

## [Guidance on when and how to ask for consent in relation to processing personal data](#)

Under the new legislation, we must have a legal basis for processing personal data<sup>1</sup>: Our legal basis could be:

- a contract with the individual – *for example, the processing of personal data by the employer for the purposes of paying the employee will be necessary for the performance of the employment contract;*
- compliance with a legal obligation – *for example, sharing employee's personal data with a pension provider based on the legal requirement to auto-enrol eligible employees into a pension scheme;*
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – *for example, to complete official functions or tasks in the public interest.*

Where none of these apply, “consent” provides another legal basis. Asking for consent will be necessary in situations where we want to process the personal information for any purpose outside of our core functions/public tasks remit, such as.

- customer satisfaction surveys,
- events
- competitions,
- retailing,
- fund raising or other campaigns.

Consent will also apply to website cookies and analytics.

The benefits of obtaining consent for these discretionary purposes means:

- we give individuals genuine choice over how we use their data;
- we ensure transparency and accountability
- we provide good customer service, putting people at the centre of the relationship,
- we build customer confidence and trust;
- we enhance our reputation through improved levels of engagement and use of new services

Even where we are not asking for consent, we will still need to provide clear and comprehensive information about how we use personal data by providing access to a Privacy Notice, in line with the ICO's privacy notices code (see [privacy notices](#)).

### [Defining Consent:](#)

Consent is defined in Article 4(11) of the GDPR as:

---

<sup>1</sup> Processing basically means anything we do with the data, including collecting it, analysing it, sharing it, storing it, amending it and deleting it

*“freely given, specific, informed and unambiguous” and that it must be given by “a clear affirmative action by the data subject”*

The ICO guidance indicates that there are 7 important elements of ‘consent’ in the GDPR:

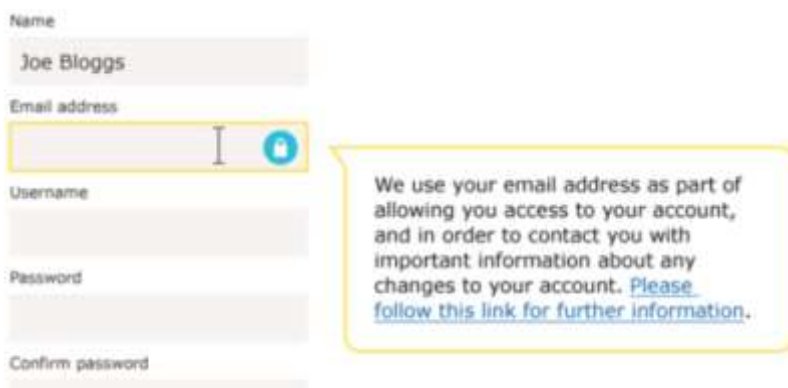
- it must be ‘unbundled’ – separate from other terms and conditions and should not be a precondition for signing up for a service unless it is necessary for that service
- it must be obtained through active ‘opt-in’ – no longer acceptable to include pre-ticked or opt-out boxes.
- include ‘granular’ consent – separate options to consent to different types of processing should be provided
- the organisation relying on consent must be ‘named’
- it must be documented – records must be kept to demonstrate what the individual has consented to, including what they were told and when and how they consented
- it must be easy to withdraw – individuals must be told that they can withdraw their consent at any time and how to do this. The process must be as easy as it was to give consent and at no cost. Records of the individual’s consent must be updated to reflect the change and to ensure that future contact is suppressed.
- There must not be an imbalance in the relationship – consent will not be ‘freely given’ where there is an imbalance between the organisation controlling the data and the individual, for example, the employer/employee relationship.

*The GDPR is particularly concerned to protect children – they may be less aware of the risks, consequences and safeguards surrounding personal data. Where consent is relied upon as a lawful basis for processing, as part of an ‘information society service’ (for example social media sites and websites aimed at children), consent will only be valid from children of at least 13 years of age.*

### Consent in practice:

Examples of simple consents:

- ticking an opt-in box on paper or electronically or clicking an opt-in button or link online, for example “*I consent to receive emails about future events/walks* ”
- ‘just-in-time’ notices. A brief message describing what the data will be used for appears on screen at the point the person inputs the relevant data.



The image shows a registration form with the following fields: Name (filled with 'Joe Bloggs'), Email address (with a cursor and a blue information icon), Username, Password, and Confirm password. A yellow callout box next to the email address field contains the following text: "We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. [Please follow this link for further information.](#)"

- selecting from equally prominent yes/no options;
- responding to an email requesting consent;
- signing a consent statement on a paper form;
- answering yes to a clear oral consent request;
- volunteering optional information for a specific purpose, for example, completing optional fields on a form (combined with just-in-time notices)

Requests for consent, where used, should be prominent, concise and easy to understand.

You must as a minimum include:

- why you want the data (the purposes of the processing);
- what you will do with the data (the processing activities); and
- confirmation that people can withdraw their consent at any time.

### **Finally, we need to:**

Regularly review our consents to check that the relationship, processing and purposes have not changed. It is not acceptable to assume that the consent lasts indefinitely. The Regulation says that consent is given 'for the time being' with a little more clarification from the Information Commissioner, adding that 'consent decays over time' Beyond this, the Regulation and guidance becomes less specific.

Consent should generally last for as long as we have a relationship with the individual and in respect of direct marketing, the recommendation is for 6 months from initial contact.