EN

Article 13.

Information to be provided where personal data are collected from the data subject

Article 13.

1. 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:

Recitals

(60) 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.

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018):

> This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address etc.).

(b) the contact details of the data protection officer, where applicable;

Guidelines & Case Law

Article 29 Working Party, Guidelines on Data Protection Officers (DPOs) (2017):

> The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the

DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.

[…]

As a matter of good practice, the WP29 also recommends that an organisation informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.

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

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018):

In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the balancing test, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. To avoid information fatigue, this can be included within a layered privacy statement/ notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.

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

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The term "recipient" is defined in Article 4.9 as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, **whether a third party or not**" [emphasis added]. As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.

(f) 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 46 or 47, or the second subparagraph of Article 49(1), 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.

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article

45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.

2. 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:

Recitals

(61) 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.

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

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020):

> Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period,etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards,as a general rule,all personal data should be erased or anonymised.

(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 to object to processing as well as the right to data portability;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right. […] In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.64 In relation to the right to portability, see WP29 Guidelines on the right to data portability.

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.

(d) the right to lodge a complaint with a supervisory authority;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.

(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;

Guidelines & Case Law

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016):

> For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are “required”, which are not, and what will be the consequences of not filling in the required fields.

(f) the existence of automated decision-making, including profiling, referred to in Article 22(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.

Guidelines & Case Law

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2018):

> Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.
> In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22

provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject.

Recital 60 states that giving information about profiling is part of the controller's transparency obligations under Article 5(1)(a). The data subject has a right to be informed by the controller about and, in certain circumstances, a right to object to 'profiling', regardless of whether solely automated individual decision-making based on profiling takes place.

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

3. 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.

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

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 13. Information to be provided where personal data are collected from the data subject

Recitals

(61) 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.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or

processing activities to which the request relates.

Guidelines & Case Law

Document

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2018)

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (2020).

EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices* (2020).

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).

EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

Case Law

CJEU, *College van burgemeester en wethouders van Rotterdam/Rijkeboer*, C-553/07 (2009).

CJEU, *YS/Minister voor Immigratie, Integratie en Asiel*, C-141/12 and C-372/12 (2014).

CJEU, *ClientEarth/European Food Safety Authority*, C-615/13 P (2015).

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

ECHR, *López Ribalda v. Spain, nos 1874/13 and 8567/13* (2019).

Belgian DPA Fines Belgian Telecommunications Provider for Several Data Protection Infringements (2020). Brief description in English.