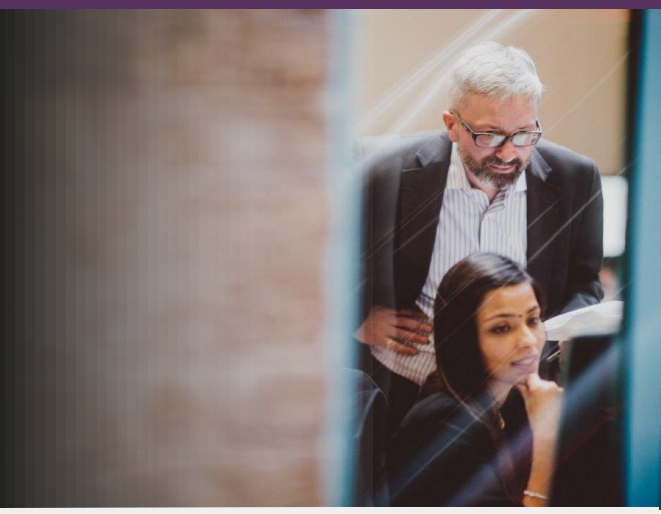
RIAA Barker Gillette

Always Available

GDPR: The concept of consent



April 2018

Consent is one of the core elements of data protection legislation, however it is not the only basis for processing personal data

Despite Brexit, the General Data Protection Regulation (GDPR) will come into effect on 25 May 2018 and will soon be enveloped into UK law under the proposed Data Protection Bill.

The GDPR clarifies the concept of consent and ensures that the concept will be interpreted consistently across all jurisdictions.

Consent under the GDPR?

The GDPR sets a high standard for consent and defines 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".

This expands upon the existing definition of consent under the Data Protection Act 1998 (DPA). The additional requirements are that consent must be:

- freely given;
- unambiguous; and
- made by a statement or clear affirmative action.

But what does that mean?

Freely given: whilst already a requirement of the DPA, the GDPR specifically clarifies that consent is not freely given if:

- there is a clear imbalance between the controller and the data subject (such as the relationship between employer and employee); and/or
- the data subject has no genuine or free choice and is unable to withdraw consent without detriment.

Unambiguous: there must be a clear indication that the data subject is positively consenting to the processing of their personal data. Where consent is obtained for a single processing activity, such as subscribing to a newsletter, this will be easier. However, where personal data is collected for multiple purposes, this will be much harder. Further, consent should be kept separate from any other terms and conditions and should not be made a precondition of any kind (see more below).

Statement or clear affirmative action: as suggested, any indication of consent must involve a clear, affirmative action or statement by the data subject. This could include:

- ticking a box or opt-in when visiting a website;
- choosing technical settings for online services; or
- any other statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data.

The GDPR specifically prohibits pre-ticked opt-in boxes and requires individual ('granular') consent options for distinct processing operations. Therefore, silence will not satisfy this condition. Further, consent must be as easy to withdraw as it is to give.

When is consent appropriate?

Consent is appropriate if the data controller can offer data subjects actual choice and control over how their data will be used. If the data controller cannot offer genuine or real choice, then consent is not an appropriate lawful basis for processing, as asking for consent would be misleading and inherently unfair to the data subject.

According to the Information Commissioner's Office (ICO), if consent is made a precondition of providing a service, it is unlikely to be the most appropriate lawful basis for processing personal data and data controllers should rely on another lawful basis provided under the GDPR. This should be well documented.

Further, public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

Other lawful bases for processing personal data

There is a general misconception that personal data can only be processed on the basis of consent. This is not true. Under the GDPR, there are five other ways to lawfully process personal data. For instance, if processing is necessary:

- for the performance of a contract;
- for compliance with a legal obligation;
- to protect the vital interests of the data subject;
- for the performance of a task carried out in the public interest;
- for the purposes of a legitimate interest.

Note: the lawful basis for processing can affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			X but right to withdraw consent
Contract			X
Legal Obligation	X	X	X
Vital Interests		X	X
Public task	X	X	
Legitimate Interests		X	

Whilst it may be true that businesses usually rely on consent as a lawful basis of processing personal data; it may be best to combine it with some other lawful basis.

According to the ICO, no single basis is better than the other, and which basis is best, depends on the purpose and relationship between the data controller and the individual.

Conclusion

Whilst businesses are not required to "repaper" or refresh all existing consents obtained under the DPA; when relying on consent it is vital to ensure that it meets the GDPR standards. If not, the consent mechanism should be altered and existing consents be refreshed and documented accordingly.

Given the additional obligations relating to consent under the GDPR, it may also be sensible for data controllers to look towards an alternative lawful basis for processing personal data.

If you have any questions regarding data protection, please contact corporate solicitor, Karen Cole.

Karen Cole
020 7299 6909
karen.cole@riaabg.com
www.riaabarkergillette.com