

WP29 publishes guidance on transparency

On 12 December, 2017, the Article 29 Working Party (WP29) published its [Guidelines on Transparency](#).

The guidance should assist controllers in understanding the obligation of transparency concerning the processing of personal data under the GDPR. The schedule to the guidance contains a list of the mandatory transparency information that must be provided to a data subject, so this note focuses on the WP29's recommendations in regard to the provision of that information to data subjects.

The meaning of transparency

Transparency is not defined in the GDPR, however recital 39 is informative as to the meaning and effect of the principle of transparency: *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used."*

Elements of transparency

Article 12 of the GDPR requires that the information or communication in question must be provided:

- in a concise, transparent, intelligible and easily accessible form;
- using clear and plain language;
- in writing, or by other means, including, where appropriate, by electronic means;
- where requested by the data subject it may be provided orally; and
- it must be provided free of charge.

"Concise, transparent, intelligible and easily accessible" information

The WP29 notes that this means the information must be presented efficiently and succinctly in order to avoid *"information fatigue"*. It should be *"clearly differentiated from other non-privacy related information such as contractual provisions"*. In an online context, the use of a layered privacy statement/notice will enable a data subject to navigate to the particular section of the privacy statement/notice which they want to immediately access rather than having to scroll through large amounts of text for particular issues. The requirement that information is *"intelligible"* means that it should be understood by an average member of the intended audience. The WP29's position is that controllers should not only provide the prescribed information under Articles 13 and 14, but also, separately, spell out in unambiguous language what the most important consequences of the processing will be.

The *"easily accessible"* requirement means that the data subject should not have to seek out the information; it should be immediately apparent to them where this information can be accessed. The WP29 gives an example of a website and an app. In regard to a website, the WP29 states that a link to the privacy statement/notice should be

clearly visible on each page of the website, and that positioning or colour schemes that make a text or link less noticeable or hard to find on a webpage are not considered “*easily accessible*”. For apps, the privacy statement/notice should be available from the online store to download, and once the app is installed, the information should never be more than “*two taps away*”. The WP29 highlights that this means that the menu functionality often used in apps should always include a “*Privacy*”/“*Data Protection*” option.

“Clear and plain language”

This means the information should be concrete and definitive. The WP29 highlights the high threshold required by the GDPR, by giving examples of phrases which are not sufficiently clear as to the purposes of processing. Examples of unclear language include: “*We may use your personal data to develop new services*” (as it is unclear what the services are or how the data will develop them); and “*we may use your personal data for research purposes*” (as it unclear what kind of research this refers to). It is recommended that language qualifiers such as “*may*”, “*might*”, “*some*”, “*often*” and “*possible*” should be avoided.

“In writing or by other means”

The default position for the provision of information to data subjects is that the information is in writing. Such information can also be provided in combination with standardised icons. The WP29 notes that “*other means*” includes electronic means, such as through layered privacy statements/ notices, or “*just-in-time*” pop-ups, 3D touch or hover-over notices, and privacy dashboards. Additional electronic means which may be provided “*in addition*” to a layered privacy statement/notice might include videos and smartphone or IoT voice alerts.

“The information may be provided orally”

The WP29 notes that this does not necessarily mean oral information provided in person or by telephone. Automated oral information may be provided in addition to written means, such as in the context of persons who are visually impaired when interacting with information society service providers. Where information is provided orally, the WP29’s position is that the controller should allow the data subject to re-listen to pre-recorded messages.

“Free of charge”

A controller cannot charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15-22 (on the rights of data subjects)

or Article 34 (communication of personal data breaches to data subjects).

Format of information

The WP29 provides guidance in relation to how the information set out in Articles 13 or 14 should be communicated to data subjects.

Layered privacy statements / notices

To avoid information fatigue in an online context, the WP29 recommends that layered privacy statements/notices should be used to link to the various categories of information which must be provided to individuals, rather than displaying all such information in a single notice on the screen.

The WP29 suggests that “*the design and layout of the first layer of the privacy statement/notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/how they can find that detailed information within the layers of the statement/notice...*” With regard to the substantive information which may be included in the first layer of the privacy statement/notice, the WP29’s position is that this should always contain information on the processing which has the most impact on the data subject and processing which could surprise the data subject. Accordingly, the data subject should be able to understand from information contained in the first layer what the consequences of the processing in question will be for the data subject.

