European Economic and Social Committee

TEN/629
Processing of personal data

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
[COM(2017) 8 final – 2017/0002 (COD)]

Rapporteur: **Mr PEGADO LIZ**

Consultation	European Commission, 26/04/2017
Legal basis	Article 16(2) TFEU
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	16/05/2017
Adopted at plenary	31/05/2017
Plenary session No	526
Outcome of vote (for/against/abstentions)	161/0/2

1. Conclusions and recommendations

1.1 The Commission proposal under examination provides a concrete response - in a generally correct and adequate manner from a strictly technical and legal point of view - to the need to adapt the current rules under **Regulation (EC) No 45/2001 and Decision No 1247/2002/EC on the protection of personal data by the Union institutions, bodies, offices and agencies** in line with the new General Data Protection Regulation (GDPR), which will be applicable throughout the EU from 25 May 2018 onwards.

1.2 This does not preclude the EESC from recalling the substance of its comments and recommendations on the now adopted proposal for a GDPR, or from expressing its regret that the final version has not taken them fully into account. Moreover, in view of the speed of technological progress in this domain, it also fears that its late adoption and entry into force may compound the risks of unauthorised appropriation of data and irregularities in data processing and marketing, and that it may become obsolete before it is even implemented. Given that the proposal under consideration is an adaptation of the GDPR to the way the EU institutions operate, the same concerns are relevant here, *mutatis mutandis*, particularly as regards the impenetrable language, which is difficult for the man in the street to understand.

1.3 Furthermore, the EESC is of the view that what happens in the EU institutions should serve as a model for Member State procedures, and therefore believes that special care is called for in drafting the proposal.

1.4 To this end, the EESC considers that issues such as aligning the wording of the proposal on that of the Staff Regulations of Officials of the European Union, procedures for dealing with harassment, cyberbullying and whistleblowing in the EU institutions, its application to the Internet of Things, Big Data and the use of search engines for the purpose of accessing, creating or using personal data, and the placing of personal information published on the websites of the institutions on social networking sites (Facebook, Twitter, Instagram, LinkedIn, etc.) should have been addressed explicitly.

1.5 In the same way, the EESC would like the proposal to have set out both the terms for the security of the IT systems that will support data processing and the guarantees against cyber-attacks and breaches or leaks of such data, ensuring technological neutrality rather than relying purely on the internal regulations specific to each department, and would also like to have better clarification of the connection between data protection and the combating of crime and terrorism without needing to resort to disproportionate or excessive surveillance measures – measures that should in any case always be subject to checks by the European Data Protection Supervisor (EDPS).

1.6 The EESC would also like the proposal to have provided a common definition of the competences, training and suitability criteria required in order to be designated data protection officer, data controller or processor in the EU institutions – again, subject to checks and monitoring by the EDPS.

1.7 The EESC is also of the view that, on account of the specific nature of the data collected and the fact that they have a direct bearing on the privacy of the data subjects - particularly as regards health - tax and social data should be limited to that which is strictly necessary for the purpose, and that the maximum protection and guarantees should be ensured in the processing of particularly sensitive personal data, drawing on international law and the most advanced legislation and best practice to be found in some Member States.

1.8 The EESC highlights the need for the proposal to expressly provide for increased resources for the EDPS, ensuring sufficient staffing and recruitment of people with high levels of knowledge and technical competence in the field of data protection.

1.9 The EESC reiterates, yet again, that the data of legally constituted, collective subjects (undertakings, NGOs, commercial companies, etc.) also need to be afforded protection in the area of data collection and processing.

1.10 Finally, the EESC includes in its specific comments a list of amendments to various provisions which, if adopted, would help to provide more effective protection of personal data in the EU institutions, not only for EU officials but also for the thousands of members of the public with whom they come into contact. It therefore urges the Commission, as well as the EP and the Council, to take these amendments into consideration when drafting the final version of the proposal.

2. Reasons for and objectives of the proposal

2.1 As stated by the Commission in the explanatory memorandum, the aim of the proposal is to **repeal Regulation (EC) No 45/2001**[1] **and Decision No 1247/2002/EC**[2] relating to the protection of personal data by the Union institutions, bodies and offices, with the twin objectives of:

- protecting the fundamental right to data protection;
- guaranteeing the free flow of personal data throughout the EU.

