Client Update

UK Information Commissioner's Office Issues GDPR Consent Guidance: What Business Should Know and Do

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

Robert Maddox
rmaddox@debevoise.com

The UK Information Commissioner's Office ("ICO") has issued detailed draft guidance on consent as a basis for dealing with personal data under the EU General Data Protection Regulation ("GDPR"), which enters into force on 25 May 2018. The ICO has also launched a consultation on the guidance open until 31 March 2017.

Businesses that will be subject to the GDPR come May 2018 should: (i) ensure their GDPR preparations reflect the ICO's guidance; and (ii) consider using the consultation to shape the ICO's interpretation of the GDPR and ensure it protects individuals' rights without placing undue burdens on business, within the GDPR's constraints.

THE GDPR & CONSENT

The GDPR overhauls data protection across the EU and beyond (where non-EU businesses offer goods or services to, or monitor activities of, EU-based individuals). Both businesses in the EU and those that target the EU should ensure they are ready to meet the GDPR's enhanced data protection requirements. Further, it appears likely that the UK government will pass legislation mirroring, or very similar to, the GDPR, which will apply after "Brexit". GDPR compliance is, therefore, likely to be relevant even for businesses operating only within the UK.

Becoming GDPR compliant will not, for most businesses, involve reinventing the wheel. The GDPR builds upon many existing legal rules and best practices. Nevertheless, failing to devote sufficient resources to GDPR-readiness could cost organisations dearly. Companies that breach the new rules will face fines of up to the higher of 4% of annual worldwide turnover or €20 million.

While individuals' consent remains a legal basis for processing personal data, the GDPR ratchets up what is required to obtain valid consent; it must be "freely given, specific, informed and unambiguous" in the form of "a statement" or "clear affirmative action".

Pre-ticked opt-in boxes, never a favourite of EU regulators, plainly will become a thing of the past. What else will change?

THE ICO GUIDANCE

First, businesses should examine the sufficiency of existing consents. Consents obtained under the current data protection regime will remain valid, provided they meet the new GDPR requirements. If they do not, businesses should obtain fresh consents or put in place alternate bases for processing of that data (and communicate that basis to the relevant individuals).

Businesses should take note that consent from a counterparty to a contract must be obtained separately from other contractual terms and conditions and should not generally be a precondition to signing up to a service. This means, for example, that in an online transaction, the consent to future marketing contacts generally should be obtained through an affirmative tick in a box separate from the consent box for the transaction itself.

However, for many business purposes, such as handling customer data to provide goods or services or employee data to manage employment relationships, consent is not required because other provisions of the GDPR can (and should) be relied upon—notably, necessity for the performance of a contract or employer's legitimate interests

Second, consent requests must be carefully drafted and tailored to their specific context. Organisations should proactively direct individuals' attention to consent requests, and keep them separate from general terms and conditions. At a minimum, a request should identify the data controller's name, reasons for the data collection, how the data will be used, and who will use it. Consent requests also must explain that the individuals can withdraw their consents at any time and how they can do it.

Such transparency is paramount. The ICO stresses, for instance, that businesses should disclose to individuals the names of the third parties that will process their data. In the ICO's view, a reference to a generic class of organisations is inadequate because it does not give individuals sufficient oversight and control over their data.

Third, organisations should ensure that their consent procedures give individuals genuine choice and control over how their data is handled. The ICO suggests that consent would be difficult, although not impossible, to obtain in the employment context, given the disparity in bargaining power between the employer and the employee. This will make it difficult to obtain valid consent in employment contracts. Instead, employers may need to rely on other bases for processing their employees' data, such as necessity for the performance of the employment contract or the employer's legitimate interests. If they do not, they may face a challenge in showing that consent was "freely given".

Similarly, organisations may find it difficult to rely on consent as a basis for processing where, if the consent is not given, they will nevertheless process the data on other grounds. Relying on "fall-back" provisions where the validity of consent is questionable could breach the GDPR's requirements of fairness and transparency.

Therefore, organisations should determine whether consent is the most appropriate and efficient basis for processing each particular category of personal data they control. Where businesses rely on non-consent grounds for processing, they should document and communicate those grounds in accordance with the GDPR's requirements, such as via privacy notices.

Fourth, organisations will have to periodically review whether existing consents remain valid. As noted above, the GDPR gives individuals the right to withdraw their consents at any time, and data processing based on a consent that has been withdrawn must cease (though pre-withdrawal data processing is unaffected).

The ICO also advocates proactive consent management by data controllers. For example, it recommends that organisations refresh consents every two years in most cases. As such, businesses should consider having systems in place to alert them when new consents might be required.

Fifth, businesses must fully document consents to create an audit trail. Under the GDPR, organisations relying on consent to process data must be able to demonstrate that the individual actually consented. Business records should indicate which individuals gave their consents, what information they were provided, when and how they consented, and whether they withdrew their consents. For example, such records could include a time-stamped capture of the individual's consent form and a copy of the privacy policy or notification in place on that date.

Sixth, complying with the current guidance does not necessarily ensure compliance in the future. The ICO acknowledges that it will continue to revisit its approach as future EU guidelines and best practices develop post-May 2018. Businesses should do the same to ensure they meet the regulators' evolving expectations as the GDPR comes into force and is enforced.

Debevoise is available to assist organisations wishing to contribute to the ICO's consultation and advises businesses, both in and outside of the EU, on all aspects of GDPR preparedness.

* * *

Please do not hesitate to contact us with any questions.