Lawful basis for processing

# Consent

ico.
Information Commissioner's Office

# Consent

## At a glance

- The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR 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 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.
- Avoid making consent to processing 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.

## Checklists

### Asking for consent

☐ We have checked that consent is the most appropriate lawful 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 consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don’t penalise individuals who wish to withdraw consent.

## In brief


- What's new?
- Why is consent important?
- When is consent appropriate?

- What is valid consent?
- How should we obtain, record and manage consent?

## What's new?

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms.

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

## Why is consent important?

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise 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 large fines.

## When is consent appropriate?

Consent is one lawful basis for processing, but 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 would still 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 the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

### What is valid consent?

Consent must be freely given; 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 we obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. 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. Consider using preference-management tools.

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

## Further Reading

Relevant provisions in the GDPR - See Articles 4(11), 6(1)(a) 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 171
External link

**In more detail - ICO guidance**

We have produced more detailed guidance on consent.

We have produced an interactive guidance tool to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

**In more detail - Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted Guidelines on consent on 10 April 2018.

About this guidance 8
What's new? 9
Why is consent important? 13
When is consent appropriate? 15
What is valid consent? 24
How should we obtain, record and manage consent? 35

# About this guidance

These pages sit alongside our Guide to the GDPR and give more detailed, practical guidance for UK organisations on consent under the GDPR.

The GDPR sets a high standard for consent. Consent means offering people genuine choice and control over how you use their data. When consent is used properly, it helps you build trust and enhance your reputation.

This guidance will help you to decide when to rely on consent for processing and when to look at alternatives. It explains what counts as valid consent, and how to obtain and manage consent in a way that complies with the GDPR.

The guidance sets out how the ICO interprets the GDPR, and our general recommended approach to compliance and good practice.

For an introduction to the key themes and provisions of the GDPR, you should refer back to the guide. You can navigate back to the Guide at any time using the link at the top of this page. Links to other relevant guidance and sources of further information are also provided throughout.

When downloading this guidance, the corresponding content from the Guide to the GDPR will also be included so you will have all the relevant information on this topic.

# What's new?

## In detail


- Is this a big change?
- What's different about the standard of consent?
- What else is new?
- What are the key changes to make in practice?
- Can we carry on using existing consents from the 1998 Act?


### Is this a big change?

The basic concept of consent, and its main role as one potential lawful basis (or condition) for processing, is not new. The definition and role of consent remains similar to that under the Data Protection Act 1998 (the 1998 Act). However, the GDPR builds on the 1998 Act standard of consent in several areas. It contains much more detail and codifies existing European guidance and good practice.

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms. You need clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw consent.

The changes reflect a more dynamic idea of consent: consent as an organic, ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away.

### What's different about the standard of consent?

The definition of consent in Article 4(11) of the GDPR is similar to the old Data Protection Directive definition, but adds some detail on how consent must be given:

| **DP Directive definition:** | **GDPR definition:** |
| --- | --- |
| "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" | "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" |

So the key elements of the consent definition remain – it must be freely given, specific, informed, and there must be an indication signifying agreement. However, the GDPR is clearer that the indication must be unambiguous and involve a clear affirmative action.

However, this definition is only the starting point for the GDPR standard of consent. Several new provisions on consent contain more detailed requirements. In particular, Article 7 sets out various conditions for consent, with specific provisions on keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent, and avoiding making consent a condition of a contract. Recitals 32, 42 and 43 also give more specific guidance on the various elements of the definition.

In essence, there is a greater emphasis in the GDPR on individuals having clear distinct ('granular') choices upfront and ongoing control over their consent.

## Further Reading

Key GDPR provisions - See Articles 4(11) and 7, and Recitals 32, 42 and 43
External link

### What else is new?

There are also specific new provisions on children's consent for online services, and consent for scientific research purposes.

Consent can also legitimise processing that has been restricted. Explicit consent can legitimise automated decision-making, including profiling.

If you rely on consent, this will also affect individuals' rights. People will generally have stronger rights when processing is based on consent – for example, the right to erasure (also known as 'the right to be forgotten') and the right to data portability.