2.2 After a lengthy and difficult process of incubation, the Council and the Parliament finally adopted the General Data Protection Regulation (GDPR)[3], which will become applicable throughout the EU on 25 May 2018. The regulation requires a number of legislative instruments[4] to be adapted, including Regulation (EC) No 45/2001 and Decision No 1247/2002/EC referred to above.

1 OJ L 8, 12.1.2001; the EESC adopted an opinion on this proposal OJ C 51, 23.2.2000, p 48.

2 OJ L 183, 12.7.2002, p. 1.

3 Regulation (EU) 2016/679 of 27.4.2016 (OJ L 119 of 4.5.2016, p. 1). OJ C 229, 31.7.2012, p. 90).

4 COM(2017) 10 final, COM(2017) 9 final.

2.3 The Commission also takes extensive account of the results of surveys and stakeholder consultations, and the evaluation study on the application of the regulation over the past 15 years, and reaches the following specific conclusions:

- Regulation (EC) No 45/2001 could be better enforced through the use of sanctions by the European Data Protection Supervisor (EDPS);
- increased use of the latter's supervisory authority powers could lead to better implementation of data protection rules;
- the regime of notifications and prior checks needs to be simplified in order to increase efficiency and reduce red tape;
- data controllers should adopt a risk management approach and perform risk assessments before carrying out processing operations in order to better implement data retention and security requirements;
- existing rules on the telecommunications sector are outdated and this chapter needs to be aligned on the ePrivacy Directive;
- some of the key definitions in the regulation need to be made clearer. These include the identification of data controllers in the Union institutions, bodies, offices and agencies, the definition of recipients and extension of the obligation of confidentiality to external processors.

2.4 In view of the nature and extent of the modifications to be made to the previous legal instruments, the Commission decided to repeal them in their entirety and replace them with the regulation currently under consideration, which is consistent with the majority of the other measures referred to and would thus enable them to enter into force at the same time as Regulation (EU) 2016/670, pursuant to Article 98 of the latter.

3. General comments

3.1 From a strictly technical and legal point of view, the EESC endorses in principle:

- the need for and timeliness of the initiative now under examination;
- a regulation as the choice of legal instrument;
- the decision to repeal the existing instruments in their entirety;
- the legal basis for adopting it;
- its proven compliance with the criteria of proportionality, subsidiarity and accountability;
- the clarity and structure of the provisions;
- the fact that some concepts, such as "valid consent", are more clearly defined;
- the consistency shown with the other legal instruments with which it is interconnected, in particular Regulation (EU) 2016/679, proposed Regulation COM(2017) 10 final and the Commission's own communication entitled Building a European Data Economy[5];
- the decision to introduce, for the first time, explicit administrative fines for any infringements or failure to comply;
- the steps to strengthen the powers of the EDPS;

5 COM(2017) 9 final.

– the fact that this initiative is not part of the REFIT programme;
– the efforts made to ensure that the regulation is compatible with other fundamental rights, in particular those enshrined in the European Charter of Fundamental Rights on freedom of expression (Article 11); protection of intellectual property (Article 17(2)); the prohibition of any discrimination on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right of access to documents (Article 42); and the right to an effective remedy and to a fair trial (Article 47).

3.2 This is without prejudice to the substance of the EESC's comments and recommendations regarding the proposal for a GDPR[6], now adopted[7], which does not take them fully into account. Moreover, in view of the rapidity of technological developments in this domain, the Committee fears its late adoption and entry into force may further compound the risks of data being misappropriated and misused in processing and marketing, since it may become obsolete before it is even implemented. Given that the proposal under consideration is an adaptation of the GDPR to the way the EU institutions operate, the same concerns apply to it, *mutatis mutandis*, particularly as regards the impenetrable language, which is difficult for the man in the street to understand. It would have been better to present and discuss the two proposals at the same time.

3.3 Furthermore, given that the approach adopted by the EU institutions should serve as a model for Member State procedures, the EESC thinks that a number of issues should have been addressed in this proposal.

3.4 To begin with, it is not clear whether the proposal has taken due account of the Staff Regulations of Officials of the European Union (Regulation No 31 EEC[8]), given the lack of specific legal provisions guaranteeing more effective protection of the personal data of officials and other staff of the institutions regarding their recruitment, career, duration of contract and any subsequent renewals, as well as their appraisals.

