FYI®
For Your Information®
UK

Volume 2018 | Issue 08 | 08 February 2018

GDPR and the end of 'consent' – What is the lawful basis upon which data may be processed?

This FYI considers why the reliance on consent, widely used by data controllers for the processing of personal data, is likely to lose its effectiveness from 25 May 2018. It highlights the need for data controllers to consider putting in place an alternative basis prior to the General Data Protection Regulation (GDPR) going live.

The processing of an individual's personal data will only be lawful if it meets one of the six bases as set out below. Although consent is one of the six lawful bases on which personal data may be processed, the ease with which consent can be withdrawn by the individual means that it is unlikely to meet the requirements of data controllers, nor potentially, data processors.

Many data controllers have historically relied on express or implied consent to process personal data. From 25 May, implied consent will not be sufficient, and many existing consents given by individuals will not comply with legislation. Consent is only appropriate if the individual is offered choice and control in relation to the processing of their personal data.

If the individual does not have real control then consent will be an invalid basis for processing, with the result that any processing activity becomes unlawful. For example, an employer is unlikely to be able to rely on the consent of an employee to process personal data.

Where the data controller is relying on consent to process personal data, and an individual's consent is not compliant with GDPR on 25 May 2018, all processing of that data must immediately cease.

Data controllers currently processing personal data based on the consent of individuals, and who are considering relying on consent as the basis for processing data after May of this year, should consult with their advisers now, both on whether consent is still an appropriate basis and on whether existing consents meet the new requirements.

Six Lawful Bases

The GDPR requires that from 25 May 2018 all personal data is processed on one of six lawful bases. The six bases are:

- The **individual has given consent** to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party.
- Processing is necessary for the **performance of a contract** to which the individual is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject.
- Processing is necessary in order to **protect the vital interests of the individual** or of another natural person.
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

Guidelines on Consent

The European Union's Article 29 Data Protection Working Party (the Article 29 Working Party) consists of representatives of the data protection authorities from each member state. It has now published Guidelines on Consent. A consultation on these guidelines ended on 23 January 2018. The Information Commissioner's Office (ICO) also consulted on guidance in March 2017 and has confirmed that it will publish a final updated version of its guidance once the Article 29 Working Party finalises its guidelines. In the meantime, the ICO's current guidance on the lawful bases for processing, including consent, is found in its Guide to the General Data Protection Regulation.

The GDPR 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."

Why is the giving of consent potentially problematic?

Freely given

Where the individual giving consent does not have a choice, feels they cannot refuse, or it will be detrimental to them if they do not consent, then consent will not be valid.

Where consent is bundled up as a non-negotiable part of terms and conditions, then it cannot be considered to be freely given. Where a service involves multiple processing operations for more than one purpose, each purpose should be spelt out and the individual concerned given the choice over which purposes they consent to.

The giving of consent must be a reversible decision with a degree of control on the side of the individual giving consent, thus if they cannot withdraw consent without detriment, then consent will not be valid.

Where there is an imbalance of power in the relationship between the data controller and the individual whose data is being processed, such as in the employer/employee relationship, then it is unlikely that the data controller will be able to rely on consent for processing data. The individual could in those circumstances feel unable to deny the data controller consent to data processing without experiencing the fear or real risk of detrimental effects as a result of the refusal. The Article 29 Working Party state that "For the majority of such data processing at work, the lawful basis cannot and should not be consent of the employees due to the nature of the relationship between employer and employee."

Specific

To prevent what the Article 29 Working Party calls “function creep”, a data controller when obtaining consent must specify each purpose for which consent is being obtained, and the individual giving consent must have a choice in relation to each purpose.

Where a data controller relies on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the individual concerned for the new processing purpose.

Informed

An individual giving their consent must understand what they are agreeing to. Accordingly it is important to provide individuals with sufficient information prior to obtaining their consent to enable them to make an informed decision. Failure to do so will render consent an invalid basis for processing.

The Article 29 Working Party has said the minimum amount of information required to allow an individual to make an informed decision is:

- The data controller’s (or if more than one) controllers’ identity
- The purpose of each of the processing operations for which consent is sought
- What type of data will be collected and used
- The existence of the right to withdraw consent
- Information about the use of the data for decisions based solely on automated processing, including profiling; and
- If the consent relates to data transfers, information about the possible risks of data transfers to third countries (i.e. outside the European Economic Area) in the absence of an adequacy decision and appropriate safeguards.

Data processors do not need to be named, although to comply with the privacy notice requirements, controllers need to provide information about recipients or categories of recipients (including processors) of the data.

