

22 December 2017

Article WP29 Issues Draft Guidelines on Consent under GDPR

On 12 December 2017, the Article 29 Working Party (**WP29**) published draft guidelines (the **Guidelines**) on consent under General Data Protection Regulation 2016/679 (the **GDPR**). It invites stakeholders to submit comments by 23 January 2018.

Consent is one of six “lawful bases” that allow the processing of personal data listed in Article 6 of the GDPR (or Articles 9 and 10 of the GDPR for “sensitive” categories of data). Other lawful bases under Article 6, *inter alia*, permit the processing of personal data if it is (i) necessary for the performance of a contract; (ii) to comply with a legal obligation; or (iii) to pursue a legitimate interest of the controller. Controllers should carefully consider whether consent is the appropriate lawful basis for the envisaged processing or whether another lawful basis should be chosen instead.

Once the GDPR applies, controllers are not allowed to swap between the lawful bases of Article 6 GDPR. Moreover, the WP29 reminds organisations that obtaining consent does not diminish the controller’s obligations with regard to fairness, necessity, proportionality and data quality. In other words, even if an organisation obtains consent, it is still not permitted to collect personal data which are “*not necessary in relation to a specified purpose of processing and fundamentally unfair*”.

1. ELEMENTS OF VALID CONSENT

According to the WP29, the concept of consent, and the requirements for obtaining a valid consent have “evolved” under the GDPR. Consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. This also follows from Article 4(11) of the GDPR which defines consent as: “*any freely given, specific, informed and 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*”. In its guidelines, the WP29 provides an analysis of the following elements of valid consent:

(i) *Free / freely given:*

This element implies real choice and control for data subjects. According to the WP29, if consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given, and is therefore invalid as a legal basis for the processing of personal data under Article 6 of the GDPR.

Further, the WP29 provides examples of situations where there exists an imbalance of power (e.g. in relation to public authorities or in the employment context) and is of the opinion that in those situations it is unlikely that consent is free. As a result, such consent would be invalid. Nevertheless, the WP29 indicates that even in such situations, it may be possible, depending on the situation at hand, for the controller to demonstrate that the data subject is free to consent. For instance, an employer could rely on the consent of the employee if giving or refusing consent for a specific purpose would have no adverse consequences for the employee.

Moreover, if a service involves multiple processing operations for more than one purpose, the WP29 urges controllers to seek separate consent for each purpose (“granularity”).

(ii) Specific

According to the WP29, in order to comply with the requirement of ‘specific’ consent the controller must, when requesting consent: (i) be specific in defining the purpose as a safeguard against “function creep”, i.e. the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of data; (ii) apply granularity in consent requests (e.g. a separate opt-in for each purpose to allow users to give specific consent for each specific purpose); and (iii) separate information related to obtaining consent for the use of personal data from information about other matters.

(iii) Informed

In order for consent to be ‘informed’, it must take account of the requirement for transparency in Article 5 GDPR (see, our note on the WP29’s draft guidelines on transparency, [here](#)). The WP29 provides a limitative list of information that must be provided to data subjects, *inter alia*, the identity of the controller, the purpose of the processing activity and the existence of the right to withdraw consent.

Furthermore, the WP29 requires controllers to use clear and plain language and provide the information in an intelligible and easily accessible form, and to clearly describe the purpose for data processing for which consent is requested.

(iv) Unambiguous indication of wishes

Under the GDPR, consent must always be given through an “active motion or declaration”. Accordingly, the WP29 declares that the use of pre-ticked opt-in boxes is invalid under the GDPR. Also, silence or inactivity, as well as merely proceeding to use a service without opposition, does not result in valid consent. The WP29 also maintains that blanket acceptance of general terms and conditions of a service cannot be seen as a clear affirmative action to consent to the use of personal data.

In an electronic context, the WP29 deems that physical motions, such as swiping, can qualify as a clear and affirmative action in compliance with the GDPR but warns at the same time about a certain degree of “click fatigue” because in a digital context data subjects might too often be faced with requests for consent. Accordingly, the WP29 argues that the actual warning effect of consent mechanisms is diminishing.

The WP29 furthermore emphasises, in accordance with its previous opinions, that consent should be given prior to the processing activity.

Further, the WP29 provides guidance on obtaining explicit consent in certain situations where serious data protection risks emerge. In such situations, the data subject must be able to exercise a high level of control over his personal data. According to the WP29, this means that the data subject must give an express statement of consent.

2. WITHDRAWING CONSENT

In accordance with Article 7(3) GDPR, controllers must ensure that consent can be withdrawn at any given time by the data subject as easily as it was for giving consent. The controller must also inform the data subject of their right to withdraw consent. As the withdrawal of consent is an essential element of the consent mechanism, the WP29 is of the opinion that consent would be invalid if the method for withdrawing consent would be overly burdensome. In an example, the WP29 explains that a requirement to contact a call-centre during business hours to withdraw consent, when the initial consent was granted by a one-click mechanism on the website, would fall short of this obligation and invalidate the consent mechanism.

Moreover, the WP29 explains that data subjects should be able to withdraw consent without detriment. This means that the controller must make withdrawal of consent possible free of charge or without lowering service levels.

3. ACCOUNTABILITY AND RETENTION OF PROOF OF CONSENT

Finally, the WP29 recalls the controller's obligation to demonstrate consent under the accountability principle of the GDPR. Therefore, it is advised to keep proof of when and how consent was given.

However, and since the GDPR does not provide a specific time limit for how long consent will last, the WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Furthermore, after the processing activity ends, proof of consent should be kept no longer than strictly necessary in accordance with Article 17(3b) and (3e) GDPR.

As with the draft guidance on transparency, published the same day, the WP29 invites comments to be submitted by 23 January 2018. The full text of the draft guidelines on consent can be consulted [here](#) (clicking the link will open the pdf document).

Authors

Thibaut D'hulst

tdhulst@vbb.com

Reshad Forbes

rforbes@vbb.com

Get in touch

If you have any questions concerning this memorandum, please call us at

+32 2 647 73 50

or send us an e-mail at

brussels@vbb.com