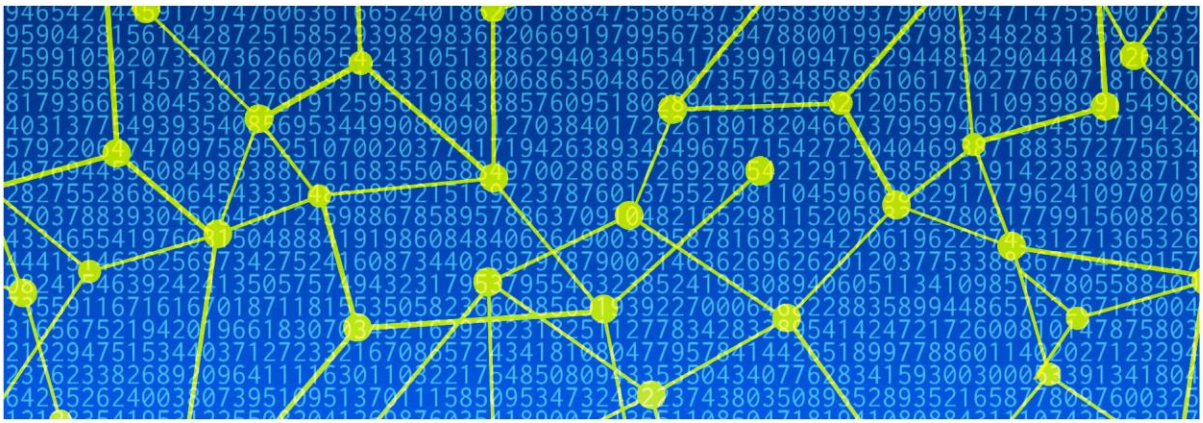

EUROPEAN DATA PROTECTION SUPERVISOR

Guidance Paper

Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations

EDPS Guidance on Articles 14 - 16 of the proposal for a Regulation 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

EDPS

15/01/2017

TABLE OF CONTENTS

I. Contents

1. INTRODUCTION AND BACKGROUND

1. On 10 January 2017, the European Commission adopted a 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[1] ("the **Proposal**").

2. The Proposal is part of a new generation of data protection standards being promulgated by the European Union. The adoption of the General Data Protection Regulation (GDPR) and the Directive for the police and justice sectors represented the most ambitious endeavour of the EU legislator so far to secure the fundamental rights of the individual in the digital era. Now is the time for EU institutions to lead by example in the rules that they apply to themselves as data controllers and data processors.

3. Regulation 45/2001 played a vanguard role, inter alia in providing directly applicable obligations for controllers and rights for data subjects, all supervised by a clearly independent supervisory body. The EU now must ensure consistency with the GDPR through an emphasis on accountability and safeguards for individuals rather than procedures. Some divergence of rules applicable to EU institutions data processing is justifiable, in the same way as public sector exceptions have been included in the GDPR, but this must be kept to a minimum. Essential however, from the perspective of the individual, is that the common principles throughout the EU data protection framework be applied consistently irrespective of who happens to be the data controller. It is also essential that the whole framework applies at the same time, that is, by 25May 2018, deadline for GDPR to be fully applicable.

4. This Guidance Paper focusses as much as possible on **Articles 14 to 16** of the Proposal[2], i.e. on providing transparent information, communication and modalities for the exercise of the rights of the data subject. It thus closes a gap, as the scope of the EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data[3] ("GL DS rights") did not encompass the information of data subjects under Articles 11 and 12 of Regulation 45/2001[4] ("Regulation 45/2001"). Nonetheless, the GL DS rights continue to provide some guidance, where the provisions of the Proposal reflect those of Regulation 45/2001. For a **summary of main changes** with relevance for the scope of this Guidance Paper, please see Annex 1.

5. For Data Protection Officers (DPOs)[5] and members of staff responsible for a particular processing operation, the **revision of existing data protection statements** (and thus the underlying processing operations) is considered an ideal first step to prepare for the entry

[1] COM(2017) 8 final; 2017/0002 (COD), see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0008&from=EN.
[2] Chapter III, Rights of the Data Subject, Section 1 ("Transparency and Modalities") and partially Section 2 (only with a view to providing information to data subjects).
[3] See https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf.
[4] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF.
[5] Under Article 46 c) of the Proposal, ensuring "*that data subjects are informed of their rights and obligations pursuant to this Regulation*" is part of the tasks of the DPO.

into force of the new legal basis, new data subject rights and (partially) tighter deadlines applying under the Proposal as of 25 May 2018[6]. For suggestions by other DPAs, please see Annex 2.