The GDPR also brings in new accountability and transparency requirements. In particular, you must now inform people upfront about your lawful basis for processing their personal data. You need to tell people clearly what you do with their consent, and whether you do anything else on a different lawful basis. If you know you will need to retain the data after consent is withdrawn for a particular purpose under another lawful basis, you need to tell them this from the start.

## Further Reading

Key GDPR provisions - See Article 8 and Recital 38 (children), Recital 33 (scientific research) Articles 17(1)(b) and Recital 65 (right to erasure), 18(2) (right to restriction), 20(1)(a) and Recital 68 (right to data portability), and 22(2)(c) and Recital 71 (automated decision making)
External link

**Further reading**

Children and the GDPR

Right to restrict processing

Rights related to automated decision making including profiling

Right to erasure

Right to data portability

Right to be informed (transparency)

### What are the key changes to make in practice?

You need to review your consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn. The key new points are as follows:

- Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
- Active opt-in: pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (eg a binary choice given equal prominence).
- Granular: give distinct options to consent separately to different types of processing wherever appropriate.
- Named: name your organisation and any other third party controllers who will be relying on the consent. If you are relying on consent obtained by someone else, ensure that you were specifically named in the consent request – categories of third-party organisations will not be enough to give valid consent under the GDPR.
- Documented: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you need to have simple and effective withdrawal mechanisms in place.
- No imbalance in the relationship: consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis where possible.

See 'How do we obtain, record and manage consent?' and the consent checklist for more detail.

## Can we carry on using existing 1998 Act consents?

You are not required to automatically 'repaper' or refresh all existing 1998 Act consents in preparation for the GDPR. But it's important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

Recital 171 of the GDPR makes clear you can continue to rely on any existing consent that was given in line with the GDPR requirements, and there's no need to seek fresh consent. However, you need to be confident that your 1998 Act consent requests already met the GDPR standard and that consents are properly documented. You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily, and tell people they have the right to withdraw consent (if you haven't already done so).

On the other hand, if existing 1998 Act consents don't meet the GDPR's high standards or are poorly documented, you need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing, or stop the processing. If you decide to rely on a different lawful basis, you need to ensure that your continued processing is still fair and transparent. This means you need to take all reasonable steps to tell individuals that you are relying on a new lawful basis and explain what that basis is. You should also minimise their loss of control over the data by giving them the chance to opt out if possible.

Our consent checklist sets out the steps you should take to seek valid consent under the GDPR. This checklist can also help you review existing consents and decide whether they meet the GDPR standard, and to seek fresh consent if necessary.

## Further Reading

Key GDPR provisions - See Recital 171 and Articles 13 and 14
External link

**Further reading**

For more on transparency obligations, see our guidance on the Right to be informed.

# Why is consent important?

## In detail

- What role does consent play in the GDPR?
- What are the benefits of getting consent right?
- What are the penalties for getting it wrong?

### What role does consent play in the GDPR?

For processing to be lawful under the GDPR, you need to identify (and document) your lawful basis for the processing. There are six lawful bases listed in Article 6(1), and consent is one of them.

If you want to process special category (sensitive) personal data, you also need to apply one of the conditions in Article 9(2). 'Explicit consent' is one option for legitimising the use of special category data.

Consent can also legitimise restricted processing, and explicit consent can legitimise automated decision-making (including profiling), or overseas transfers by private-sector organisations in the absence of adequate safeguards.

If you rely on consent, this will affect individuals' rights. For example, they will have the right to erasure (also known as 'the right to be forgotten') and the right to data portability. Although individuals do not have the right to object where processing is based on consent, they do have the right to withdraw consent – which in effect operates as a right to stop the processing.

## Further Reading

Key GDPR provisions - See Articles 6(1)(a), 9(2)(a), Article 17(1)(b) and Recital 65 (right to erasure), Article 18(2) (right to restriction), Article 20(1)(a) and Recital 68 (for data portability), Article 21 (right to object), Article 22(2)(c) and Recital 71 (automated decision making) and Article 49(1)(a) (international transfers) and Recital 111, and Recital 50
External link

**Further reading**

Lawful basis for processing

Special category data

Right to restrict processing

Rights related to automated decision making including profiling

Right to erasure

Right to data portability

International transfers

### What are the benefits of getting consent right?

Basing your processing of personal data on GDPR-compliant consent means giving individuals genuine choice and ongoing control over how you use their data, and ensuring your organisation is transparent and accountable.

