UK Consent Guidance Under the EU’s General Data Protection Regulation

Introduction

On March 2, 2017, the UK Information Commissioner’s Office (ICO) published draft guidance (the Guidance) on consent under the EU’s General Data Protection Regulation (GDPR) which comes into force in May 2018. The GDPR defines valid 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.”

The Guidance explains: (i) when is consent required or appropriate and the alternatives to consent; (ii) what constitutes valid consent under the GDPR with specific guidance on children’s consent and consent for research purposes; and (iii) advice on how to obtain, record and manage consent. The Guidance also contains a consent checklist. The ICO’s consultation on the Guidance is open until March 31, 2017.

Companies will face very considerable challenges implementing consent practices that will satisfy both the Guidance (if it remains in its current form) and the GDPR. The Guidance confirms that the way consents are managed and obtained will need to change fundamentally. As a result companies will need to carefully review existing consents and to determine whether to obtain a GDPR form of consent or to rely on alternative legal grounds for the processing, such as legitimate interest.

Freely Given Consent

The Guidance confirms that consent is only an appropriate legal basis to process their personal data when data subjects are offered a genuine choice over the use of their data. This may not be the case where the data would be processed on a different lawful basis if consent is refused or withdrawn, if the consent is a precondition to accessing services or where the entity seeking consent is in a position of power over the data subject, e.g., their employer. Pre-ticked opt-in boxes will also no longer be sufficient to demonstrate consent under the GDPR. Clear affirmative action is required, such as ticking a box or switching default technical settings. In addition to the need to seek new consents where pre-ticked boxes have been used, the GDPR poses a further challenge because in many circumstances it will not be possible to make ticking a consent box a condition for accessing a service (e.g., by refusing to allow customers to progress to the next page of an online account creation unless...
they tick the consent box). Consent will also not be freely given if the provision of a service is dependent on such consent, unless it is also necessary for the performance of the service.

**Granularity**

The Guidance indicates that in order for consent to be specific and informed, it must be granular. In practice this means both (i) identifying each of the third parties who will rely on the consent; and (ii) obtaining separate consents for each processing activity and purpose. It is likely that few existing consents would meet these granularity standards and they will also be difficult to satisfy for future consents. For example, listing third parties reliant upon the consent may be difficult where the list of such third parties changes regularly. A further problem is that granular consents requiring separate consents will be difficult to implement from a technical perspective. Where a data subject consents to some processing activities but not others, it will be necessary to segregate his or her personal data in such a way that it is only processed for purposes that the data subject has consented to.

An additional aspect of granularity is that consent must be “unbundled.” This means that the consent should not be bundled with other non-privacy related terms. The Guidance accepts that there may be exceptions to this rule where bundling is “appropriate,” but unfortunately the Guidance does not clarify when this is likely to be the case. It is currently common for data protection consents to be bundled together with other terms. This aspect of the Guidance therefore suggests that many existing consents will not be valid under the GDPR.

**Record Keeping**

Article 7(1) of the GDPR requires a controller processing personal data based on consent to be able to demonstrate that the data subject has consented to the processing. The Guidance interprets this requirement to mean that organizations must have an “effective audit trail” showing how and when consent was given. Where consent is obtained online, this will in practice mean that the data submitted as part of the consent must be evidenced by a timestamp. In addition to upgrading systems to record consent in this way, organizations will need to consider the fact that their existing online consents have likely not been recorded in this way.

**Withdrawal Mechanisms**

Parts of the Guidance make it clear that in line with the GDPR controllers will need to make it as easy to withdraw a consent as it was to obtain it. The Guidance recommends that in order to achieve this, it should be possible for data subjects to use the method by which they gave consent, to withdraw consent. For example, where consent was given online, it must also be possible to withdraw it online. However, this alone may not be sufficient under the GDPR and the ICO also recommends that organizations should consider sending occasional reminders to individuals of their right to withdraw consent.

Currently, it is likely few consent management systems would satisfy the ICO’s draft guidance. Even where organizations are able to implement GDPR compliant consent management systems, they will need to carefully consider the consequences of using such systems. If data subjects can quickly and easily withdraw consent and
must be reminded of their right to do so, the operational effects of large numbers of withdrawn consents could be difficult to manage.

Alternatives to Consent

The cumulative effect of the draft Guidance is likely to render most existing consents invalid once the GDPR takes effect in May 2018. Obtaining new, GDPR compliant consents from new data subjects and replacing existing consents with enhanced ones satisfying the GDPR is one option for organizations, but this could be challenging from a practical perspective.

The ICO appears to recognize the practical difficulties of obtaining consent under the GDPR and points out that there are often alternative legal bases for data processing that may be more appropriate than consent, for example, processing the personal data is in the legitimate interests of the business, or where the processing is necessary for the performance of a contract. As the Guidance points out if there are practical difficulties in obtaining consent then this is a good sign that consent is not appropriate and an alternative legal ground should be used.

Next Steps

The public consultation on this draft Guidance will be open to responses until March 31, 2017, with the view to publishing final guidance on consent in May 2017. Given the significance of the draft Guidance, we expect that the ICO will receive a large number of responses.

In the meantime, companies should carefully consider how they will implement the numerous new requirements under the GDPR and in particular review data privacy policies, notices and consents to determine how these will need to be amended and whether use of consent is still appropriate in a GDPR world.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

William Long
Partner
+44 20 7360 2061
wlong@sidley.com

John Casanova
Partner
+44 20 7360 3739
jcasanova@sidley.com

Geraldine Scali
Counsel
+44 20 7360 2086
gscali@sidley.com

Privacy, Data Security and Information Law

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property and criminal issues.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.