6. As stated in his Opinion 5/2017, the EDPS advocates **aligning** the future rules applicable to personal data processing by EU institutions **with the provisions of the GDPR**[7], unless narrowly interpreted specificities of the public sector justify otherwise. This Guidance Paper therefore complements the **upcoming WP 29 Guidelines on Transparency**.

7. Apart from substantive alignment with the GDPR, it is essential that the revised rules become fully applicable at the same time as the GDPR i.e. on 25 May 2018. The existing network of Data Protection Officers ("DPO") provides for an efficient channel of information sharing and cooperation. Consequently, the EDPS is confident that compliance could be achieved following a relatively **short transition period**, e.g. three months ought to be sufficient to revise the data protection statements.

8. The **principle of accountability** which underpins both, the GDPR as well as the Proposal, goes beyond simple compliance with the rules and implies a culture change. To facilitate the transition, the EDPS launched an "accountability project"[8]. In this context, the EDPS was in contact over the course of 2016 and 2017 with seven key EU institutions to help prepare in due time for the GDPR application and, based on the exchange of views during the DPO meeting in Tallinn in May 2017, separate guidance documents will be provided by the EDPS.

[6] EDPS Opinion 5/2017: "*...the EDPS encourages the EU legislator to reach agreement on the Proposal as swiftly as possible so as to allow EU institutions to benefit from a reasonable transition period before the new Regulation can become fully applicable*".
[7] Under Article 98 of the GDPR, "*The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data*."
[8] See https://edps.europa.eu/press-publications/press-news/blog/accountability-initiative_en.

2. EXECUTIVE SUMMARY

New rules on data protection will apply throughout Europa as of 25 May 2018. EU institutions and bodies are no exception: the currently applicable rules (Regulation (EC) 45/2001) will be replaced by a new Regulation as of the same day.

As staff member responsible for processing personal data on behalf of your EU institution or body, you will need to implement these revised data protection rules as of 25 May 2018.

As always, the Data Protection Officer (and Data Protection Coordinator where applicable) of your employer are your first port of call when resolving any data protection challenge you face. But in the light of the accountability principle, it is not your Data Protection Officer or your Data Protection Coordinator who is responsible for correctly implementing the new rules. This responsibility lies with you as staff member responsible for processing personal data on behalf of the EU institution or body you work for.

This Guidance Paper is meant to help you help you get started to fulfill your new obligations.

It focusses on providing transparent information to those concerned by your data processing, on how to communicat about your use of personal data with those concerned and the modalities that apply to the exercise of their rights. For an overview of your new obligations regarding these aspects, please consult Annex 1 of this document.

The EDPS considers the revision of existing data protection statements an ideal first step to prepare for the entry into force of the new legal basis, new rights for those whose personal data you use and some tighter deadlines that apply under the new rules.

We hope you will find the guidance provided by this Guidance Paper useful. More guidance and training on other aspects of the new rules is available - please contact your Data Protection Officer for more information.

3. ARTICLE 14 - Transparent information, communication and modalities for the exercise of the rights of the data subject

2.1 General remarks

7. Fair processing relates to Articles 15 and 16 of the Proposal: There should be no hidden processing operations. Fairness relates closely to transparency, ensures predictability and enables user control. Recital 28 of the Proposal further outlines the following: "*The **principles of fair and transparent processing** require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable*."

2.2 Article 14(1): "The controller shall take appropriate measures..."

> The controller shall take appropriate measures to provide any information referred to in Articles 15 and 16 and any communication under Articles 17 to 24 and 38 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2.2.1 "...concise, transparent, intelligible and easily accessible form"

8. According to Recital 15 of the Proposal, "*The principle of transparency requires that any information and communication relating to the processing of those personal data be **easily accessible** ... That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*." (emphasis added)

9. **Communication channel**: Depending on the target audience (staff, general public, bidders etc.), the EDPS has suggested using the most adapted channel of communication and multiplying these communication channels where possible. E.g. in the EDPS Guidelines on Video-surveillance[9], the EDPS recommends a multi-layer approach combining on-the-spot

[9] See https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

notices and a detailed data protection notice posted on the Institution's intranet and internet sites.

