for the empowerment of consumers so that they can make informed decisions on the privacy implications of using new technologies and to ensure fair and transparent processing by providing easy-to-use options to give and withdraw consent to the processing of their personal data as provided for by the GDPR;

The Law Enforcement Directive

40. Is concerned that data protection rules used for law enforcement purposes are vastly inadequate to keep up with newly created competences for law enforcement; calls therefore on the Commission to evaluate the Law Enforcement Directive earlier than the deadline provided for in the directive and to make the review publicly available;

The ePrivacy Regulation

41. Expresses its deep concern about the lack of implementation of the ePrivacy Directive ([10]) by the Member States in view of the changes introduced by the GDPR; calls on the Commission to speed up its assessment and initiate infringement procedures against those Member States that failed to properly implement the ePrivacy Directive; is greatly concerned that the overdue reform of the eprivacy for several years leads to fragmentation of the legal landscape in the EU, detrimental to both businesses and citizens; recalls that the ePrivacy Regulation ([11]) was designed to complement and particularise the GDPR and coincide with the entry into application of the GDPR; underlines that the reform of the ePrivacy rules must not lead to a lowering of the current level of protection afforded under the GDPR and the ePrivacy Directive; regrets the fact that it took four years for the Council to eventually adopt its negotiating position on the proposal for the ePrivacy Regulation, while Parliament adopted its negotiation position in October 2017; recalls the importance of upgrading the ePrivacy rules from 2002 and 2009 in order to improve protection of fundamental rights of citizens and legal certainty for companies, complementing the GDPR;

([9]) 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).

([10]) 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 (OJ L 201, 31.7.2002, p. 37).

([11]) Proposal 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 (COM(2017)0010).

o

o o

42. Instructs its President to forward this resolution to the Commission, the European Council, the governments and the national parliaments of the Member States, the European Data Protection Board and the European Data Protection Supervisor.