Consent

information commissioner
Barrantagh Fysseree

This guidance explains what 'consent' is in terms of processing personal data, when it is required, and what controllers are required to do to ensure consent is valid.

There are two common misconceptions about consent, which are:-

1. Consent is always required to process personal data; and
2. Informing data subjects how their personal data will be processed constitutes 'consent' to the processing.

In order for the processing of personal data to be lawful, it must meet at least one of the six grounds set out in Article 6(1) of the Applied GDPR.

> Consent is one of those grounds: consent to the processing only becomes **necessary** if NONE of the other five grounds for processing applies.

To rely on consent as the ground for processing, a controller must be able to demonstrate that they have obtained consent. There must be no ambiguity in obtaining or evidencing consent.

Where the personal data being processed includes special category data, and the "explicit consent" exception to the prohibition on processing special category data is being relied upon, the controller must be able to demonstrate that **"explicit consent"** has been given.

In addition to the Articles and Recitals of the Applied GDPR, this guidance refers to the EDPB Guideline on consent, which is published online at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

What is "consent"? **2**

Meeting the criteria for valid 'consent' **3**

1. 'freely given' 3
2. 'specific' 4
3. 'informed' 5
4. "unambiguous indication of ... wishes"... "by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed" 6

Consent and Minors - general **8**

Child's consent in relation to information society services (Article 8) **8**

Mental Incapacity **9**

Special category data and explicit consent **10**

What is "consent"?

Consent, in data protection terms, has a specific meaning.

Article 4 of the Applied 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."*

The legal requirement for consent is intentionally challenging and requires all the elements of the above definition to be met.

> *Note: 'consent' will not make the processing of personal data 'lawful' when the processing is prohibited by law. (For example, Regulation 137 of the GDPR and LED Implementing Regulations 2018 (Prohibition on the requirement to produce relevant records))*

Article 7 sets out further conditions that must be met.

In summary, those conditions are:-

1. Consent for different processing activities or purposes must be separate and distinguishable.

2. Prior to giving consent, data subjects must be advised that it can be withdrawn at any time.

3. Consent must be as easy to withdraw as it was to give.

4. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

5. The performance of a contract or provision of a service cannot be conditional upon consent to processing personal data that is not necessary for that contract or service.

In addition, Article 7(2) states:-

> "*Any part of such a [written] declaration which constitutes an infringement of [the Applied GDPR] shall not be binding.*"

Meeting the criteria for valid 'consent'

1. 'freely given'

Recitals 42 & 43 to the Applied GDPR provide further information regarding "freely given".

The EDPB Guideline states that "free" implies real choice and control for data subjects where there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if they do not consent.

Recital 42 states:-

> *"…. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."*

Consent is <u>not</u> "freely given" if:

- separate consent cannot be given for different purposes/data processing operations;
- it is bundled up within general terms and conditions for a service; or
- the data subject has no genuine and free choice, is unable to refuse or withdraw consent without detriment, or there is any element of compulsion or coercion.

Recital 43 ("imbalance") states:-

> *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."*

Imbalance, i.e. where data subjects cannot effectively exercise real choice or free will, can occur in many circumstances; however, two examples are the relationships between data subjects and public authorities or with their employers.

Public authorities

In most cases, a public authority will have a 'vires', or a statutory power, to process personal data and, as such, will not require consent.

However, if an individual choses to request or accept a discretionary service, facility or assistance provided by a public authority, for example, the provision of discretionary social care services for a child or elderly persons, the public authority <u>will</u> require consent to process the associated personal data and must be able to demonstrate that consent.

Employer and employees

Where employers are required to process personal data by law, such as income tax returns, health and safety reporting, etc., consent is not be required.

However, an imbalance is likely to occur in other processing of an employee's personal data, for example, the use of biometric attendance systems or active employee monitoring. Unless there would be no adverse effects on employees if they refused to give 'consent' to that processing of their personal data, the controller cannot demonstrate that consent was 'freely given'.

The EDPB Guideline states:-

"Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees … due to the nature of the relationship between employer and employee.

However, this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent."

2. 'specific'

Article 6(1)(a) *(and 9(2)(a) - Special category data*) states that consent must be given for *"one or more specific purposes"*.

Recital 42 relates to the "specific" element of consent and states:-

> *"the controller should be able to demonstrate that the data subject has given consent to the processing operation."* (emphasis added)

Recital 39 states:-

> *"the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data."* (emphasis added)

Therefore, the controller must have determined the specific, explicit and legitimate purpose(s) for the intended processing activity **prior** to seeking consent and those purposes for processing must be specified, distinguishable and unambiguous to the data subject. (Guidance on transparency is available on the website)

When the processing of personal data has **multiple purposes**, and consent is being relied on as the only lawful ground for processing, separate consent must be given for each of the distinct processing purposes (*granular consent*), in particular, for direct marketing.

Consent will not be valid if the purposes are unspecified or the processing undefined. For example, phrases such as *"in your interests"* or *"where expedient"* are not "specific".

Consent cannot be obtained for 'sharing' of personal data with third parties unless there is certainty (or specifics) as to why, when, how and what sharing of personal data will occur and with whom.

Instead, and unless another ground for processing applies at that time, consent to the lawful sharing of specific personal data must be sought once the requirement has been identified and obtained prior to the sharing occurring.

The EDPB Guideline states:-

"Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject."