10. **Easily accessible**: In a complaint case (not published), the EDPS found that "*The controller shall provide the data subject with the relevant information and this requirement has not been met if the data subject has not been informed of the location of the privacy statement or even of the existence of the same. Furthermore, the privacy statement cannot be considered to be readily accessible if it is not to be found in direct relation to other relevant information on the processing operation. The fact that the privacy statement was published on the webpage of the DPO is not enough in this respect*"[10].

11. **Format**: The right of access is usually granted by providing paper or electronic copies of the data subject's personal data[11]. Sometimes the format of the data to be transmitted must be adapted to the data subject (such as in the case of a blind person who needs electronic copies[12]). The Proposal in Article 14(1), last sentence also foresees that the information may be provided orally, when requested by the data subject (and provided that the identity of the data subject is proven by other means[13]).

2.2.2 "...using clear and plain language"

12. According to Recital 15 of the Proposal, "*The principle of transparency requires that any information and communication relating to the processing of those personal data be ...**easy to understand, and that clear and plain language be used**. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*." (emphasis added)

13. Some general pieces of advice include the following[14]:

- adopt a simple style and straightforward language that your target audience will find easy to understand (considering that most members of your audience are people whose first language is not the one in which you are giving the information);
- do not assume that everybody has the same level of understanding as you;
- avoid confusing terminology or legalistic language;
- ensure your data protection statements are consistent across multiple platforms and enable rapid updates to them all when needed.

[10] "Location" in the sense of this statement is the e-link under which the privacy statement is made available.
[11] See also GL DS rights, p. 17 on Article 13 (see https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf).
[12] See case 2009-0151 (not published).
[13] E.g. where the data subject displays obvious insider knowledge (usually only available to the individual concerned) and can be called back under a telephone number on file and previously indicated by the data subject.
[14] Look for more ideas here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/how-should-you-write-a-privacy-notice/ (ICO).

14. **Best practice examples** include the Annexes to the Working Party 29 Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities[15] or the European Ombudsman's policy on dealing with personal data in a complaint or an inquiry that have not been obtained from the data subject[16].

2.2.3 "...any information addressed specifically to a child"

15. See also Article 8 and Recital 21 of the Proposal. The EDPS is only aware of one case[17] in which EU institutions provide information society services to children, which renders Article 8 of the Proposal applicable. Nevertheless, given the broad scope of the Proposal and the large variety of EU institutions and their processing operations, it cannot be excluded that such a provision becomes more relevant in the future[18].

2.3 Article 14(2) "...facilitate the exercise of data subject rights..."

> The controller shall facilitate the exercise of data subject rights under Articles 17 to 24. In the cases referred to in Article 12(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 17 to 24, unless the controller demonstrates that it is not in a position to identify the data subject.

15. Recital 2 of Proposal refers to the fact that Regulation 45/2001 provides natural persons with legally enforceable rights and Recital 27 of the Proposal stipulates that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation*". As noted in the GL DS rights (p. 9), this implies that the data processing **obligations of the controllers need to be specified** and that the controller -regularly the EU institution responsible for the data processing operation- is subject to a **positive obligation to act** in order to allow individuals to exercise their right.

2.4 Article 14(3)

> The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

2.4.1 "...without undue delay and in any event within one month of receipt..."

16. Recital 27 of the Proposal: "...*The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month*...".As regards **CCTV footage**, the EDPS Guidelines on Video-surveillance[19] (p. 46/47) note that, whenever possible, access should be given within **15 calendar days**. If this is not possible,

---

[15] WP151, see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_en.pdf.
[16] See https://www.ombudsman.europa.eu/en/resources/dataprotection/document.faces/en/70851/html.bookmark.
[17] See http://europa.eu/kids-corner/index_en.htm.
[18] See EDPS Opinion 5/2017(see https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf), §20, e.g. in the context of awareness raising activities targeting children.
[19] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf ; see also GL DS rights, p. 16.

another meaningful response (not merely an acknowledgement of receipt) should be given within 15 calendar days.

17. **Extension by two further months**: There are no hard and fast rules and no precedent cases (yet) as to when such extension might be "necessary", in particular with a view to the "complexity" and "number of the requests". However, the EDPS had previously acknowledged[20] (in the context of access requests under Article 13 of Regulation 45/2001, emphasis added) that "*...whilst the level of detail has to enable the data subject to evaluate the accuracy of the data and the lawfulness of the processing,* ***the burden of the task for the controller has to be kept in mind***[21]."

