Cooley

GDPR: Guidance on Consent Requirements

March 9, 2018

In December 2017, the Article 29 Working Party released for comment a draft of its guidance on consent under the GDPR. Consent is one of the lawful bases for processing personal data and one of the permitted means by which personal data may be transferred to a third country outside of the European Union, even if that country has not been found by the European Commission to provide an "adequate" level of protection. The following is a quick summary of the Working Party's interpretations of the GDPR requirements for "consent" and for "explicit consent."

The GDPR requires explicit consent, which must meet the consent requirements plus the additional requirements set forth below, in the following three circumstances. (a) where the data subject is asked to consent to the processing of special categories of information; (b) where the data controller relies on consent as the basis for the transfer and processing of personal data to countries or organizations lacking an adequacy decision, under Article 49; and (c) in the case where personal data is used for automated individual decision making, including profiling, under Article 22.[1]

Consent

Consent must be freely given, specific, informed and unambiguous.

1. **Freely given:** Consent must involve "real choice and control for data subjects." It will not be considered to have been freely given if: (a) it is bundled in non-negotiable terms and conditions; (b) it cannot be refused or withdrawn; (c) it requires consent to the processing of personal data that is not necessary for the performance of the contract; or (d) where there is an imbalance in power between the data controller and the data subject. What is "necessary for the performance of a contract" will be interpreted strictly, such that there must be a direct and objective link between processing and performance for the performance to qualify as a lawful basis. By way of example, the Working Party provides that a mobile phone-editing application that requires users to activate GPS location services for behavioral purposes would not qualify as "freely given" because consent to processing of unnecessary personal data cannot be seen as a mandatory consideration in exchange for performance. The Working Party warns that the imbalance in power between data controller and data subject means that for the majority of data processing at work, consent cannot be relied on as the lawful basis for processing personal data of employees since it is unlikely employees will feel able to freely respond to a request by their employer to process their personal data, or to refuse such request, without detriment.
2. **Specific:** Specific consent is intended to "ensure a degree of user control and transparency for the data subject" and is closely related to the requirement that consent be informed. The Working party identifies three components of specificity that data controllers must apply: (a) there should be a specification of the purpose of the processing; (b) there should be granularity in consent requests; and (3) there should be a clear separation of information related to obtaining consent for processing from information about other matters.
3. **Informed:** The requirement for informed consent is derived in part from the principle of transparency in Article 5 of the GDPR. The Working Party states that the following categories of information are the minimum necessary for consent to be informed: (a) the identity of the data controller; (b) the purpose of each of the processing operations for which consent is sought; (c) what types of personal data will be collected and processed; (d) the existence of the right to withdraw consent; (e) information about the use of personal data for decisions based solely on automated processing, including profiling; and (f) if the consent relates to transfers, information about the possible risks of data transfers to third countries in the absence of an adequacy decision and/or appropriate safeguards. If there are joint controllers, all joint controllers must be named. The Working Party notes that valid informed consent can exist, even when not all of the above elements are mentioned in the process of obtaining consent, so long as the relevant disclosures are made elsewhere by the data controller.
4. **Unambiguous indication of wishes:** Consent must include a statement or affirmative act from the data subject. Written or recorded oral statements, including electronic statements, may satisfy this requirement,

but pre-ticked boxes, or silence, inactivity, consent implied by the user proceeding with the service, or general agreement to a blanket terms of service agreement, do not constitute an unambiguous indication of wishes. Withdrawal of consent must be as easy as what was required to provide consent. The Working Party provides several examples of a physical motion which can qualify as unambiguous indication of wishes (swiping on screen, waving in front of a smart camera and turning a phone in a specified direction) so long as clear information is provided and agreement to a specific request is indicated. The Working Party recognizes that an issue of fatigue could result from multiple requests for consent, but reminds controllers that they retain the responsibility for solving this problem. If a data controller relies on the data subject's consent to process personal data and the data subject does not check the box agreeing to the data controller's privacy policy or confirm his or her consent via a clear affirmative act, the data subject should not be permitted to proceed with registration, account creation and/or submission or uploading of any personal data.

In addition, the Guidelines recommend refreshing consent at "appropriate intervals" and, when doing so, providing all of the required information discussed above again to ensure that the consent is still informed.

Explicit consent

"Explicit consent" is distinguished from regular consent (which must be confirmed via an "unambiguous indication of consent," as discussed above) via the means by which it is obtained. "Explicit" requires “an express statement." A written statement (for example, typed instructions) is a "best practice" form of explicit consent. The Working Party Guidelines state that a written statement signed by the data subject is one method of obtaining explicit consent. Other methods including having the data subject fill in an electronic form; send an email; upload a scanned document with a signature; record an oral statement; or verify consent via a two-stage authentication process (for example, an email followed by an SMS message). For explicit consent obtained online, the Working Group suggest retaining information of the session in which consent was obtained, along with "documentation of the consent workflow at the time of the session" and a copy of the information (i.e., the page displayed) presented to the data subject.

As with other consents, the Guidelines recommend refreshing explicit consent at "appropriate intervals" and, when doing so, providing all of the required information discussed above again to ensure that the explicit consent is still informed.

Re-consenting

The Guidelines make clear that data controllers that currently rely on consent to process personal data are not required to ask data subjects to re-consent if the original consent meets all of the requirements set out above. However, if existing consents do not meet these requirements (e.g., because they rely on a more implied form of action by a data subject), they will need to be renewed. Alternatively, data controllers may be able to rely on a different lawful basis (e.g., legitimate interests).

Key takeaway

1. Each data controller subject to the GDPR that relies on consent as the basis for any of the following will need to review when and how it obtains consent from data subjects: the general collection and use of personal data, the use of cookies, and the sending of direct marketing communications, such as newsletters, promotional emails, etc.
2. Each data controller subject to the GDPR that relies on consent will need to ensure that it has implemented a process for obtaining explicit consent: (a) where the data subject is asked to consent to the processing of special categories of information; (b) where the data controller relies on consent as the basis for the transfer and processing of personal data to countries or organizations lacking an adequacy decision, under Article 49; and (c) in the case where personal data is used for automated individual decision making, including profiling, under Article 22.
3. Each data controller subject to the GDPR should refresh consent at appropriate intervals and, when doing so, provide all the information to the data subject again to ensure that the consent is still informed.
4. Each data controller subject to the GDPR must ensure that the process for a data subject to withdraw his or her consent is as easy as the process by which the data subject gave his or her consent.

Notes

1. "Special categories of personal data" is defined in Article 9 of the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Key Contacts

Ann Bevitt **London**	**abevitt@cooley.com** **+44 (0) 20 7556 4264**