Seeking consent under the General Data Protection Regulation

23/08/2017

TMT analysis: How should businesses go about obtaining valid consent to the processing of personal data? Tim Hickman, associate at White & Case, takes a closer look at the conditions that must be met for the purposes of the General Data Protection Regulation (GDPR) and says businesses should ensure that they seek consent when appropriate, rather than relying solely on consent as their default legal basis for processing personal data.

What are the changes to the definition of consent under the GDPR?

The concept of consent, set out in Article 4(11) of the General Data Protection Regulation (EU) 2016/679, largely builds upon the existing definition of consent in Article 2(h) of the Data Protection Directive 95/46/EC.

However, the GDPR also makes it harder for businesses to obtain valid consent to the processing of personal data. For consent to be valid, the following conditions must be satisfied:

- unambiguous—both the Data Protection Directive and the GDPR are clear that there can be no room for ambiguity (ie there must be no doubt that the relevant individual consented to the relevant processing activity, regardless of whether consent is given expressly, or by implication). Any doubt will be construed against the business
- clear affirmative action—the GDPR places significant emphasis on the fact that valid consent requires a positive action from the relevant individual. Silence and failure to opt-out (eg failure to untick a pre-ticked box) will not amount to valid consent
- freely given—consent will not be valid if the individual has no genuine and free choice, or is unable to refuse or withdraw his or her consent without detriment
- informed—both the Data Protection Directive and the GDPR require that consent must be 'informed' (ie the individual must be given sufficient information to understand what he or she is consenting to). This information must be provided in an easily accessible form, using clear and plain language which does not contain unfair terms
- specific—the business seeking consent must provide the individual with a clear explanation of the purposes for which his or her personal data will be processed. It is not possible to seek consent for purposes that have yet to be decided
- evidence of consent—under the GDPR, businesses must be able to demonstrate to data protection authorities (DPAs) that they have obtained valid consent (to the extent that they rely on consent to justify the processing of personal data). If a business cannot demonstrate that it has obtained valid consent, then it will be presumed that the business has failed to do so

What challenges are raised?

Many businesses seek consent where they do not need to do so (or where they should not do so). Consider an online service provided to consumers. A business that provides a consumer service typically provides that service subject to a set of terms of use (or similar) that govern the provision of the service.

The business could justify the processing of the user's personal data on a number of different legal bases (eg performance of the contract, legitimate interests, compliance with applicable law etc). Nevertheless, many businesses persist in asking users to consent to the processing of their personal data in connection with the provision of such services.

If a user signs up to the service and the business collects consent, and the user later withdraws his or her consent (which he or she is entitled to do) but wishes to keep using the service, then the business will be in a difficult position. Either:

- the business honours the withdrawal of consent and ceases all processing of the user's personal data—effectively requiring the business to terminate the user's account (which can be difficult to justify under consumer protection law, as it would make it impossible to process any refunds, etc), or
- the business continues to process the personal data needed to provide the service, regardless of the withdrawal of consent (in which case the original consent was invalid, since it was not freely given)—given that the user's personal data can be lawfully processed in the context of such a service using legal bases other than consent, it would be better for many businesses not to seek consent at all

Of course, it is important for businesses to carefully consider whether they need consent or not on a case-by-case basis. In some circumstances (eg where a service involves the processing of health data, or other sensitive personal data) consent may be the only option.

However, businesses should only seek to rely on consent as a legal basis for processing personal data where that processing is genuinely voluntary, without any element of compulsion or obligation, and where the individuals are free to withdraw their consent at any time. If these conditions are not met, then any consent obtained is unlikely to be valid for the purposes of the GDPR.

It should also be noted that consent is not always available in all cases. To the extent that there is a 'clear imbalance' between a business and an individual (ie, an unequal bargaining position) any consent obtained for the purposes of the GDPR will be invalid. For example, if an employer asks its employees to consent to the processing of their personal data, the employees may feel as though they cannot refuse without jeopardising their employment. In such cases, it would not be possible for the employer to obtain valid consent.

Is there any practical guidance from the regulators about how connected service providers might fulfil the consent requirements?

The Article 29 Working Party has published guidance on the definition of consent for the purposes of EU data protection law. The guidance clarifies, among other things, that:

- consent requires an action or statement by the individual that clearly signifies agreement (ie, passive acquiescence is insufficient), and
- businesses must provide individuals with a clear and simple explanation of the processing activities to which they are consenting

How might lawyers advise their clients about complying with the new consent requirements?

Businesses should:

- ensure that they seek consent when appropriate, rather than relying on consent as their default legal basis for processing personal data
- be able to demonstrate that valid consent was actually obtained (eg by maintaining a clear electronic audit trail connecting the clicking of a consent button to the relevant user's account)
- provide mechanisms that make it as easy for individuals to withdraw consent as it was to give consent in the first place

Tim Hickman advises on all aspects of UK and EU privacy and data protection law, from general compliance issues (such as implementing privacy policies and consent forms) to more specialised issues (such as managing data breaches, structuring cross-border data transfers, and complying with the 'right to be forgotten'). Tim has a detailed knowledge of the GDPR, and co-authored White & Case's Handbook on that legislation. Tim has significant experience of working with a wide range of clients in the EU, the US and Asia and has also spent time on secondment at Google, advising on cutting-edge privacy and data protection issues.

Kimberly Sharp, a trainee solicitor at White & Case, assisted with this interview.

Interviewed by Kate Beaumont.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.