WILMERHALE

The Article 29 Working Party Releases Draft Guidelines on Consent and Transparency Under The GDPR

DECEMBER 15, 2017

On December 12, 2017, the European Union's Article 29 Working Party ("Working Party") released two new guidelines on consent (WP 259) and transparency (WP 260) that it had adopted late in November 2017. These guidelines are open for comments through January 23, 2018. The Working Party will add a FAQ section in the final version of the consent guidelines.

Since the transparency guidelines are more of a tool that companies will use when preparing their data protection mechanisms and compliance documents, this article focuses on the consent guidelines, which reflect the Working Party's interpretation of the key consent requirements under the GDPR.

Why Does Transparency Matter?

Under the GDPR, transparency applies to how companies inform individuals about their processing activities, how they communicate with them about their rights, and how they facilitate the exercise of these rights. Transparency is really about a company communicating its approach to personal data.

Companies must be able to demonstrate that they act in a transparent manner in all circumstances. Companies that process personal data in a transparent manner should be in a better position to demonstrate compliance with their obligations under the GDPR than those that do not.

Why Does Consent Matter?

Consent is one of the legal bases for processing personal data under the GDPR. It is therefore crucial for companies to make sure any consent they obtain from individuals is actually valid where this is the legal basis they rely on for processing personal data.

In addition, the fact that a processing activity is based on consent affects individuals' rights, as follows:

- **The right to erasure ("right to be forgotten")** only applies in certain conditions, one of which is when an individual withdraws the consent on which the processing is based, and when there is no other lawful basis for the processing (Article 17(1)(b) GDPR).
- **The right to portability** only applies where the processing is based on consent (Article 20

GDPR).

- **The right to object**, however, does *not* apply where the processing is based on consent (Article 21(1) GDPR) – except where the processing is for direct marketing purposes, in which case the data subject may object at any time (Art. 21(2) GDPR). In any event, consent may always be withdrawn.

How Do the New Guidelines Help Companies?

- The transparency guidelines are designed to help companies understand how to structure and draft their privacy notices and comparable documents. To that end, as required by the GDPR and further explained in the transparency guidelines, information must always be concise, easily understandable for an average person, and easily accessible. The information must also be provided free of charge.
- The consent guidelines clarify the notion of consent and specify the requirements for obtaining and demonstrating it under the GDPR. These guidelines attempt to help companies understand and anticipate the authorities' expectations. They, at least, clearly show that the Working Party has adopted a very strict approach to consent.

What About Earlier Consent Guidelines and Consent Obtained Under the Data Protection Directive?

- Earlier Consent Guidelines Remain Relevant. The new consent guidelines focus on the changes under the GDPR compared to the Data Protection Directive. However, most of the key elements of consent remain the same under the GDPR. For this reason, the Working Party noted that its earlier consent guidelines remain relevant where they are consistent with the GDPR (in particular, the Working Party's opinion on the definition of consent, WP187). In this light, the new guidelines expand and complete the earlier Working Party's opinions, but they do not replace them.
- Consent Obtained Under the Data Protection Directive Is Valid (Only) if It Is in Line with the GDPR Requirements. Companies do not necessarily need to completely refresh all the consents they obtained under the Data Protection Directive. Rather, companies are expected to review them and make sure they meet the GDPR standards by May 25, 2018 (as stated in Recital 171 GDPR). This may be challenging, as it is clear that the GDPR raises the bar as regards the implementing consent mechanisms, which would require most companies to alter their consent mechanisms.

Understanding the Notion of Consent Under the GDPR

Under the GDPR, consent must be freely given, specific, informed, and unambiguous (Article 4(11) GDPR). The Working Party interprets each of these aspects as follows.

- **Free Consent**. Individuals must have a real choice. For example, in the view of the Working Party, consent is not free where individuals feel compelled to consent, where they will endure negative consequences if they do not consent, or where consent is bundled up as a non-negotiable part of terms and conditions. The Working Party analyzes four issues as

regards free consent: imbalance; conditionality; granularity; and detriment. The Working Party is aware of the "click fatigue" that consent requests based on these principles could involve. Yet it merely notes that it would be up to the controllers to find a solution to this issue.