Getting this right should be seen as essential to good customer service: it will put people at the centre of the relationship, and can help build confidence and trust. This can enhance your reputation, improve levels of engagement and encourage use of new services and products. It's one way to set yourself apart from the competition.

### What are the penalties for getting it wrong?

Handling personal data badly – including relying on invalid or inappropriate consent – can erode trust in your organisation and damage your reputation. Individuals won't want to engage with you if they think they cannot trust you with their data; you do things with it that they don't understand, want or expect; or you make it difficult for them to control how it is used or shared.

It may also leave you open to substantial fines under the GDPR. Article 83(5)(a) states that infringements of the basic principles for processing personal data, including the conditions for consent, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

## Further Reading

Key GDPR provisions - See Article 83(5), and Recitals 148-152
External link

# When is consent appropriate?

## In detail


- Do we always need consent?
- When must we have consent?
- In what other circumstances might consent be appropriate?
- When is it appropriate to use consent for special category data?
- When is consent inappropriate?
- What are the alternatives to consent?


### Do we always need consent?

In short, no. Consent is one lawful basis for processing, but there are five others. Consent won't always be the most appropriate or easiest.

You must always choose the lawful basis that most closely reflects the true nature of your relationship with the individual and the purpose of the processing. If consent is difficult, this is often because another lawful basis is more appropriate, so you should consider the alternatives. See the section on 'What are the alternatives to consent?'.

Similarly, explicit consent is one way to legitimise processing special category personal data, but not the only way. Article 9(2) lists nine other conditions (supplemented by schedule 1 of the Data Protection Bill). The alternative conditions for processing special category data are generally more restrictive and tailored to specific situations, but you should still check first whether any of them apply.

## Further Reading

> Key GDPR provisions - See Articles 6(1) and 9(2)
> External link

### When must we have consent?

You are likely to need to consider consent when no other lawful basis obviously applies. For example, this may be the case if you want to use or share someone's data in a particularly unexpected or potentially intrusive way, or in a way that is incompatible with your original purpose.

If you are using special category data, you may to need to seek explicit consent to legitimise the processing, unless one of the other specific conditions in Article 9(2) applies. Note that some of the other conditions still require you to consider consent first, or to get consent for some elements of your processing. For example, if you are a not-for-profit body and you choose to rely on Article 9(2)(d), you still need explicit consent to disclose the data to any third party controllers.

You are also likely to need consent under e-privacy laws for many types of marketing calls and marketing messages, website cookies or other online tracking methods, or to install apps or other software on people's devices. These rules are currently found in the Privacy and Electronic

Communications Regulations 2003 (PECR). The EU is in the process of replacing the current e-privacy law (and therefore PECR) with a new e-privacy Regulation (ePR). However the new ePR is yet to be agreed. The existing PECR rules continue to apply until the ePR is finalised, but will apply the GDPR definition of consent.

If you need consent under e-privacy laws to send a marketing message, then in practice consent is also the appropriate lawful basis under the GDPR. If e-privacy laws don't require consent for marketing, you may be able to consider legitimate interests instead.

If you need consent to place cookies, this needs to meet the GDPR standard. However, you may still be able to consider an alternative lawful basis such as legitimate interests for any associated processing of personal data.

**Further reading**

For more about the existing e-privacy rules, please see our Guide to PECR.

For more information about marketing under the GDPR, see:

Direct marketing guidance

Legitimate interests guidance

## In what other circumstances might consent be appropriate?

Consent is likely to be the most appropriate lawful basis for processing (or the appropriate gateway through other relevant provisions) if you want to offer individuals real choice and control over how you use their data. In particular, you may want to consider using consent to improve their level of engagement with your organisation and encourage them to trust you with more useful data.

However, whether consent is appropriate and valid will always depend on the particular circumstances.

See also 'What are the benefits of getting consent right?'