Privacy Dashboards & Just-in-time notices

Other online methods advocated by the WP29 include privacy dashboards, which are particularly useful when the same service is used by data subjects on a variety of different devices, and just-in-time notices to provide specific privacy information as and when it is most relevant for the data subject to read.

Other methods of communicating transparency information

The WP29 provides examples of ways to convey transparency information to data subjects in the following different personal data environments:

- a. **Hard copy / paper environment:** for example, contracts by postal means, a privacy statement/notice can be provided by written explanation, leaflets, information in contractual documentation, cartoons, infographics, flowcharts;
- b. **Telephonic environment:** oral explanations by an individual to allow interaction and questions

to be answered, automated or pre-recorded information with options to hear further more detailed information;

- c. **Screenless smart technology/ IoT environment such as wifi tracking analytics:** icons, voice alerts, written details incorporated into paper set-up instructions, written information on the smart device, messages sent by SMS or email, public signage, etc.
- d. **Real life environment with CCTV/ drone recording:** visible boards containing the information, public signage, newspaper/media notices

Visualisation tools / Icons

The GDPR makes provision for information to be provided to a data subject “*in combination*” with standardised icons, to allow for a multi-layered approach (Recital 60 and Article 12.7). The purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the WP29 highlights that the utility of using icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent on the standardisation of symbols/images to be universally used and recognised across the EU as shorthand for that information. The GDPR assigns responsibility for the development of a code of icons to the European Commission (Article 12.8 & Recital 166).

Exceptions to the obligation to provide information

Article 13 exception

The only exception to a controller’s Article 13 information obligations, where it has collected personal data directly from a data subject, occurs “*where and insofar as, the data subject already has the information*” (Article 13(4)). The WP29 notes that this exception should be construed narrowly, and the principle of accountability requires controllers to demonstrate and document precisely what information the data subject has, how and when they received it and that no changes have occurred to that information that would render it out of date.

Article 14 exceptions

Article 14(5) contains three further exceptions to the information obligation on a controller where personal data has not been obtained from the data subject. Once again, the WP29 states that these exceptions should be interpreted narrowly:

1. Article 14(5)(b) “*the provision of such information proves impossible or would involve disproportionate effort...or seriously impair*

the achievement of the objectives of that processing”. The WP29 provides the example of a Bank A receiving information from Bank B about suspicious activities in regard to an account, which Bank A subsequently passes onto the relevant financial enforcement authority. As anti-money laundering legislation makes it a criminal offence for a reporting bank to tip off the account-holder that they may be subject to regulatory investigations, Article 14(5)(b) applies, and exempts Bank A from providing the account-holder with information on the processing of the data it received from Bank B, as the communication of such information would seriously impair the objectives of the legislation.

2. Article 14(5)(c) allows the lifting of the information requirements insofar as obtaining or disclosure of personal data “*is expressly laid down by Union or Member State law to which the controller is subject*”. The WP29 warns that this exemption will not apply where the controller is under an obligation to obtain the data directly from a data subject, in which case Article 13 will apply, and the only exemption under the GDPR applicable for providing the data subject with information on processing will be that under Article 13(4) (i.e. where and insofar as the data subject already has the information).
3. Finally, Article 14(5)(d) exempts a controller from the information requirement where the personal data “*must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law, including a statutory obligation of secrecy*”. The WP29 provides the example of a patient who provides a medical practitioner with certain personal data of her relatives who have the same medical condition. In such an instance, the medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14(5)(d) applies. If the medical practitioner were to provide such information to the relatives, the obligation of professional secrecy, which he owes to his/her patient would be violated.

Conclusion

Transparency is an overarching obligation under the GDPR, and is intrinsically linked to the fairness and the new principle of accountability. The guidance emphasises that the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information which must be provided to data subjects. It is vital that, prior to 25 May 2018, controllers ensure they are compliant with the new transparency obligations. This will entail controllers revisiting all the information they have provided to data subjects on the processing of their personal data, such as in privacy statements and notices, and ensuring that they adhere to the requirements in relation to transparency.

CONTACT US



John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com



John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com



Claire Morrissey
Partner, Dublin
+353 1 649 2246
cmorrissey@algoodbody.com



Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com



Davinia Brennan
Associate & Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com