- **Imbalance between the entity processing the personal data and the individual**. The Working Party mainly provided examples involving public organizations to illustrate this issue, which is of little help for businesses. Still, the Working Party confirms its view that it is unlikely that employees would be able to freely give consent to their employers. According to the Working Party, this means that employees' consent would only be freely given in exceptional circumstances, where it will have no adverse consequences at all whether or not they give consent.
- **Conditionality of consent**. Consent is not free where a company ties the consent request to the provision of a contract or a service. Consent is also free if an individual can choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service that does not involve such consenting
- **Granularity**. Where a service involves multiple processing operations for more than one purpose, consent is only free if individuals can choose which purpose they accept (this is called "granularity"), rather than having to consent to a bundle of processing purposes.
- **Detriment**. Companies must demonstrate that individuals can refuse or withdraw consent without detriment, e.g. that withdrawing consent does not lead to any costs (Recital 42 GDPR).

- **Specific Consent**. Consent is specific where a company explains the purpose of the processing, implements the granularity principle in consent requests, and clearly separates information related to obtaining consent for data processing activities from information about other matters.
- **Informed Consent**. The Working Party considers that companies should at least provide the following information for consent to be informed: the controller's identity; the purpose of each of the processing operations; what type of data will be collected and used; the existence of the right to withdraw consent; information about the use of the data for decisions based solely on automated processing, including profiling; and the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards where applicable. The information may be presented in various ways (e.g., written statements or video messages), but it should always be easily understandable for the average person. This means that companies must identify their audience to adapt the wording of their consent requests.
- **Unambiguous Consent**. Consent is unambiguous where it is given through an active motion or declaration. In the Working Party's opinion, unambiguous means that it must be "obvious" that individuals have consented to the processing. For this reason, pre-ticked boxes do not constitute unambiguous consent. However, swiping on a screen, waiving in front of a smart camera, or turning a smartphone around clockwise provide a valid consent

where it is clear that such motions signify agreement to a specific request (e.g., "if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm").

When Do You Need "Explicit" Consent and What Is It?

In addition to the requirements just described, consent as a legal basis for processing sensitive data (Article 9 GDPR), justifying an automated individual decision-making process (Article 22 GDPR), or transferring personal data outside the European Union (Article 49 GDPR) must also be "explicit." The Working Party considers that this requires an express statement of consent, such as a written statement, filling in an electronic form, sending an email, uploading a scanned document carrying the individual's signature, or using an electronic signature.

Companies Should Be Able to Demonstrate that They Obtained Consent

A company's ability to demonstrate consent includes its ability to show that this consent is valid, as explained above. For example, a company may keep records of consent statements received. Such records should show when consent was obtained and what information was provided to the consenting individuals. Where consent is given online, a company can retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It is not sufficient to merely refer to a correct configuration of the website.

Withdrawal of Consent

Individuals can withdraw their consent at any given time, and it should be as easy to withdraw it as to give it. For example, if consent is obtained through a one mouse-click or swipe, individuals must be able to withdraw that consent equally as easily. Likewise, where consent is obtained through use of a service-specific user interface (e.g., a website, an app, the interface of an IoT device or by e-mail), individuals must be able to withdraw consent via the same interface.

Two Specific Areas of Concern: Children and Scientific Research

- **Children**. Companies can obtain valid consent from a child where they offer online services directly to this child and where he or she is at least 16 years old, unless Member State law provides a lower age. Companies must make reasonable efforts to verify the child's age, and these measures should be proportionate to the nature and risks of the processing activities. Companies should also use appropriate language to ensure the child understands how the company intends to process his or her personal data. Where the child is less than 16 years old (again, unless Member State law provides a lower age), consent must be given or authorized by the holder of parental responsibility. The Working Party considers that in in low-risk cases, verification of parental responsibility via email may be sufficient. The Working Party states that in high-risk cases, it may be appropriate to ask for more proof but, again, it leaves it up to companies to determine what measures are appropriate.
- **Scientific research**. The Working Party defines scientific research as a research project

set up in accordance with relevant sector-related methodological and ethical standards. Scientific research projects can only include personal data based on consent if they have a well-described purpose. Where the purposes of the processing cannot be specified at the outset, Recital 33 GDPR allows that the purpose may be described at a more general level. However, the Working Party considers that this exception should be subject to a strict interpretation and should require a high degree of scrutiny where the processing involves sensitive data. Such an interpretation significantly restricts the scope of this exception.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Frédéric Louis

PARTNER

frederic.louis@wilmerhale.com

+32 2 285 49 53

Itsiq Benizri

COUNSEL

itsiq.benizri@wilmerhale.com

+32 2 285 49 87