## When is it appropriate to use consent for special category data?

If you want to process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9, as supplemented by Schedule 1 of the Data Protection Bill.

The first condition listed in Article 9 is 'explicit consent'. However, this does not mean it is always the best or most appropriate condition. You should always consider whether any of the other conditions better fit the particular situation.

Your choice of lawful basis under Article 6 does not necessarily dictate which Article 9 condition you have to apply. Even if you did not rely on consent as your lawful basis for processing, you can still consider 'explicit consent' as your Article 9 condition for any special category data. However, you must remember that explicit consent must meet the GDPR standard for valid consent, and can be withdrawn at any time.

See 'What is valid consent?' for more on what counts as 'explicit' consent.

If you need to process special category data to provide a service the individual has requested, the most appropriate lawful basis is likely to be 'necessary for contract'. But explicit consent may still be available as your condition for processing necessary special category data. However, you must be confident that you can demonstrate consent is still freely given – in particular, that the processing is actually necessary for the service.

**Example**

An individual signs up for a pregnancy yoga class. The instructor will be processing data concerning their health (ie the fact of their pregnancy along with any information about due dates) and therefore needs both a lawful basis and a condition for processing special category data.

As the instructor needs to process these details to provide the yoga class, the appropriate lawful basis is likely to be 'performance of a contract'.

Although the individual cannot sign up to the class without revealing information about their pregnancy, explicit consent is still likely to be the appropriate condition for processing health data. The processing is objectively necessary to provide the requested class, and the individual has a free choice whether or not to sign up to that class.

**Further reading – ICO guidance**

For our latest guidance on conditions for processing special category data, see the Special category data page of our Guide to GDPR.

**Further reading – Article 29 guidance**

WP29 Guidelines on Consent (external link) contain further examples of explicit consent for special category data where processing is necessary for a service.

## When is consent inappropriate?

It follows that if for any reason you cannot offer people a genuine choice over how you use their data, consent will not be the appropriate basis for processing. This may be the case if, for example:

- you would still process the data on a different lawful basis if consent were refused or withdrawn;
- you ask for 'consent' to the processing as a precondition of accessing your services; or
- you are in a position of power over the individual – for example, if you are a public authority or an employer processing employee data.

**You would still process the data without consent**

If you would still process the personal data on a different lawful basis even if consent were refused or withdrawn, then seeking consent from the individual is misleading and inherently unfair. It presents the individual with a false choice and only the illusion of control. You must identify the most appropriate lawful basis from the start.

**Example**

A company that provides credit cards asks its customers to give consent for their personal data to be sent to credit reference agencies for credit scoring.

However, if a customer refuses or withdraws their consent, the credit card company will still send the data to the credit reference agencies on the basis of 'legitimate interests'. So asking for consent is misleading and inappropriate – there is no real choice. The company should have relied on 'legitimate interests' from the start. To ensure fairness and transparency, the company must still tell customers this will happen, but this is very different from giving them a choice in data protection terms.

Prior to processing the personal data, you need to think carefully whether you would still need to retain any of the data for any other purpose if the individual withdraws their consent. For example, you might need to keep it to comply with a legal obligation or for audit purposes. If so, you must be clear and upfront at the start what your purpose and lawful basis is for retaining that data after consent is withdrawn.

**The 'consent' is a condition of service**

If you require someone to agree to processing as a condition of service, consent is unlikely to be the most appropriate lawful basis for the processing. In some circumstances it won't even count as valid consent.

Instead, if you believe the processing is necessary for the service, the more appropriate lawful basis is likely to be 'necessary for the performance of a contract' under Article 6(1)(b). You are only likely to need to rely on consent if required to do so under another provision, such as for some electronic marketing under PECR.

If processing of special category data is genuinely necessary to provide a service to the individual, you may still be able to rely on explicit consent as your condition for processing that special category data where no other Article 9 condition applies. See When is it appropriate to use consent for special category data?

It may be that the processing is a condition of service but is not actually necessary for that service. If so, consent is not just inappropriate as a lawful basis, but presumed to be invalid as it is not freely given. In these circumstances, you could consider whether 'legitimate interests' under Article 6(1)(f) is appropriate as your lawful basis for processing instead. You could not rely on explicit consent for any special category data in this case, and need to look for another Article 9 condition.

