Consent vs legitimate interests: Part 1

In the first of this two part series, Mark Watts, Partner at Bristows, looks at the key elements of consent as a grounds for data processing. The second part will deal with legitimate interests

As a result of the publicity surrounding the introduction of the General Data Protection Regulation ('the GDPR'), several popular myths took root regarding the need for consent. Apparently, 'consent is always required under the GDPR in order to process personal data'. Clearly, this isn't true, and there are a number of other 'lawful bases' under Article 6 upon which the processing of personal data can be based.

Even now, it is not unusual to hear it said that, 'consent is the best lawful basis to rely on under the GDPR if you can get it.' Even this is not true. While there are circumstances where consent is the best option, this is not generally the case; it all depends on the circumstances of the processing.

This article looks at the key elements of two of the lawful bases under Article 6 of the GDPR, namely, consent and legitimate interests.

Essential elements of consent

Most of the requirements for a valid consent under the GDPR are the same as those under the previous law. However, some aspects of consent under the GDPR have been 'upgraded'. For example, consent now needs to be 'unambiguous' and given by a clear, unambiguous action. Moreover, Article 7 of the GDPR elaborates further such that, taken together, the requirements for a valid consent can be thought of as comprising:

- informed;
- specific;
- freely given;
- granular;
- revocable;
- affirmative; and
- recorded.

'Informed'

The idea that consent needs to be informed in order to be lawful is well understood and common, for example in the fields of healthcare and employment. The basic requirement is that an individual who is asked to consent to particular processing must be in a position to understand what they are consenting to. In many ways, this requirement overlaps significantly with the obligations of 'fairness' and 'transparency' (under Articles 12-14 of the GDPR); that is, the obligation to give 'notice' of the processing to the individual. However, the obligation to obtain consent (where consent is used as the processing basis) and the obligation to give notice are separate obligations that must each be complied with.

One question that arises is: how detailed the information provided to the individual should be and what areas it should cover?

In summary, to be 'informed', an individual must be informed of who is relying upon consent (the controller), who else will be relying on the consent (other controllers), the purpose for which the consent is being sought, what will be done with the data, and the existence of their right to withdraw their consent. This information needs to be both understandable and distinguishable from other information provided to the individual concerning other matters, although there is some flexibility about how the information may be provided.

'Specific'

The obligation that consent must be specific overlaps with the obligation that it should be informed. There are two main aspects to this.

Firstly, the consent must be specific about the identity of the controller(s) who are relying upon the consent to the processing (e.g. it can't refer vaguely to 'selected third parties').

Secondly, the consent must also be specific about the 'purpose' of the processing; that is, it cannot be vague and must put an individual in a position where he or she is able to make an informed decision over the use (or uses) for which their personal data are to be processed. It should be noted, though, that there is some leeway in respect of processing for

(Continued on page 12)

(Continued from page 11)

the purposes of scientific research where it is acknowledged in the GDPR (Recital 33) that it is not always possible to specify in advance the detail of future research purposes that may be undertaken.

'Freely given'

The difficulties associated with obtaining 'freely given' consent are not entirely new and many of the challenges faced under the GDPR also existed under the previous law. However, these difficulties have become more acute under the GDPR in circumstances where there is either an imbalance of power, or at least a perception of an imbalance of power.

For example, it is now widely understood to be problematic for an employer to rely on the consents of its work force in any general way in respect of its processing of their data for employment purposes. A public authority fulfilling certain public functions may also not rely on consent where provision of personal data is mandatory, and an individual has no real choice.

Essentially, to be freely given there must be no detriment or negative consequences to the individual as a result of any refusal to give consent. If there are, then this is often a sign that the consent is not being obtained in a freely given manner.

One new aspect of the requirement that consent be freely given is 'conditionality'. This is the idea that a controller may not 'condition' its performance or acceptance of a contract on an individual consenting to processing that is not necessary for the performance of that contract. Where this is the case, there is a strong presumption that any such consent so obtained is not valid. Behind this concept (under Article 7(4) of the GDPR) is the idea that an individual's consent and control over his or her personal data is a fundamental right that may not be traded as consideration for a service, even where that service is provided free of charge as with many online services.

One example given by the EU data protection authorities is of an online photo editing service where individuals are required to consent to direct marketing in order to receive the service. In such a case, for any consent to be valid, the service provider would also have to offer an alternative service where consent to direct marketing is not a condition.

