ROPES & GRAY ALERT

Privacy & Data Security

May 9, 2017

The Information Commissioner's Guidance on Consent under the GDPR

Attorneys
Rohan Massey
Clare Sellars

The General Data Protection Regulation (the "GDPR") came into force in May 2016 and makes numerous changes to European data protection laws. Among other things, the GDPR updates the rules on the use of consent by data controllers to justify their processing of personal data in various circumstances. The UK Information Commissioner's (the "ICO") consultation on its draft GDPR Consent Guidance (the "Guidance") ended on 31 March 2017. The ICO reported on 13 April that over 300 responses have been received and these are now being analysed.

The draft Guidance is generally helpful and provides clear practical advice regarding many aspects of consent. However, there are some elements of the draft Guidance which are likely to prove contentious. It is clear that valid consent will become significantly harder to obtain and that it will often be more appropriate for data controllers to rely on an alternative legal basis other than consent to justify their personal data processing.

What Has Changed?

The Guidance confirms that the basic concept of consent and its main role as one potential lawful basis (or condition) for processing personal data has not changed; however, the GDPR builds on the existing definitions and standards of consent in various ways, setting a high standard for consent. Current methods of obtaining consent will need to be reviewed and refreshed. Clearer and more granular opt-in consent methods, good consent records and easy ways to withdraw consent will all be required.

The definition of consent set out in the GDPR includes additional requirements regarding how consent should be given. Consent is defined to mean "*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 the personal data relating to him or her*" (emphasis added). The new elements of the definition are considered in more detail below.

For those involved in scientific research or processing children's personal data online, there are new provisions on consent for scientific research purposes and children's consent for online services. Consent and explicit consent, respectively, can also legitimise restricted processing and automated decisionmaking and profiling and international transfers of personal data if adequate safeguards are not in place. Consent can also give individuals stronger rights in some cases (e.g., the rights to data portability and erasure).

The ICO makes it clear that, if consents have been obtained previously, data controllers will not be required to refresh such consents if they meet the GDPR's standards and have been properly documented, although they will need to implement mechanisms allowing individuals to withdraw their consent easily. In the light of the Guidance, it seems unlikely that many (if any) existing consent mechanisms will meet GDPR standards and, if they do not, fresh GPDR compliant consent will need to be sought. This may well involve significant work for data controllers who have historically relied on consent to justify their personal data processing.

When is Consent Appropriate?

A significant issue that the Guidance addresses is the fact that, under the GDPR, consent may well not always be required to provide a legal basis for processing personal data and may not always be the most appropriate basis or the easiest to achieve (there are six lawful bases for processing personal data, including consent). Essentially, data

controllers are likely to need to obtain consent when no other lawful basis is available, but it is less likely to be appropriate in other circumstances.

Consent will only be the most appropriate legal basis for processing when people are offered real and ongoing choice and control over how their personal data will be used. If a genuine choice cannot be offered, the ICO is clear that asking for consent could be considered misleading and unfair.

Valid Consent

The draft Guidance focuses on the various elements required to obtain valid consent. First, to ensure that consents are freely given, individuals must be able to refuse consent without penalty and withdraw consent easily at any time. Consents must be unbundled from other terms and conditions (with granular options provided for different types of processing) and not made a condition of receiving a service unless the relevant personal data processing is necessary for that service. For example, requiring individuals to agree to the use of their personal data for direct marketing purposes in order to receive a "free" online service, where the processing of personal data is not required for the individual to receive the service, is unlikely to be regarded as valid consent.

Employers and public authorities in particular should note that the Guidance also stresses that it will be difficult to obtain freely given consent in any relationship where there is an imbalance of power and they are likely to need to identify an alternative legal basis for personal data processing in many cases.

Of particular interest to data controllers involved in areas such as direct marketing is the fact that the ICO stresses that consents must specifically identify the data controller and any third party who will be relying on the consent and state the purposes of the processing. Consent for categories of third-party organisations will not be sufficiently specific. The requirement to specifically name each third party to whom personal data will be made available may well restrict certain data controllers' ability to send direct marketing communications to potential customers.

Granular options to consent separately to separate purposes must also be provided covering each type of processing activity, where possible (unless such activities are clearly interdependent). Details of how to withdraw consent at any time must also be provided. Wording must be prominent, concise, separate from other terms and conditions and in plain language. For data controllers who wish to process personal data in various different ways for various different purposes, there may be a risk that complying with these requirements will confuse data subjects instead of clarifying the use of their data for them.

