# GDPR in Context: Consent

## Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

## Overview

Under existing Data Protection Rules, a data controller may rely on the consent of an individual (or explicit consent in the case of processing of sensitive personal data) in order to justify and legitimise its use of personal data. The existing rules do not give any clear definition of consent, although the Article 29 Working Party ("**WP29**") has issued guidance, both generally and in the context of the employment relationship, which makes clear that consent must be genuine, meaning that it must be freely given, specific and informed, and must be capable of being withdrawn.

However, it is important to note that consent has never been a panacea to relieve data controllers of their overriding obligations to comply with the data protection principles (eg, notwithstanding any consent, data controllers still may not obtain and process excessive amounts of data in the context of the specific purpose for which the data is being collected). Reliance on consent has always required careful consideration as to whether use of consent is appropriate, and if so, whether the manner in which it is obtained is valid. Under the GDPR, that analysis becomes even more important.

## Consent under the GDPR

Under the GDPR, consent remains a legitimate processing ground for processing of both sensitive and non-sensitive data. However, the GDPR, unlike existing rules, sets out clearly defined requirements around consent, and mandates that consent may only be obtained for one or more specific purposes, with multiple consents required where the controller intends using data for multiple purposes.

The GDPR also addresses the common quandary as to whether, where a controller proposes using personal data for new purposes, it will be required to obtain consent from individuals for that new purpose, and clarifies that controllers may only process personal data for purposes, other than those for which the data was originally collected, if the new purpose is compatible with the original purpose in the sense that there is a link between the purposes. In considering the question of compatibility, controllers should take into account factors such as the consequences of the additional processing, the safeguards that are in place for both the original and the further processing, and importantly, the reasonable expectations of the individuals, bearing in mind the context of the original processing.

The requirement for explicit consent remains with regard to processing of special categories of data, and has now been introduced in the context of automated decision making and profiling, as well as consent based transfers to third countries. Furthermore, the GDPR specifically links the concept of consent to certain data subject rights, including the right to be forgotten, the right to data portability and the right to restriction of processing.

---

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

# Consent

## Meaning of consent

Reflecting much that is in existing WP29 guidance, under the GDPR, consent must be freely given, specific and informed, and must constitute an "*unambiguous indication of [an individual's] wishes by which he or she, by statement or clear affirmative action, signifies his or her agreement*". The GDPR makes clear that it is misleading to rely on consent if a controller is in a position to, and will be relying on, another legitimate processing ground.

***Freely Given***

Consent will only meet the "freely given" criterion where an individual has genuine or free choice and the ability to refuse or withdraw consent without detriment. Individuals must be informed of the right to withdraw, and the exercise of this right must be as easy for the individual as giving consent in the first place.

Furthermore, the GDPR makes clear that it is not permissible to rely on consent if a contract is made conditional on the consent, notwithstanding that the consent is not strictly necessary for the performance of the contract.

***Specific and Informed***

In order for consent to meet the specific and informed criterion, the individual needs to be made aware of the identity of the controller (including third parties) and the purposes of the processing, bearing in mind that if there are multiple processes, multiple consents will be required.

***Unambiguous***

The requirement the consent be unambiguous is a key element of the definition of consent under the GDPR, requiring as it does a statement or clear affirmative action signifying agreement to the processing. In that regard, the GDPR makes it clear that silence or inactivity is not acceptable as a form of consent, so that eg, pre-ticked boxes, or failure to opt out by an individual, will not constitute valid consent.

There has been some debate in relation to the distinction between unambiguous consent and explicit consent under the GDPR. However, the difference appears to centre on the understanding that unambiguous consent can be demonstrated through affirmative conduct, whereas explicit consent probably requires more.

# Consent

## Consent and children

The GDPR contains specific provisions in relation to children's consent to the provision of information society services. Member states have the option as to whether the age for consent is set at 16 years (as set out in the GDPR) or lower, and below the specified age, parental or guardian consent will be required where information society services (which will cover the vast majority of online services) are offered to a child. Controllers will need to expend reasonable efforts to verify that parental consent has been given, using available technology.

## Conditions for consent

First and foremost, a controller relying on consent to legitimise processing will need to be in a position to demonstrate that it has obtained the necessary consent. It is also important to note that consent will not be valid if an individual has not been notified of his or her right to withdraw, and as set out above, that right must apply at any time and must be implemented as easily as giving consent in the first place. If consent is subsequently withdrawn, there will, however, be no impact on pre-withdrawal processing.

As with all of the information requirements under the GDPR, the information must be provided to individuals in an intelligible and easily accessible form, in clear and plain language. In that regard, there is a clear link between the GDPR requirements relating to consent, and consumer protection and the prohibition on unfair terms in consumer contracts. As a result of this, where consent is sought in the context of a written declaration which also concerns other matters, any data processing consent must be clearly distinguishable.

## Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning customer data and other personal data which it controls, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place.

In order to ensure compliance with the GDPR, data controllers will need to review their existing processing activities, to identify where they rely on consent, and to consider whether, in the specific contexts where they do rely on consent, other legitimate processing grounds are more appropriate justifications for processing. Where reliance on consent is unavoidable, or has been mandated under the GDPR, controllers should review their existing consent language and collection methodologies, to ensure that they implement procedures to ensure that consent is demonstrable and targeted, taking into account whether it needs to be explicit, and that they revise consent language, if necessary, to ensure that separate consents, meeting the intelligible and easily accessible information requirements, are obtained.

## Contacts


**Anne-Marie Bohan**
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

**Deirdre Kilroy**
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

**Chris Bollard**
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

**Carina Lawlor**
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

**Christine Woods**
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com


12.10.17