3.4.1 If not in this text, measures of a general nature should be laid down containing rules on the health records of officials and their family members, the protection of data created or used by officials and their respective genetic data, the processing and protection of emails, whether sent by members of the public to EU bodies or sent or exchanged by officials of these bodies, either amongst themselves or with outside parties, and the content of these emails and the websites visited[9].

3.4.2 Likewise, instances of harassment, cyberbullying and whistleblowing in the EU institutions warrant special treatment, notwithstanding the provisions of Article 68.

---

6 OJ C 229, 31.7.2012, p. 90.

7 Regulation (EU) 2016/679 of 27.4.2016 in OJ L 119 of 4.5.2016, p. 1.

8 OJ L 45, 14.6.1962, and subsequent amendments.

9 An example of this is the collection of opinions and recommendations of the Belgian Privacy Commission in its brochure on privacy in the workplace (Avis et Recommandations de la Commission de la Vie privée de la Belgique sur la vie privée sur le lieu de travail), January 2013.

3.4.3 The EESC also queries the terms of application of the proposal under examination and of Regulation (EU) 2016/679 as regards the Internet of Things, Big Data and the use of search engines for the purpose of accessing, creating or using personal data, and putting personal information published on the websites of the institutions on social networking sites (Facebook, Twitter, Instagram, LinkedIn, etc.), regardless of whether the data subject has given their explicit consent.

3.5 In addition to the reference to the confidentiality of electronic communications in Article 34 of the proposed regulation, the EESC would like the Commission proposal to have set out both the terms for the security of the IT systems that will support the processing of data and the guarantees against cyber-attacks and breaches or leaks of such data[10], ensuring technological neutrality rather than relying purely on the internal regulations specific to each individual department. It would also like to have better clarification of the connection between data protection and the combating of crime and terrorism without needing to resort to disproportionate or excessive surveillance measures – measures that should in any event always be subject to checks by the EDPS.

3.6 The EESC emphasises that the interconnection of personal data in the EU institutions cannot be left solely to the principle of accountability set out in recital 16, and to this end urges the Commission to introduce a specific rule stipulating that an interconnection can only be made with the authorisation of the EDPS, on request by the controller or jointly with the processor.

3.7 However, without prejudice to recital 51 of the preamble and Article 44(3) of the proposal, the EESC would also like the Commission to have provided a common definition of the competences, training and suitability criteria required in order to be designated data protection officer, data controller or processor in the EU institutions[11]. Any breaches of these functions should be subject to sanctions in the form of disciplinary, civil or criminal proceedings that are a genuine deterrent and are set out in the proposal – again, subject to checks and monitoring by the EDPS.

3.8 Whilst recognising that this proposal raises the level of protection compared to that prevailing under Regulation (EC) No 45/2001 currently in force, the EESC is of the view that, on account of the specific nature of the data collected and the fact that such data have a direct bearing on the privacy of the data subjects - particularly as regards health - tax and social data should be limited to that which is strictly necessary for the purpose and that the maximum protection and guarantees should be ensured in the processing of personal data, drawing on international law and the most advanced legislation and best practice to be found in some Member States[12].

---

10 As set out, for example, in the own-initiative recommendation on security measures to be complied with to prevent data leaks (Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données), Belgian Privacy Commission, 1/2013, 21 January 2013.

11 As mentioned, for example, in the Guidelines on Data Protection Officers, WP 243 on Article 29, 13 December 2016.

12 By way of example, see the Portuguese law on data protection (Law 67/98 of 26 October 1998).

3.9 Whilst cognisant of the fact that both Regulation (EU) 2016/679 and the proposal under consideration apply exclusively to data for which the subjects are individuals, it reiterates that the data of legally constituted, collective subjects (undertakings, NGOs, commercial companies, etc.), also need to be afforded protection in terms of collection and processing.

4. Specific comments

4.1 Analysis of the text raises a number of doubts and reservations in the light of the fundamental principles of the right to privacy set out in the EU Charter of Fundamental Rights, the principle of proportionality and the precautionary principle.

4.2 Article 3

Paragraph 2(a) defines the Union institutions and bodies as the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, TFEU or the Euratom Treaty. The EESC wonders whether the definition also includes working parties, advisory councils, committees, platforms, other groups, etc., as well as international computer networks in which the institutions participate, but do not own.

4.3 Article 4

4.3.1 In view of the fact that the regulation currently under discussion applies to data processed within the EU institutions, the EESC would like the principle of non-discrimination to be expressly introduced, given the nature of the data being processed.