**Example**

A café decides to provide free wifi to its customers. In order to access the wifi the customer must provide their name, email address and mobile phone number and then agree to the café's terms and conditions.

Within the terms and conditions it states that by providing their contact details the customer is consenting to receive marketing communications from the café. The café is therefore making consent to send direct marketing a condition of accessing the service.

However collecting their customer's details for direct marketing purposes is not necessary for the provision of the wifi. This is not therefore valid consent.

See 'What is valid consent?' for more on when consent is freely given.

**You are in a position of power**

Consent will not usually be appropriate if there is a clear imbalance of power between you and the individual. This is because those who depend on your services, or fear adverse consequences, might feel they have no choice but to agree – so consent is not considered freely given. This will be a particular issue for public authorities and employers.

**Example**

A company asks its employees to consent to monitoring at work. However, as the employees rely on the company for their livelihood, they may feel compelled to consent, as they don't want to risk their job or be perceived as difficult or having something to hide.

**Example**

A housing association needs to collect information about the previous convictions of tenants and prospective tenants for risk-assessment purposes when allocating properties and providing home visits. However, it is inappropriate to ask for consent for this as a condition of the tenancy. A tenant applying for social housing may be in a vulnerable position and may not have many other housing options. So they may have no real choice but to sign up to the housing association's terms. Even if the processing is necessary to provide the accommodation, their consent is not considered freely given because of the imbalance of power.

If you are a public authority or are processing employee data, or are in any other position of power over an individual, you should look for another basis for processing, such as 'public task' or 'legitimate interests'.

However, public authorities and employers are not banned from using consent as their lawful basis. Even if you are in a position of power, there may be situations when you can still show that the consent is freely given.

**Example**

A local council runs a number of fitness centres. It wants to find out what people think of the facilities in order to decide where to focus improvements. It decides to email a questionnaire to individuals who have fitness memberships to ask them about the facilities.

The decision as to whether or not to take part in the survey is entirely optional, and given the nature of the relationship and the survey there is no real risk of adverse consequences for failing to respond. The council could consider relying on consent to process the responses.

**Example**

An employer decides to make a recruitment video for its website. It has instructed some professional actors but gives staff the opportunity to volunteer to have a role in the video. The employer makes it clear that there is no requirement for any staff to take part and participation will not be taken into account for performance evaluation purposes.

As participation is optional and there are no adverse consequences to those who do not want to take part the employer could consider consent.

However, you need to look carefully at the particular circumstances and be confident that you can demonstrate that the individual really does have a free choice to give or to refuse consent. You may need to take steps to ensure that the individual does not feel any pressure to consent and allay any concerns over the consequences of refusing consent.

**Example**

The police respond to an emergency call and deal with an individual who has been a victim of a crime. The officer advises that help is available from a support service and that they can pass the individual’s details to that service if the individual wants them to.

On the face of it there is a clear imbalance of power where an individual is dealing with a uniformed police officer. If the officer suggests that the police would like to contact the support service or that this is standard practice, the imbalance of power issue will come into play as the individual may feel that they should agree. They may also fear that their case might not get as much police attention unless they agree.

However, if the officer takes care to make sure the offer of help is neutral and optional and makes clear that it is a separate service with no effect on the police investigation, then the police may be able to demonstrate that consent is freely given.

The police must also make sure the consent is specific, informed, given by a clear affirmative

action, and properly documented. In particular they need to properly explain what data they will share with the support service, what it will be used for, and identify the organisation providing the service.

See 'What is valid consent?' for more on when consent is freely given.

**Other inappropriate uses of consent**

Be very careful about using other pre-existing concepts of consent out of context, as these may not always be appropriate for data protection purposes.

Even if you are under a separate legal or ethical requirement to get 'consent' to do something, this does not mean that you automatically have or need to have valid GDPR consent for any associated processing of personal data. In some cases, the standard of consent can be very different. It's still important to consider your lawful basis carefully.