"… to comply with the element of 'specific' the controller must apply:

> *i Purpose specification as a safeguard against function creep,*
>
> *ii Granularity in consent requests, and*
>
> *iii Clear separation of information related to obtaining consent for data processing activities from information about other matters."*

3. 'informed'

To consent to processing the data subject must be able to make a properly informed decision.

Recital 42 states:-

> *"For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."*
>
> *"In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given."*
>
> *"… a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair [contractual] terms."*

"Informed" is linked to Article 5(1)(a), the principle of lawfulness, fairness and transparency, and Article 13, the obligation to provide the data subject with information about the processing of personal data.

However, providing transparency information (Articles 5(1)(a) and 13) must not be confused with, 'consent' to the processing under Article 6 . Any requirement to confirm 'consent' must be separate to, and distinguishable from, the transparency information.

Consent cannot be "informed" if it is "bundled" with other written agreements or statements, for example, as part of general terms and conditions.

Recital 39 states:-

> *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned …"*

The EDPB Guideline states:-

"The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR."

"… where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named."

"… depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand."

4. "unambiguous indication of … wishes"… "by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed"

Controllers must be able to **demonstrate** that consent was clearly given - Article 7(1) states:-

> *"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."*

Consent can be given by a written, electronic or oral statement. For example,

- by ticking a box on a website
- by choosing technical settings for information society services , or
- by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data.

However, silence, inactivity or the use of pre-ticked boxes **does not** constitute valid consent.

Recital 42 states:-

> *"… the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given."*

Recital 32 states:-

> *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent."*

The EDPB Guideline states:-

"The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice."

"… consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing."

"A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing…. "

"Consent can be collected through a written or (a recorded) oral statement, including by electronic means."

"Perhaps the most literal way to fulfil the criterion of a "written statement" is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR."

"The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice."

Consent and Minors - general

It is generally accepted that a person who has attained the age of 16 can give consent, provided he or she is capable of understanding the action to which he or she is consenting. Equally, a minor under the age of 12 years cannot, generally, consent and the consent of a parent or guardian must be sought.

Whether a person between the ages of 12 and 16 years of age can give consent to the processing of their personal data depends upon the circumstances of the case and the nature and purposes of the processing.

Unless a controller is certain that the processing will not, or could not, cause any adverse effect to the minor, it is recommended that, the consent of a parent or guardian should be sought. However, in some cases, the action of seeking the consent of a parent or guardian to the processing may itself cause adverse effects for the minor.

There are specific requirements in relation to the language used when seeking consent from minors.

In particular, **Article 12** states:-

> *"The controller shall take appropriate measures to provide any information referred to in Articles 13 … in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. "*

Whilst **Recital 58** states:-

> *"any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."*

Child's consent in relation to information society services (Article 8)

In relation to the offering of Information Society Services directly to children **below the age of 13**, special rules apply.

The processing is only lawful if consent is given by a person with parental responsibility for that child and the controller makes reasonable efforts to verify that valid consent has been given.

> *Note: Article 8, and the associated age limit of 13 (in the Isle of Man), does not apply to any other processing of children's data or in any other circumstances.*

Recital 38 states:-

> *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. "*

The EDPB Guideline provides extensive commentary on Article 8 in paragraphs 124 - 151.

The 'exception' to parental consent

Whilst there is nothing expressed in Article 8, or in other Articles, Recital 38 refers to a specific, important, set of circumstances where parental consent will not be necessary, irrespective of the age of the child.

Recital 38 states:-

> *"The consent of the holder of parental responsibility should not be necessary in the context of* ***preventive or counselling services offered directly to a child****."*

The **EDPB Guideline** clarifies this by stating:

"It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation."

This can apply equally to the processing of personal data of children by such services provided 'offline' or via 'Helplines'.

Mental Incapacity

A person over 18 who lacks capacity through mental impairment cannot give valid consent.
Where a person has some form of mental impairment then consent may be obtained from a person with the relevant power of attorney for the data subject.

Special category data and explicit consent

Where processing includes special category data, such as information relating to health, an exception to the general prohibition on processing special category data set out in Article 9(2) of the Applied GDPR (or Schedule 2 to the GDPR and LED Implementing Regulations 2018) must also apply.

Article 9(2)(a) provides the 'explicit consent' exception to the prohibition on such processing as follows:-

> *"the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law provide that the prohibition [on processing special category data] may not be lifted by the data subject"*

When it is necessary to obtain 'explicit consent', it must be made clear to the data subject what specific processing the 'explicit consent' covers to enable them to understand the particular aspects of the processing which may affect them, such as further disclosures/sharing.

Explicit consent cannot be 'pre-emptively' obtained for 'sharing' personal data with other parties.

Instead, and unless another exception to the prohibition on processing special category data applies, explicit consent to the lawful sharing must be sought once the necessary requirement to share has arisen and obtained prior to the sharing occurring.

Explicit consent suggests that the data subject should signify agreement in writing. However, this would not be appropriate in all cases, for example where confidentiality is required. If explicit consent is not in writing, it is recommended that some form of record, such as a file note, is kept indicating how explicit consent was given, in order to demonstrate compliance.

For medical practitioners, further information about the practicalities of seeking and recording consent is available from their relevant regulatory body, or the NHS website, for example: https://www.nhs.uk/conditions/consent-to-treatment/