Electronic consent requests must not be unnecessarily disruptive to users, and the ICO recommends the use of user-friendly layered information and "just-in-time" notices. Data controllers are likely to have to make changes to their existing electronic consent procedures in many cases to ensure that these requirements are adhered to.

The GDPR requires it to be obvious that individuals have consented and what they have agreed to and a clear signal that they give consent is required. Clear affirmative action requires individuals to take deliberate action to opt in. The draft Guidance suggests that various forms of action will comprise a valid opt-in, for example, ticking an opt-in box (on paper or electronically), clicking a link online, signing a consent statement, making an equally prominent binary choice, or switching technical settings away from the default, among others. Relying on acceptance of general terms and conditions, failure to opt out, default settings, silence, pre-ticked boxes or inactivity will not constitute valid consent.

Implied Consent

The draft Guidance adopts a pragmatic approach to implied consent, confirming that it can still constitute an affirmative act in some circumstances, especially more informal offline situations, although it must also be possible to verify consent. The ICO has confirmed, however, that implied consent cannot be explicit consent.

Duration of Consent

Data controllers should note that consent is not static and that the validity of consent is contextual. Consents should be reviewed regularly as they will probably degrade over time, although this depends on the context, the scope of the

original consent and the data subject's expectations. If processing operations change, consents may no longer be sufficiently specific or informed and data controllers will need to seek refreshed consents unless another lawful basis for processing exists, (as a default position, the ICO recommends considering refreshing consent every two years, but this may not always be appropriate).

The draft Guidance requires that withdrawal of consent should be an easily accessible one-step process and, if possible, data subjects should be able to withdraw their consent in the same way that they gave it (e.g., if consent is given using an online form, it should also be possible to withdraw consent using an online form). Data controllers should consider publicising both online preference management tools (such as privacy dashboards) so that individuals can access and update their consent settings easily and other easy ways of withdrawing consent (e.g., customer service phone numbers) and should also offer opt-out by reply to every contact (e.g. opt-out phone numbers, addresses or unsubscribe links in e-mails).

Children

For service providers targeting online services at children, the draft Guidance emphasises the new GDPR provisions which increase protection for children's personal data and are additional to those already considered above. Subject to certain exceptions, if "information society services" (essentially, services requested and delivered over the internet) are offered to children and data controllers want to rely on consent as a lawful basis for processing, then consent from the child's parent or guardian is required for any child under 16 (although Member States may impose a lower age not below 13). Data controllers will need to introduce age verification measures and must make reasonable efforts to verify parental responsibility for those under the relevant age.

Data controllers who process children's personal data other than in the context of information society services should decide whether the child has the capacity to understand and consent for themselves. Age verification measures and steps to verify parental consent for children who cannot consent may still be needed. It is worth considering whether legitimate interests rather than consent could form a legal basis for the processing of children's personal data in some circumstances.

Records

Data controllers will need to be able to show that individuals have consented to personal data processing, and effective audit trails of how and when consent was given should be established to provide evidence if challenged. The draft Guidance includes some useful examples of what consent records should include. Details should be kept of (i) who consented; (ii) when (e.g., the ICO suggests retaining copies of a dated document or online records that include timestamps); (iii) what they were told at the time; (iv) how they consented (e.g., if consent was given online, records should include the data submitted and a timestamp to link it to the relevant version of the data capture form); and (v) whether consent has been withdrawn and, if so, when. The Guidance suggests that records should also be specific and granular to show exactly what the consent relates to.

Comment

The Guidance sets out some helpful practical suggestions regarding how data controllers should obtain and manage consents in the context of personal data processing; however, some aspects of the Guidance may be controversial. For example, as noted above, there is a concern that the requirement to specifically identify every third party who will be relying on the consent rather than being able to list categories of third-party organisations will raise challenges for many data controllers. Similarly, there is a concern that the required level of granularity regarding opt-in mechanisms may, in practice, serve to confuse individuals rather than giving them enhanced choice and control over how they consent to the use of their personal data. Based on the draft Guidance, it seems likely that consent will be used by data controllers significantly less often to justify their personal data processing than has been the case prior to implementation of the GDPR. It will be interesting to see whether and, if so, in what ways, the Guidance is updated following the ICO's consultation (the ICO hopes to publish the final version of the Guidance in June 2017).