18. Article 17 of the **European Code of Good Administrative Behaviour**[22] stipulates as reasonable time-limit for taking decisions "*...in any case no later than two months from the date of receipt... If a request or a complaint to the institution cannot, because of the complexity of the matters which it raises, be decided upon within the above mentioned time-limit, the official shall inform the author as soon as possible. In such a case,* ***a definitive decision should be communicated to the author in the shortest possible time***."

19. Although Article 14(3) of the Proposal does not contain an equivalent to the sentence in Article 14(5) of the Proposal according to which "*controller shall bear the burden of demonstrating*" the particular nature of the request, the principle of **accountability implies** that whichever reasoning led the controller to conclude that such extension might be "necessary", in particular with a view to the "complexity" and "number of the requests", must be **properly documented**.

2.4.2 Electronic means

20. As expressly noted by the EDPS Guidelines on staff recruitment[23] (p. 7/8), but not limited to instances of staff recruitment, a request for access may be submitted in any written format[24]. For example, requests can be made by e-mail[25] or by filling in an access request form, although the use of the latter cannot be made mandatory.

2.5 Article 14(4): complaint with the EDPS / judicial remedy

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the European Data Protection Supervisor and seeking a judicial remedy.

21. **Lodging a complaint with the EDPS**: Article 20(3) of the Regulation 45/2001 already stipulated that where a restriction provided for by Article 20(1) of Regulation 45/2001 is imposed, the data subject shall be informed of his or her right to have recourse to the EDPS.

[20] GL DS rights p. 17.
[21] See case 2009-0550 (see https://edps.europa.eu/sites/edp/files/publication/09-10-01_olaf_right_access_en.pdf).
[22] See https://www.ombudsman.europa.eu/resources/code.faces#/page/5, which is grounded in Article 41 of the EU Charter of Fundamental Rights.
[23] See https://edps.europa.eu/sites/edp/files/publication/08-10-10_guidelines_staff_recruitment_en.pdf.
[24] See also GL DS rights p. 16.
[25] In which case there is a need to consider security measures, e.g. email ecryption or https protocol for the submission via a dedicated online portal.

Existing formulations can thus be reused, if they have worked for you (and your data subjects).

22. Article 19 of the **European Code of Good Administrative Behaviour**[26] stipulates on the indication of appeal possibilities that "*A decision of the institution which may adversely affect the rights or interests of a private person shall contain an indication of the appeal possibilities available for challenging the decision. It shall in particular indicate the nature of the remedies, the bodies before which they can be exercised, and the time-limits for exercising them*".

2.6 Article 14(5): "free of charge", "manifestly unfounded", "excessive"

> Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 38 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request.
>
> The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

23. "...**manifestly unfounded**": For the requirement of a case-by-case analysis, see below §25.

24. "...**excessive, in particular because of their repetitive character**": As mentioned above (§17), the EDPS had previously acknowledged[27] (in the context of access requests under Article 13 of Regulation 45/2001, emphasis added) that "*...whilst the level of detail has to enable the data subject to evaluate the accuracy of the data and the lawfulness of the processing, **the burden of the task for the controller has to be kept in mind***[28]."

25. A similar provision to Article 14(5), 2nd sentence can be found in Article 14(3) of the **European Code of Good Administrative Behaviour**[29] (emphasis added): "*No acknowledgement of receipt and no reply need be sent in cases where letters or complaints are abusive because of their excessive number or because of their repetitive or **pointless character***." Insofar, the European Ombudsman has highlighted that "*any decision reaching the conclusion that correspondence sent by a citizen is improper, for example, because it is repetitive, abusive and/or pointless, must be based on an individual and substantive assessment of a citizen's correspondence*"[30].

2.7 Article 14(6): "...reasonable doubts concerning the identity..."

> Without prejudice to Article 12, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 17 to 23, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

[26] See https://www.ombudsman.europa.eu/resources/code.faces#/page/5, which is grounded in Article 41 of the EU Charter of Fundamental Rights.
[27] GL DS rights p. 17.
[28] See case 2009-0550 (see https://edps.europa.eu/sites/edp/files/publication/09-10-01_olaf_right_access_en.pdf).
[29] See https://www.ombudsman.europa.eu/resources/code.faces#/page/5, which is grounded in Article 41 of the EU Charter of Fundamental Rights.
[30] See §29 of Decision of the European Ombudsman closing his own-initiative inquiry OI/7/2011/EIS concerning the European Commission, https://www.ombudsman.europa.eu/cases/decision.faces/en/51043/html.bookmark.