If you are intending to rely on consent as your lawful basis, always check that the consent also meets the GDPR standard, rather than simply assuming it applies. In particular, implied consent won't often be appropriate as a lawful basis for processing under the GDPR.

**Example**

In the healthcare sector, patient data is held under a duty of confidence. Healthcare providers generally operate on the basis of implied consent to share patient data for the purposes of direct care, without breaching confidentiality.

Implied consent for direct care is industry practice in that context. But this 'implied consent' to share confidential patient records is not the same as consent to process personal data in the context of a lawful basis under the GDPR.

In the healthcare context consent is often not the appropriate lawful basis under the GPDR. This type of assumed implied consent would not meet the standard of a clear affirmative act – or qualify as explicit consent for special category data, which includes health data. Instead, healthcare providers should identify another lawful basis (such as vital interests, public task or legitimate interests). For the stricter rules on special category data, Article 9(2)(h) specifically legitimises processing for health or social care purposes.

Even if you are required to get a patient's consent to the medical treatment itself, this is entirely separate from your data protection obligations. It does not mean that you have to rely on consent for your processing of the patient's personal data.

As a general rule, whenever you have difficulty meeting the standard for consent, this is a warning sign that consent may not be the most appropriate basis for your processing. So we recommend you look for another basis.

## Further Reading

Key GDPR provisions - See Article 7(4) and Recitals 42 and 43
External link

**Further reading – ICO guidance**

For more information on selecting the most appropriate lawful basis for your processing, see the lawful basis pages of our Guide to GDPR and use our Lawful basis interactive guidance tool

**Further reading – Article 29**

WP29 Guidelines on Consent

## What are the alternatives to consent?

If you are looking for another lawful basis, these are set out in Article 6(1). In summary, you can process personal data without consent if it's necessary for:

- **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.
- **Compliance with a legal obligation**: if you are required by UK or EU law to process the data for a particular purpose, you can.
- **Vital interests**: you can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else.
- **A public task**: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.
- **Legitimate interests**: you can process personal data without consent if you need to do so for a genuine and legitimate reason (including commercial benefit), unless this is outweighed by the individual's rights and interests. Please note however that public authorities are restricted in their ability to use this basis.

Private-sector or third-sector organisations will often be able to consider the 'legitimate interests' basis in Article 6(1)(f) if they find it hard to meet the standard for consent and no other specific basis applies. This recognises that you may have good reason to process someone's personal data without their consent – but you must avoid doing anything they would not expect, ensure there is no unwarranted impact on them, and that you are still fair, transparent and accountable.

If you are a public authority and can demonstrate that the processing is to perform your official functions as set down in UK law, then the 'public task' basis is likely to be more appropriate. If not, you may still be able to consider legitimate interests or one of the other bases. As always, you need to ensure you are fair, transparent and accountable.

If you are looking for other conditions for processing special category data, these are set out in Article 9(2) (supplemented by the Data Protection Bill). These are more limited and specific, and for example they include provisions covering employment law, health and social care, and research. See our guidance on special category data for more information.

The Guide to GDPR also contains more guidance on the rules for restricted processing, automated decision-making (including profiling), and overseas transfers.

Remember that even if you are not asking for consent, you still need to provide clear and comprehensive information about how you use personal data to comply with the right to be informed.

## Further Reading

Key GDPR provisions - See Articles 6(1) and 9(2)
External link

**Further reading – ICO tool**

We have produced the lawful basis interactive guidance tool, to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

**Further reading – ICO guidance**

Lawful basis for processing

Legitimate interests

Public task

Special category data

Right to be informed

Right to restrict processing

Rights related to automated decision making including profiling

International transfers

# What is valid consent?

## In detail


- How is consent defined?
- What is 'freely given'?
- What is 'specific and informed'?
- What is an unambiguous indication (by statement or clear affirmative action)?
- What is explicit consent?
- How long does consent last?
- Can a third party give consent on an individual's behalf?
- What are the rules on capacity to consent?
- What are the rules on children's consent?
- What are the rules on consent for scientific research purposes?
- When is consent invalid?


### How is consent defined?

Consent is defined in Article 4(11) 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".