> ***"Another myth about GDPR consent is that it may not be implied, but this is not correct. Affirmative consent may be implied but only from an act, as opposed to silence or inactivity."***

Moreover, the existence of other similar, competitive services in the marketplace that do not require consent to direct marketing is not sufficient to avoid the conclusion that any consent is not freely given. One interesting aspect of this is that consent linked to the performance of a contact is only valid in respect of processing 'necessary for the performance of the contract'. At first blush, this appears to overlap completely with the lawful bases under Article 6(1)(b) that processing may be performed if it is necessary for the performance of the contract. However, while it is true that there may be circumstances where the overlap is complete, there are also circumstances where obtaining such a 'linked' (and overlapping) consent is still helpful.

For example, the lawful basis under Article 6(1)(b)) is only relevant in relation to the processing of 'ordinary' personal data; no such basis is available in respect of the processing of 'special category data' (under Article 9 of the GDPR). This being the case, where the performance of a contract involves the processing of (say) health data, there may be circumstances where it is nevertheless necessary to rely an individual's 'linked' consent.

'Granular'

There are several aspects to the requirement for consent to be 'granular'.

Firstly, it must be 'unbundled'; that is, it should be presented and obtained separately to any other terms and conditions that may be relevant and not be buried in the small print either of a contract or of a privacy policy. Secondly, if data are being collected for several purposes at the same time and consent is to be relied upon for each of these different purposes, such consents must be obtained individually; that is, the consent must be sufficiently 'fine-grained' that an individual may select between the various purposes.

'Revocable'

For consent to be valid, it should be as easy to revoke as it is to give. To some extent, this requirement is why there has been an increase the number and granularity of settings and 'sliders' in connection with certain online and mobile services. This requirement would not be fulfilled, for example, where consent is initially obtained online (e.g. via clicking a link or ticking a box) but may only be revoked by making a phone call or sending an email. If consent is revoked, there should be no detriment or cost to the individual concerned (this is the other side of consent needing to be freely given). And, of course, if consent is revoked any processing based on it must cease. However, processing, even of the same personal data, which is based on a lawful basis other than consent may continue for as long as that lawful basis continues to be met.

'Affirmative'

To be valid, consent must be 'active'; that is, it may not be implied from silence, and the use of pre-ticked boxes is expressly prohibited. There must be an act that is an unambiguous indication of the individual's wishes, and it

must be obvious to the individual concerned that he or she has consented.

Another myth about GDPR consent is that it may not be implied, but this is not correct. Affirmative consent may be implied but only from an act, as opposed to silence or inactivity. So, for example, an individual may indicate that he or she consents in a variety of ways, including dropping a business card into a fish bowl at a trade show, or swiping on his or her mobile phone (having been informed that this is the act of consent).

In some situations, consent required needs to be 'explicit. This means that it cannot be implied from an act, but needs to be based on a statement, which may be written or oral. It is also important that the statement refers to the processing that requires explicit consent under the GDPR so that an individual is in no doubt as to what he or she has consented to. This might, for example, include the processing of 'special category data' (under Article 9) or automated decision making (under Article 22).

'Recorded'

Under the GDPR, it is a requirement that consent replied upon is recorded by the controller. It should also be borne in mind that the burden of proof to establish a processing basis is on the controller and its ability to discharge this obligation forms part of its broader 'accountability' obligation.

Controllers should record the following:

- who consented;
- when the consent was obtained (e.g. through a time stamp);
- what the individual was told (what they understood they were consenting to);
- the means by which they consented; and
- the status of the consent (i.e. whether it is valid or withdrawn).

Consent: a summary

As can be seen, consent is not as straight forward to rely on under GDPR as under the previous law. Generally speaking, consent as the processing basis works best when:

- something unexpected is being done with the personal data, such as a change of processing purpose or new data sharing;
- the processing involves special category data and no other processing basis under Article 9 is available;
- the processing involves geolocation data;
- the processing is likely to involve the sending of direct marketing communications; and/or
- the processing works in conjunction with the setting of cookies (or other tags) in circumstances where consent is required under the e-Privacy Directive (Privacy and Electronic Communications Directive 2002/58/EC).

In the next part, I will turn my attentions to the legitimate interests ground for data processing. In addition, Part 2 will provide case studies showing how consent and legitimate interest operate in practice to legitimise data processing.

Mark Watts
Bristows
mark.watts@bristows.com