26. "...**additional information necessary to confirm the identity of the data subject**": Recital 25 Proposal: "*If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.*"

27. **Copy of an identification document**: An EU institution consulted[31] the EDPS on the scanning of ID cards to identify access requestor. Our main elements of guidance resulting from these reflections can be summarized as follows (§§28-30); please note that this reply was only *informal* advice provided at staff level (i.e. not an official and publically available EDPS Opinion).

28. **Data minimisation:** Requestors should be invited to provide a copy of an identification document for confirmation of their identity. For this purpose, normally only a **limited number of personal data** (identity document number, country of issue, first and last name, address, date and place of birth and document expiration date) needs to be visible on the copy of the identification document. In principle, all **other data** on the copy of the identification document (e.g. the photo, any personal characteristics,) **can be blacked out** on the copy (but does not have to be blackened out). This also resonates with the requirements stipulated in Recitals 57 and 64 GDPR:

    - Recital 57 GDPR: *"If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller."*

    - Recital 64 GDPR: *"The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests."*

29. **Purpose limitation:** The principle of purpose limitation suggests that the personal data thus obtained can only be used to verify the requestor's identity; they cannot become part of the data inventory of the EU institution. The **retention period** for the copy of an identification document should be limited to the period required to establish the identity of the requestor, including for cases of doubt.

30. **Information to data subjects:** The EDPS informs data subjects under Article 11 of Regulation 45/2001 along the following lines on the EDPS website[32]:

[31] Informal consultation by the European Commission, case 2016-0758.
[32] See https://edps.europa.eu/about/data-protection-within-edps/data-protection-officer-edps_en.

How to exercise your data protection rights at the EDPS

- *If the EDPS is processing your personal data and you would like to exercise your data protection rights, please send us a written request;*
- *In principle, we cannot accept verbal requests (telephone or face-to-face) as we may not be able to deal with your request immediately without first analysing it and reliably identifying you;*
- *You can send your request to the EDPS by post in a sealed envelope or use our contact form;*
- *Your request should contain a detailed, accurate description of the data you want access to;*
- *You must provide a copy of an identification document to confirm your identity, for example, an ID card or passport. The document should contain an identification number, country of issue, period of validity, your name, address and date of birth;*
- *Any other data contained in the copy of the identification document such as a photo or any personal characteristics, may be blacked out;*
- *Our use of the information on your identification document is strictly limited: the data will only be used to verify your identity and will not be stored for longer than needed for this purpose;*
- *In principle, we will not accept other means of assuring your identity. Should you wish to propose alternatives, we will assess their adequacy on a case-by-case basis;*
- *You can read our data protection notice for more information on how we deal with your personal data when handling a written request from you.*

2.8 Article 14(7)+(8): use of icons

7. The information to be provided to data subjects pursuant to Articles 15 and 16 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. If the Commission adopts delegated acts pursuant to Article 12(8) of Regulation (EU) 2016/679 determining the information to be presented by the icons and the procedures for providing standardised icons, Union institutions and bodies shall, where appropriate, provide the information pursuant to Articles 15 and 16 in combination with such standardised icons.

31. Recital 28 of the Proposal stipulates that: "*...information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be* ***machine-readable***." Please consider that most aspects of data protection are difficult to picture and does not necessarily involve binary choices ("Y/N"). The use of icons in the **absence of standardised icons** (Article 14(8) of the Proposal) is thus probably not a good idea.

4. ARTICLE 15 - Information to be provided where personal data are collected from the data subject

2.9 General remarks

32. Recital 29 of the Proposal states that "*The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller*

intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided."

33. Like its predecessor (Article 11 of Regulation 45/2001), this Article contains a "shopping list" of elements to be provided to the data subject upfront, at the time of collection. The **objective is twofold**: this information is a precondition for the data subject to verify the lawfulness of the processing as well as for the further exercise of other data subject rights[33].

34. Article 15 of the Proposal applies in cases where **data are collected from the data subject** with their active participation. For example[34], data collected in an application form, or recorded calls to an emergency line after an automated announcement about the recording before the call is passed to an operator.