4.3.2 With respect to Article 4(1)(b) on processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, this should be subject to prior authorisation by the European Data Protection Supervisor, something which is not provided for in Article 58.

4.3.3 Finally, there should be an expressly worded provision that is the equivalent of Article 7 of Regulation (EC) 45/2001, currently in force, concerning the transfer of data between the EU institutions.

4.4 Article 5

4.4.1 It is not clear why Article 5(1)(b) of the proposed regulation is not subject to the requirement set out in paragraph 2 of that article, unlike indents (c) and (e) of Article 6, both of which are subject to the provision laid down in Article 3 of the GDPR.

4.4.2 The EESC considers that indent (d) ought to include a reference to the fact that consent should be subject to the principle of good faith.

4.5 **Article 6**

4.5.1 Application of this article should always be subject to authorisation by the European Data Protection Supervisor.

4.5.2 In such cases, the data subject should always be informed prior to any data collection or at the moment of any new decision, and should possibly have the option of requesting rectification, the right to object, erasure or restriction of processing.

4.6 **Article 8**

4.6.1 In the EESC's view, the exception to the rule of the validity of consent for children under the age of 16 (between 13 and 16 years of age) – which is already an aberration in itself – is only admissible for Member States for cultural reasons of domestic law (Article 8 of the GDPR), but should not be admissible as a rule for the EU institutions, which establishes the age of consent at 13 years (Article 8(1).

4.6.2 Furthermore, it has not been specified how in practice the EDPS is to address "specific attention" to children, as referred to in Article 58(1)(b), particularly when it comes to the list of users referred to in Article 36 when data is publicly accessible.

4.7 **Article 10**

4.7.1 Paragraph 1 should also include political affiliation (which is not the same thing as political opinion) and private life.

4.7.2 In paragraph 2(b), even where the purpose is to carry out the obligations and exercise specific rights of the data subject, the latter should always be given prior notice.

4.7.3 In paragraph 2(d), processing should only be carried out with the consent of the data subject.

4.7.4 Indent (e) should only constitute an exception when it can be legitimately surmised from the subject's statements that consent has been given to the processing of data.

4.8 **Article 14**

Given that the EU institutions are not authorised to charge fees for the services provided, refusal to act on a request may only be adopted as a last resort.

4.9 **Articles 15, 16 and 17**

4.9.1 With regard to further information, as referred to in Article 15(2), it should be added that the data subject should be informed as to whether the controller's reply to the request is of an obligatory or optional nature and of the possible consequences of failure to reply.

4.9.2 Where data is collected from open networks, the data subject must always be informed that their personal data may be circulated on networks without security measures, running the risk of being seen and used by unauthorised third parties.

4.9.3 The right provided for in Article 17(1) should be exercised freely and without restriction, at reasonable intervals, swiftly or immediately and at no cost.

4.9.4 The EESC would suggest that it should also be a requirement for the data subject to receive confirmation as to whether data regarding himself or herself are being processed or not.

4.9.5 The information referred to in Article 17(1) should be provided in an intelligible, clear and comprehensible manner, particularly as regards data to be processed and any information on the origin of such data.

4.10 **Article 21**

Our understanding of the fact that provisions identical to those set out in Article 21(2) and (3) of the GDPR are to be excluded from the proposed regulation is that the data can never be processed for the purpose of direct marketing, which would be laudable. However, this interpretation is uncertain and the wording of the provision should make this quite clear.

4.11 **Article 24**

4.11.1 The EESC believes that it should be added to paragraph 2(c) that consent only occurs after express information is provided of the repercussions of the legal effects of decisions on the data subject, as only then will the consent be duly informed.

4.11.2 As regards paragraph 3, the EESC is of the view that appropriate measures should be drawn up by the European Data Protection Supervisor and not by the data controller.

4.12 **Article 25**

4.12.1 The EESC is concerned that the wording of Article 25 in the proposed regulation offers too broad an interpretation of Article 23 of the GDPR as regards restrictions on the application of the principles establishing the fundamental rights of the data subject. It would advise the Commission to subject it to a critical review, analysing the various paragraphs according to strict criteria, possibly setting out the scope of each indent, particularly in respect of the limitation of the right to confidentiality in electronic communications networks provided for in Article 7 of the Charter of Fundamental Rights, referred to in the ePrivacy Directive and retained in the proposed regulation being assessed in another EESC opinion.

