Consent

At a glance

- The DPA sets a high standard for consent. However, consent will not always be the appropriate legal basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- If you rely on consent, check your business processes that involve collecting consent and your existing consents. Refresh your consents if they don't meet the DPA standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate and distinguishable from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third-party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Consent to processing cannot be a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.
- Where there is a significant imbalance between the position of the data subject and the data controllers (e.g. in relationship between citizens and public authorities, or relationship between employees and employers) consent may be difficult to qualify as a valid legal basis for processing.

Checklist

Asking for consent

- We have checked that consent is the most appropriate legal basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.

- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We make it easy for individuals to withdraw their consent at any time, and publicize how to do so.
- We act on withdrawals of consent as soon as we can.
- We don’t penalize individuals who wish to withdraw consent.

In brief

Why is consent important?

Consent is one of a number of conditions for processing, and explicit consent can also legitimize use of sensitive personal data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimize automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to enforcement actions.

When is consent appropriate?

Consent is one legal basis for processing, but it is not the only legal basis and there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you still plan to process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be a valid legal basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent. This is because consent is unlikely to provide a valid legal basis for the processing where there is a significant imbalance between the data subject and the data controllers.

What is valid consent?

Consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. This means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should you obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. It is best practice to include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Relevant provisions

Data Protection Act (2021 Revision)

Schedule 2, paragraph 1: Legal conditions for processing personal data

Schedule 3, paragraph 1: Legal conditions for processing sensitive personal data

Section 1: Definition of "consent"

Schedule 5: Conditions of consent

Further guidance

ICO: Guidance on consent

Article 29 Working Party: Guidelines on consent under Regulation 2016/679