35. Note the **differences to Article 16 of the Proposal** (same as for the predecessor provisions Articles 11 and 12 of Regulation 45/2001):
    - there is no need to inform about the categories of data: the person already knows which data he/she provided, e.g. in replies on a questionnaire;
    - no need to inform about the sources;
    - no exception like Article 16(5)(b) of the Proposal for "disproportionate effort" to inform data subject: if collecting directly from a data subject, providing the information at the same time cannot be construed to be disproportionate.

36. As for the predecessor provisions Articles 11 and 12 of Regulation 45/2001[35], note that many processing operations will **combine situations under Articles 15 and 16** of the Proposal. Example: in selection and recruitment procedures, personal data provided in application forms falls under Article 15 of the Proposal, while the notes of the selection panel fall under Article 16 of the Proposal. In such mixed cases, both Articles need to be complied with.

37. For further guidance on the **concept of personal data**, see the GL DS rights, pp. 12+13. Recital 6 of the Proposal excludes deceased persons; however, processing personal data of deceased persons might also have impact on living persons (e.g. information on hereditary diseases), in particular family members.

2.10 Article 15(1): "Where personal data...are collected from the data subject..."

> Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
>
> (a) the identity and the contact details of the controller;

[33] See for Articles 11 and 12 of Regulation 45/2001: GL DS rights, p. 8.
[34] Further example: Working Party 29 Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities WP151: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_en.pdf.
[35] For a distinction between those two Articles, see EDPS cases 2013-0297 and 2008-0491 (see https://edps.europa.eu/sites/edp/files/publication/13-06-20_eib_en.pdf and https://edps.europa.eu/sites/edp/files/publication/08-11-19_commission_appels_interventions_en.pdf respectively).

(b) the contact details of the data protection officer;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the recipients or categories of recipients of the personal data, if any;

(e) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

38. "**(b) the contact details of the data protection officer**": A novelty compared to Regulation 45/2001, which the EDPS in Opinion 5/2017[36] links to the "*increased transparency of the DPO function*". In the EDPS Video-surveillance Guidelines (p. 64/Appendix 2), regarding the contact details of the security unit, the EDPS recommends referring to **telephone number and email address** of the security unit. In one case[37], where an EU institution had *justified* the intention of refraining from giving a telephone number to avoid "prank calls", the EDPS accepted and noted the existence of an email address provided in the on-the-spot CCTV notice.

39. "**(d) the recipients or categories of recipients of the personal data**": Already according to Article 2(g) of Regulation 45/2001, entities that receive data in the framework of a particular inquiry are not to be considered recipients, which represents an exemption from the information obligation under Articles 11(1)(c) and 12(1)(d) of Regulation 45/2001[38]. In the light of Article 4(9) GDPR (via Article 3(1)(a) of the Proposal), the same applies under the Proposal. There is no need to inform about the fact that in such inquiries, e.g. Courts, the Ombudsman, OLAF, the IAS or the EDPS may receive data, as otherwise these entities would have to be mentioned in every single data protection notice.

40. **"(e)** ... controller **intends to transfer / ... transfers"**: Another novelty compared to Regulation 45/2001. For general guidance on transfers, including on what can be considered "*appropriate or suitable safeguards*", see EDPS position paper on "The transfer of personal data to third countries and international organisations by EU institutions and bodies"[39].

2.11 Article 15(2): "In addition to the information referred to in paragraph 1..."

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

[36] See https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf, §34.
[37] Case 2012-0031.
[38] With regard to Article 2(g) of the Regulation, authorities which would only receive data in the context of specific targeted inquiries are not considered "recipients" and do not need to be mentioned in the data protection statement. This is an exception to the information obligations in Articles 11 and 12 of the Regulation, but not to the rules on transfers in Articles 7 to 9 of the Regulation. In practice, this means that authorities such as the OLAF, the European Ombudsman or the EDPS do not need to be mentioned in the data protection statement (unless the processing operation in question involves transfers to these organisations as part of the procedure); however, the applicable rules on transfers will always need to be respected.
[39] See https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf; additional information on the transfer of personal data to third countries and international organisations by EU institutions and bodies was collected in the context of the Survey 2017 and is likely to be published later in 2017.

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;

(c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with the European Data Protection Supervisor;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

41. Items listed in Article 15(1) of the Proposal are mandatory, except where the data subject already has them. The items under Article 15(2) of the Proposal should be included where they are necessary for the fairness and transparency of the processing. The amount of further information needed depends on the processing operations in questions.