Information does not have to be in any particular form but it must be clear and in plain language and understandable for the average person. Where it forms part of a written contract it cannot simply be a clause in the terms and conditions. It must either be set out in a way which clearly stands out or contained in a separate agreement.

Unambiguous indication

The burden of proving consent has been given is on the data controller. An individual giving consent must do so in a clear unambiguous way by an affirmative act involving an actual deliberate action or declaration. The use of silence, inactivity or pre-ticked opt-in boxes is no longer valid.

Neither can consent be given by the same action as agreeing a contract or accepting the general terms and conditions.

When consent is to be given by electronic means, consent requests may interrupt the user’s experience to some extent to make that request effective. However, repeated interruptions may result in a degree of click fatigue rendering the giving of consent to be invalid.

In certain situations, for example where special categories of personal data are being processed (e.g. information about an individual’s health or sexual orientation) and consent is sought, there is an additional requirement that the consent be explicit. The Article 29 Working Party has not laid down requirements in relation to explicit consent but has given examples such as:

- Express confirmation of consent in a written document; and
- A two stage verification process.

There is a reminder that consent is not the only legal gateway for processing special categories of personal data and that it may not be appropriate in many situations.

The Withdrawal of Consent

Easy to do

It must be as easy to withdraw consent as it was to give it. Thus, where consent is given by one method or means then the withdrawal of consent must be possible by the same route. The provision of a method of making consent easy to withdraw is a necessary aspect of obtaining consent in the first place. If the withdrawal right does not meet the GDPR requirements the original consent is invalid. If the individual is not informed of their right to withdraw consent before actually giving consent then the original consent is also invalid.

Effect of withdrawing consent

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent remain lawful. However, the data controller must immediately stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, then the data should be deleted or anonymised by the controller.

In addition to withdrawing consent, an individual has the opportunity to request erasure of other data referring to the individual that still resides with the data controller.

Where an individual withdraws consent, data controllers wishing to continue to process the personal data on another lawful basis cannot silently migrate from consent (which is withdrawn) to another lawful basis. Any change in the lawful basis for processing must be notified to the individual in accordance with the information requirements and principles of transparency set out in the GDPR.

Consent and the Other Lawful Bases

Generally, a processing activity for one specific purpose cannot be based on more than one lawful basis. A data controller cannot, therefore, hedge their bets by listing a selection of the six lawful bases. However, if data is being processed for several purposes, each purpose may be based on a different lawful basis, provided these have been identified and communicated to the relevant individual in advance.

The lawful basis cannot be modified or changed during the processing and the data controller cannot swap from one legal basis to another. The Article 29 Working Party stresses that a data controller cannot retrospectively use the legitimate interest basis to justify processing where problems are found with the validity of consent. A data controller relying on consent cannot use any of the other lawful bases for processing personal data as back up to demonstrate GDPR compliance.

Comment

Data controllers have, in many situations, traditionally relied on the consent of an individual to process data. That consent has either been expressly given or implied. Implied consent is consigned to history, and the difficulties both in obtaining consent, and dealing with situations where consent is withdrawn, are likely to make consent a far less attractive basis for processing data following the coming into force of the GDPR on 25 May 2018.

Data controllers who can use one of the other five bases for processing data, such as legitimate interest, are far more likely to only seek an individual's consent where they don't have another legitimate basis for the processing.

The onus is on data controllers (and not data processors) to establish a legitimate basis to process personal data and they should thus:

- Determine the lawful basis for processing personal data in all circumstances.
- Document the reasons for determining the lawful basis so that it can be explained if challenged.
- Audit what special categories of personal data are held by them and by any of their data processors.
- Explain the lawful basis in privacy notices.
- Review any contracts / application forms that contain requests for consent.
- Establish or review any procedures for obtaining consent as well as dealing with an individual's request to withdraw their consent.

Both the Article 29 Working Party and the ICO remind data controllers that there is a one-off opportunity to move from one legal basis to another in relation to data processing already being carried out. This opportunity ends on 25 May 2018 after a two-year transitional period starting on 25 May 2016 when the GDPR was published and technically came into force. It does not start on 25 May 2018. The ICO confirms that it will be fair and proportionate in exercising its powers.

Authors
Gary Crockford, Head of the Knowledge Resource Centre
Nikki Williams, Senior Technical Consultant

Produced by the Knowledge Resource Centre
The Knowledge Resource Centre is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your consultant or call us on 0800 066 5433.

CONDUENT