A&L Goodbody

WP29 publishes guidance on consent

On 12 December, 2017, the Article 29 Working Party (**WP29**) published its Guidelines on Consent under the GDPR.

Consent is one of the lawful grounds on which personal data processing may be based. The consent guidance considers the extent to which the GDPR requires controllers to change their consent requests/ forms.

Elements of valid consent

Article 4(11) of the GDPR defines consent as: *"(i) any freely given, (ii) specific, (iii) informed and (iv) unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".* The WP29 considers and provides guidance on the meaning of each of these elements.

(i) Freely given

The WP29 notes that *"free"* implies real choice and control for data subjects. If consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given. The WP29 warns that consent and contract, as two lawful bases for processing personal data, should not be merged and blurred. If a controller seeks to process personal data that are necessary for the performance of a contract, such as processing credit card details in order to facilitate payment, the correct lawful basis is likely contractual necessity, and there is no need to use another lawful basis such as consent.

The imbalance of power between the controller and the data subject is also taken into consideration by the GDPR. The WP29 points out that recital 43 of the GDPR clearly indicates that it is unlikely that public authorities can rely on consent for processing, as in most cases the data subject will have no realistic alternatives to accepting the processing terms of a public authority. The WP29 considers that there are other lawful bases, notably compliance with a legal obligation or performance of a task carried out in the public interest, which are more appropriate to the activity of public authorities. Once again, the WP29 notes that an imbalance of power also occurs in the employment context, and that consent given by employees to the processing of their data at work is unlikely to be deemed as freely given.

The WP29 emphasises the important of granularity, noting that consent is presumed not to be freely given if the process for obtaining consent does not allow data subjects to give separate consent for separate processing activities. Where processing has multiple purposes, consent should be obtained for each of them.

(ii) Specific

The WP29 notes that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them. If a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose.

(iii) Informed

If a controller does not provide accessible information then consent will be an invalid basis for processing. The WP29 warns that the GDPR introduces a high standard for clarity and accessibility of the information, and a controller should consider its targeted audience to determine what information to provide and how to provide it. In practice compliance with the information requirements laid down in Articles 13 and 14 of the GDPR and compliance with the requirement of informed consent may often lead to an integrated approach.

(iv) Unambiguous consent

The WP29 clarifies what constitutes *"unambiguous"* consent to the processing of non-sensitive personal data, noting that the data subject must have taken a deliberate action to consent to the particular processing, such as through a written or recorded oral statement, including by electronic means. The WP29 highlights that blanket acceptance of Ts & Cs, which include a consent provision, cannot be seen as a clear affirmative action to consent to the use of personal data. The WP29 notes that the GDPR does not permit controllers to offer pre-ticked boxes that require an intervention from the data subject to prevent agreement.

The WP29 states that physical motions can constitute affirmative action in compliance with the GDPR. Example 12 highlights that swiping on a screen may indicate consent, as long as clear information is provided, and its clear the motion signifies consent to a specific request. For example *"If you swipe this bar to the left, you agree to the use of information x for purpose y. Repeat the motion to confirm"*. On the other hand, Example 13 shows that scrolling down or swiping through Terms and Conditions, which include declarations of consent (i.e. a statement comes up on the screen to alert the data subject that continuing to scroll constitutes consent), will not suffice, as the alert may be missed by a data subject scrolling quickly through large amounts of text, and such action would not be sufficiently unambiguous.

The WP29 warns that multiple consent requests, that require data subjects to answer through clicks and swipes every day, may result in *"click fatigue"*, which may subsequently lead to the effect of consent mechanisms diminishing as consent questions are no longer read. The GDPR puts the burden on controllers to develop ways to tackle this issue, noting that an oft-mentioned solution is to obtain consent through browser settings.

GDPR standard of consent required for electronic marketing

The concept of consent in the draft e-Privacy Regulation is aligned with that in the GDPR. However, the WP29 highlights that even if the proposed e-Privacy Regulation has not been adopted by 25 May 2018, the GDPR conditions for obtaining valid consent will be applicable in situations falling within the scope of the current e-Privacy Directive 2002/58/EC (including consent to direct marketing communications and online tracking).

The WP29 notes that references to the repealed Data Protection Directive 95/46/EC must be construed as references to the GDPR (pursuant to Article 94 of the GDPR), and as the e-Privacy Directive adopts the definitions set out in the Data Protection Directive 95/46/EC, this means that it now adopts the definitions set out in the GDPR (including the definition of consent).