Article 7 also sets out further 'conditions' for consent, with specific provisions on:

- keeping records to demonstrate consent;
- prominence and clarity of consent requests;
- the right to withdraw consent easily and at any time; and
- freely given consent if a contract is conditional on consent.

## Further Reading

Key GDPR provisions - See Articles 4(11) and 7
External link

### What is 'freely given'?

Consent means giving people genuine choice and control over how you use their data. If the individual

has no real choice, consent is not freely given and it will be invalid.

This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible.

The GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service:

Article 7(4) says:

> “When assessing whether consent is freely given, utmost account shall be taken of whether… the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”

And Recital 43 says:

> “Consent is presumed not to be freely given… if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.”

**Example**

An online furniture store requires customers to consent to their details being shared with other homeware stores as part of the checkout process. The store is making consent a condition of sale – but sharing the data with other stores is not necessary for that sale, so consent is not freely given and is not valid. The store could ask customers to consent to passing their data to named third parties but it must allow them a free choice to opt in or out.

The store also requires customers to consent to their details being passed to a third-party courier who will deliver the goods. This is necessary to fulfil the order, so consent can be considered freely given - although ’performance of a contract’ is likely to be the more appropriate lawful basis.

In some limited circumstances you might be able to overturn this presumption that bundled consent is not freely given, and argue that consent might be valid even though it is a precondition and the processing is not strictly necessary. You need to be able to demonstrate a very clear justification for this, based on the specific circumstances.

However, this is likely to be unusual. Given the language of Article 7(4) and Recital 43, you would always be taking a risk that the consent would be considered invalid as not ‘freely given’. In general, it would be

better to rely on 'legitimate interests' as your lawful basis in such cases, combined with clear and transparent privacy information.

The GDPR is also clear that people must be able to refuse and withdraw consent without being penalised:

> "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."

The ICO's view is that it may still be possible to incentivise consent to some extent. There will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal. However, you must be careful not to cross the line and unfairly penalise those who refuse consent.

Freely given consent will also be more difficult to obtain in the context of a relationship where there is an imbalance of power – particularly for public authorities and employers. Recital 43 says:

> "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….."

See the section on when is consent appropriate for further guidance on imbalance of power.

## Further Reading

Key GDPR provisions - See Article 7(4) and Recitals 42 and 43
External link

### What is 'specific and informed'?

Consent needs to be specific and informed. This means it must specifically cover the following:

- **The controller's identity**: recital 42 says the individual should know the identity of the controller. This means you need to identify yourself, and also name any third party controllers who will be relying on the consent. If you buy in 'consented' data, that consent is only valid for your processing if you were specifically identified. You don't need to name your processors in your consent request (although you do need to comply with separate transparency obligations).

- **The purposes of the processing**: recital 43 says separate consent will be needed for different processing operations wherever appropriate – so you need to give granular options to consent separately to separate purposes, unless this would be unduly disruptive or confusing. And in every case, a consent request must specifically cover all purposes for which you seek consent.
- **The processing activities**: again, where possible you should provide granular consent options for each separate type of processing, unless those activities are clearly interdependent – but as a minimum you must specifically cover all processing activities.
- **The right to withdraw consent at any time**: we also advise you should include details of how to do so.

These rules about consent requests are separate from your transparency obligations under the right to be informed, which apply whether or not you are relying on consent.

You must clearly explain to people what they are consenting to in a way they can easily understand. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent.

Recital 32 also makes clear that electronic consent requests must not be unnecessarily disruptive to users. You need to give some thought to how best to tailor your consent requests and methods to ensure clear and comprehensive information without confusing people or disrupting the user experience – for example, by developing user-friendly layered information and just-in-time consents.

It is important to remember however that this is not an exemption and avoiding disruption does not override the need to ensure that consent requests are clear and specific. Some level of disruption may be necessary to obtain valid consent.

You need to keep your consents under review and refresh them if your purposes or activities evolve beyond what you originally specified. Consent will not be specific enough if details change – there is no such thing as 'evolving' consent.

Even if your new purpose is considered 'compatible' with your original purpose, this does not override the need for consent to be specific. If you were relying on consent you therefore need to either get fresh specific consent, or else identify a new lawful basis for the new purpose.