2.12 Article 15(3): further processing

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

42. . ...

2.13 Article 15(4): Exception to paragraphs 1, 2 and 3

Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

43. . ...

5. ARTICLE 16 - Information to be provided where personal data have not been obtained from the data subject

2.14 General remarks

44. Article 16 of the Proposal deals with cases where personal data have been obtained from **sources other than the data subject**, e.g. from other persons (example: data about alleged harasser provided by alleged victim in anti-harassment procedures), received from third parties (e.g. referral to OLAF) or collected from public sources.

45. There are two main differences to Article 15 of the Proposal:

- Data subjects must be informed about the categories of data processed and, where possible, their source;
- Paragraph 5 provides a carve-out for not informing data subjects in certain cases.

2.15 Article 16(1): "Where personal data have not been obtained from the data subject..."

> Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
>
> (a) the identity and the contact details of the controller;
>
> (b) the contact details of the data protection officer;
>
> (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
>
> (d) the categories of personal data concerned;
>
> (e) the recipients or categories of recipients of the personal data, if any;
>
> (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 49, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

46. "...**(b) the contact details of the data protection officer**": A novelty compared to Regulation 45/2001, see §38 above.

47. Controllers have to *actively provide* this information to data subjects; mere publication of a data protection notice is as a rule not enough.

2.16 Article 16(2): "In addition to the information referred to in paragraph 1..."

> In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:
>
> (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
>
> (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;
>
> (c) where the processing is based on point (d) of Article 5(1) or point (a) of Article 10(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
>
> (d) the right to lodge a complaint with the European Data Protection Supervisor;
>
> (e) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
>
> (f) the existence of automated decision-making, including profiling, referred to in Article 24 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

48. **Article 16(2)(b): Existence of other data subject rights**: As already noted in the GL DS Rights (p. 9), merely mentioning these rights is insufficient[40]: The data subject is entitled to receive adequate information as to how these rights are guaranteed and which limitations might apply. Usually, the Implementing Rules for Regulation 45/2001 should contain usable guidance for data subjects, but see section 2.2.2 above (§§12/13) for a possible need to adapt the wording.

49. **Article 16(2)(e) from which source the personal data originate**...": See Recital 29 of the Proposal, which stipulates that "*Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided*." In doing so, keep in mind the twofold objective (see above §33): informing the data subject is a precondition for verifying the lawfulness of the processing as well as for the further exercise of other data subject rights.

2.17 Article 16(3): "...within a reasonable period..."

The controller shall provide the information referred to in paragraphs 1 and 2; (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

50. Recital 29 of the Proposal stipulates that "*The information in relation to the processing of personal data relating to the data subject should be given to him or her... where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case*...". As this case-by-case requirement indicates, there are no hard and fast rules as to what represents "*a reasonable period*" in the sense of Article 16(3)(a) and, currently, there are no precedent cases.

2.18 Article 16(4): further processing

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

51. "...**information on that other purpose and with any relevant further information**": See Article 15(3).

2.19 Article 16(5): Exceptions to paragraphs 1 to 4

Paragraphs 1 to 4 shall not apply where and insofar as:

[40] See Opinion in case 2011-0806: "*La simple citation de ces droits ne suffit pas, car il est nécessaire d'expliquer adéquatement les moyens de les garantir ainsi que les limitations de ces droits qui sont applicables dans le cadre des traitements en question*".

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing;

(c) obtaining or disclosure is expressly laid down by Union law; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law.

52. "...**(b) the provision of such information ...would involve a disproportionate effort**": Article 12(2) of Regulation 45/2001 already contained a similar provision. This exception aims at cases in which the personal data of the data subject do not provide a way to contact him/her, e.g. because no address or other means of contact are known[41]. In such situations, the controller is usually not obliged to conduct further research to reach the data subject. Where the e-mail addresses of a data subject is known, sending an email with the data protection notice or a link to it does not appear to require a disproportionate effort[42].

53. In a consultation from the European Ombudsman on their policy regarding the information of third party data subjects[43], the EDPS had the opportunity to provide further guidance on this exemption. The consultation regarded the provision of individual information to third parties mentioned in (i) complaints outside the European Ombudsman's mandate and (ii) inadmissible complaints and inquiries that do not give rise to a transfer of personal data of third parties to an EU institution. The EDPS considered that for those (limited!) situations, adequate safeguards were provided by the publication of an information note on the European Ombudsman's website with a link to the European Ombudsman's policy on the info of third party data subjects[44].