The WP29 clarifies that even though Article 95 of the GDPR states that it introduces no "*additional obligations*" to those already imposed under the e-Privacy Directive 2002/58/EC, the valid consent conditions in Article 7 of the GDPR should not be viewed as "*additional obligations*". Therefore, in regard to direct marketing, from 25 May 2018, opt-out consent (except in regard to existing customers who are permitted to object to direct marketing) will no longer be sufficient, as silence and pre-ticked boxes do not constitute consent under the GDPR.

Meaning of "explicit" consent

In regard to what constitutes *"explicit"* consent to the processing of sensitive personal data, the WP29 states that the data subject must give an express statement of his/her consent, such as by a written or signed statement. In an online context, a data subject may give an express statement of consent by filling in an electronic form; sending an email; uploading a scanned document carrying the signature of the data subject; using an electronic signature; or by two-stage verification (e.g. by the data subject confirming "*I agree*" by email, and then receiving a verification link to click on, or an SMS message with a verification code, to confirm agreement). The WP29 notes that whilst, in theory, the use of recorded oral statements may be sufficient to obtain explicit consent, it may prove difficult for the controller to show that all conditions for valid explicit consent were met when the statement was given.

A&L Goodbody

Burden on controller to demonstrate valid consent

The WP29 notes that it is up to the controller to prove that valid consent was obtained from the data subject. The controller should keep a record of consent statements received, so it can show how consent was obtained, when it was obtained, and the information provided to the data subject. In an online context, the WP29 suggests that a controller could 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.

Duration of consent

There is no specific time limit in the GDPR for how long consent will last, but the WP29 recommends as a best practice that consent should be refreshed at appropriate intervals, and that providing all the information again helps to ensure data subjects remain well informed about how their data is being used and how to exercise their rights.

Withdrawal of consent

Companies need personal data for several purposes, and processing is often based on more than one lawful basis, e.g. contract and consent. In such circumstances, the WP29 notes that a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. This highlights the importance of controllers being clear from the outset which purpose applies to each type of data and which lawful basis is being relied on.

The WP29 warns that where a data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent to this other lawful basis. As a general rule, the WP29 states that a processing activity for one specific purpose cannot be based on multiple lawful bases, however it is possible to rely on more than one lawful basis to legitimise processing if the data is used for several purposes, as each purpose must be connected to a lawful basis. However, the controller must have notified these purposes and lawful bases in advance. The controller cannot swap between lawful bases during the course of processing. These observations by the WP29 highlights once again the risks of relying on consent to legitimise processing. The controller cannot rely on a data subject's consent, and then simply rely on other lawful bases as a back-up if consent is subsequently withdrawn, or if the controller cannot demonstrate that valid GDPR compliant consent has been given by a data subject.

Digital consent of child – how to verify parental authorisation?

In regard to the offer of information society services (i.e. online contracts and services) directly to a child, the GDPR requires controllers to obtain parental authorisation and make *"reasonable efforts"* to verify that the person providing that consent is a holder of parental responsibility. The WP29 warns that age verification should not lead to excessive data processing. The guidance notes that what constitutes *"reasonable efforts"* may depend on the risks inherent in the processing as well as available technology. In low risk cases, verification of parental responsibility via email may suffice, whilst in high risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify that parental authorisation was given. The WP29 gives an example of a parent or guardian being asked to make a payment of €0.01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Trusted third party verification services may also offer solutions which minimise the amount of personal data the controller has to process itself.

Refreshing consent prior to May 2018

The WP29 notes that controllers are not required to refresh existing consents, unless such consent does not meet the higher standard required by the GDPR. Rather than renewing consent, controllers may consider switching to a different lawful processing basis. The WP29 warns, however, that *"this is a one-off situation as controllers are moving from applying the Directive to applying the GDPR. Under the GDPR it is not possible to swap one lawful basis and another"*. The WP29 points out that in any event *"the controller needs to observe the principle of lawful, fair and transparent processing"*. Prior to 25 May 2018, controllers will need to revisit all information provided to data subjects in their privacy statements/notices, to ensure that they clearly set out the lawful processing bases for each of their processing activities, and that they meet the GDPR's requirements in relation fair and transparent processing (pursuant to Article 13 or 14 of the GDPR).

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
+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