4.12.2 The EESC is completely opposed to the possibility granted in Article 25(2) allowing EU institutions and bodies to restrict the application of limitations on the rights of data subjects to legal acts for which they have not given their express consent. The same applies to Article 34.

4.13 **Article 26**

It should be made clear that personal data controllers, processors and persons who, in the exercise of their duties, gain knowledge of the personal data processed, shall be bound by professional secrecy, even after termination of their duties and for a reasonable period.

4.14 **Articles 29 and 39**

Whilst it is evident that the provisions set out in Articles 24(3) and 40 et seq. of the GDPR have not been included in the proposed regulation (codes of conduct), as expressly pointed out in the recital of the preamble relating to Article 26, it does not seem appropriate that in Articles 29(5) and 39(7) of the proposed regulation it is accepted that mere adherence to a code of conduct referred to in Article 40 of the GDPR can be considered a sufficient guarantee of the performance of tasks by a processor that is not a Union institution or body.

4.15 **Article 31**

The EESC believes that the mere "possibility" provided for in Article 31(5) should rather be converted into an "obligation" to keep records of processing activities in a publicly accessible central register.

4.16 **Article 33**

The EESC further suggests that the controller and processor should exercise controls over data media and the inputting, use and transmission of data, in order to:

- prevent any unauthorised person from having access to installations used for the processing of such data;
- prevent the reading, copying, modification or removal of data media by unauthorised persons;
- prevent unauthorised input and unauthorised gaining of knowledge, modification or removal of personal data;
- prevent the use of automated data processing systems by unauthorised persons using data transmission equipment;
- ensure that it is possible to verify those bodies to which personal data may be communicated;
- ensure that authorised persons may only gain access to data covered by the requirement for prior authorisation.

4.17 **Article 34**

The EESC hopes that this article will be in keeping with the provisions of the proposed ePrivacy Directive and that the EU institutions and bodies will be subject to the scrutiny of the EDPS regarding the confidentiality of electronic communications.

4.18 **Article 42**

The EESC is concerned that the term "following" in paragraph 1 may be understood to mean an obligation to consult only after adoption of the act, and that consultation will no longer take place even on an informal basis, as is the case today.

4.19 **Article 44**

The EESC considers that in principle only officials should be appointed as data protection officers. If under exceptional circumstances this is not possible, data protection officers should in any event be recruited on the basis of the public procurement rules on service provision and be subject to the scrutiny of the EDPS.

4.20 **Article 45**

4.20.1 If, notwithstanding the above and where the data protection officer is not an official, in view of the nature of his/her office, it should be possible to dismiss him/her at any time, a favourable opinion of the EDPS being sufficient for this purpose (Article 45(8) of the regulation).

4.20.2 It takes the view that the term of the mandate should be 5 years and should be renewable only once.

4.21 **Article 56**

In the light of recent, well-known events involving top officials from the institutions, we would recommend establishing criteria on incompatibility and impediments for a reasonable period of time with regard to the performance of certain functions, particularly in private companies, after the term of office of the person concerned has ended.

4.22 **Article 59**

In some languages, notably English, the term "actions" used in paragraph 5 is too limited and should be replaced by the term "proceedings" (the concept has been correctly translated in the Portuguese version).

4.23 **Article 63**

With regard to paragraph 3, and in the light of the sensitivity of the subject matter of this proposal, the EESC considers that the principle of tacit rejection should be reversed, thereby obliging the European Data Protection Supervisor to reply explicitly to all complaints lodged with him or her. Failing this, they will be considered to be upheld.

4.24 **Article 65**

As mentioned in its opinion on the original proposal for a regulation (Regulation (EU) 2016/679), the EESC would emphasise that, in addition to the terms of Article 67, provision

should be made in the event of a breach of personal data for allowing a response in the form of a group action, without the need for an individual action, since generally speaking when such breaches occur, they affect not just a single individual but a sometimes indeterminate group of people.

4.25 The proposal for a regulation is riddled with expressions or concepts of an ambiguous nature. These should be revised and replaced. Examples include "to the extent possible", "if possible", "without delay", "high risk", "due account", "reasonable time limit" and "particular importance".

Brussels, 31 May 2017

Georges DASSIS
The president of the European Economic and Social Committee