54. "... (c) obtaining or disclosure is **expressly laid down by Union law**": This exception applies only to cases in which there is a clear *obligation in Union law to record or disclose information* not collected from the data subject. The EDPS has found[45] that the fact that Union law provides that a whistleblowing scheme has to exist for a particular EU institution is not enough to trigger this exception. This is because under such circumstances, it is only the *existence of a procedure* that is mandatory, not the recording or disclosure of data relating to specific data subjects[46].

[41] See e.g. EDPS case 2010-0426 (see https://edps.europa.eu/sites/edp/files/publication/12-02-22_cfsp_en.pdf).
[42] See EDPS case 2016-0271 (see https://edps.europa.eu/sites/edp/files/publication/16-07-19_letter_easa_eamr_en.pdf).
[43] Case 2016-0629. 16-12-01-draft letter to EO DPO-2016-0692 to WW
[44] https://www.ombudsman.europa.eu/en/resources/dataprotection/document.faces/en/70851/html.bookmark
[45] See EDPS case 2014-0871 (see https://edps.europa.eu/sites/edp/files/publication/14-12-08_breach_reporting_mechanism_ecb_en.pdf).
[46] See section 2 (§§6--9) of the EDPS Whistleblowing Guidelines on confidentiality in that context: https://edps.europa.eu/sites/edp/files/publication/16-07-18_whistleblowing_guidelines_en.pdf.

Annex 1: Summary of main changes

Regarding transparency rights and obligations, the Proposal provides for the following main changes compared to Regulation 45/2001:

	Article Proposal	**Ex-article** (if any)	**Change / novelty**
Transparent information			
1.	14(1)		Use of plain language for Privacy statements + replies to data subjects' requests
2.	14(2)		Controller shall *facilitate* data subjects' rights exercise
3.	14(3)		Controller bound to reply to data subjects requests, in principle within max 1 months
4.	14(4)		Controller needs to motivate non-action + inform data subject about complaint possibility to EDPS
5.	14(5)		Controller's reply free of charge. Manifestly unfounded or excessive requests may not be answered.
6.	14(7)+(8)		Controller shall provide information through standardised icons if COM adopts delegated acts determining such
Information to data subjects [where data are collected from data subject]			
7.	15 (1) under (b)		Contact details of DPO should be contained in the Privacy statement where data are collected from the data subject.
8.	15 (1) (e) See also 47-51	11	Controller shall inform through Privacy statement - the fact that data are intended to be transferred to 3rd countries or international Organisations - existence/absence of a Commission's adequacy decision - reference to safeguards (if transfer under article 49)
9.	15 (1) and (2)		More detailed information to be provided to data subjects, e.g. on rights + withdrawal of consent + existence of automated decision making
Information to data subjects [where data have not been obtained from data subject]			
10.	16(1) under (b)		Contact details of DPO should be contained in the Privacy statement where the data have not been obtained from data subject.
11.	16 (1) (e) See also 47-51	12	Controller shall inform data subjects about - the fact that data are intended to be transferred to 3rd countries or international Organisations - existence/absence of a Commission's adequacy decision - reference to safeguards (if transfer under article 49)
12.	16 (1) and (2)		More detailed information to be provided to data subjects, e.g. on rights + withdrawal of consent + existence of automated decision making
13.	16(3)		Obligation for Controller to inform data subjects within reasonable period but at the latest 1 month after having obtained the data

14.	16(4)+ (5)		If change of purpose intended, obligation to inform data subjects inter alia about other purpose and details

Annex 2: Suggestions by other DPAs

- The CNIL (France) advocates a "mapping exercise" ("*Cartographier vos traitements de données personnelles*"), see ;

- The UK's ICO has published comprehensive guidance, see https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/;

- The Spanish DPA has published extended guidance on information obligations, see https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf;

- Other DPAs have published a variety of brochures:

    - 'The GDPR and you - Preparing for 2018' by the Irish Data Protection Commissioner: https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf
    - 13-step plan by the Belgian Privacy Commission: https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf (in NL) and https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf (in FR):
    - Garante (Italy): http://www.garanteprivacy.it/regolamentoue (in IT).