See 'How should you obtain, record and manage consent?' for guidance on what this means in practice.

## Further Reading

Key GDPR provisions - See Article 7(2) and (3), and Recitals 32, 42 and 43
External link

**Further reading – ICO guidance**

For more on your separate transparency obligations, see our right to be informed guidance.

## What is an unambiguous indication (by statement or clear affirmative action)?

It must be obvious that the individual has consented, and what they have consented to. This requires more than just a confirmation that they have read terms and conditions – there must be a clear signal that they agree. If there is any room for doubt, it is not valid consent.

The GDPR is clear that consent requires clear affirmative action, and Recital 32 sets out additional guidance on this:

> "Consent should be given by a clear affirmative act… 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."

Clear affirmative action means someone must take deliberate and specific action to opt in or agree to the processing, even if this is not expressed as an opt-in box. For example, other affirmative opt-in methods might include signing a consent statement, oral confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default.

The key point is that all consent must be opt-in consent, ie a positive action or indication – there is no such thing as 'opt-out consent'. Failure to opt out is not consent as it does not involve a clear affirmative act. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way. All of these methods also involve ambiguity – and for consent to be valid it must be both unambiguous and affirmative. It must be clear that the individual deliberately and actively chose to consent.

The idea of an affirmative act does still leave room for implied methods of consent in some circumstances, particularly in more informal offline situations. The key issue is that there must still be a positive action that makes it clear someone is agreeing to the use of their information for a specific and obvious purpose. However, this type of implied method of indicating consent would not extend beyond what was obvious and necessary.

**Example**

An individual drops their business card into a prize draw box in a coffee shop. This is an affirmative act that clearly indicates they agree to their name and contact number being processed for the purposes of the prize draw. However, this consent does not extend to using those details for marketing or any other purpose and you would need a different lawful basis to do so.

**Example**

An individual submits an online survey about their eating habits. By submitting the form they are clearly indicating consent to process their data for the purposes of the survey itself. Submitting the form will not, however, be enough by itself to show valid consent for any further uses of the information.

Unambiguous consent also links in with the requirement that consent must be verifiable. Article 7(1) makes it clear you must be able to demonstrate that someone has consented.

See 'How should you obtain, record and manage consent?' for guidance on what this all means in practice.

## Further Reading

Key GDPR provisions - See Recital 32
External link

### What is 'explicit consent'?

Explicit consent is not defined in the GDPR, but it is not likely to be very different from the usual high standard of consent. All consent must involve a specific, informed and unambiguous indication of the individual's wishes. The key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written).

The definition of consent says the data subject can signify agreement either by a statement (which would count as explicit consent) or by a clear affirmative action (which would not). Consent that is inferred from someone's actions cannot be explicit consent, however obvious it might be that they consent. Explicit consent must be expressly confirmed in words.

Individuals do not have to write the consent statement in their own words; you can write it for them. However you need to make sure that individuals can clearly indicate that they agree to the statement – for example by signing their name or ticking a box next to it.

If you need explicit consent, you should take extra care over the wording. Even in a written context, not all consent will be explicit. You should always use an express statement of consent.

**Example**

A beauty spa gives a form to its customers on arrival which includes the following:

Skin type and details of any skin conditions (optional):

> We will use this information to recommend appropriate beauty products.

If someone enters details of their skin conditions, this is likely to be a freely given, specific, informed and unambiguous affirmative act agreeing to use of that data to make such recommendations – but is arguably still implied consent rather than explicit consent.

Another beauty spa uses the following statement instead:

> Skin type and details of any skin conditions (optional):
>
> I consent to you using this information to recommend appropriate beauty products ☐

If the individual ticks the box, they have explicitly consented to the processing.

An explicit consent statement also needs to specifically refer to the element of the processing that requires explicit consent. For example, the statement should specify the nature of the special category data, the details of the automated decision and its effects, or the details of the data to be transferred and the risks of the transfer.

The 'explicit' element of any consent should also be separate from any other consents you are seeking, in line with the guidance in Recital 43 on appropriate granular control.

You can obtain explicit consent orally, but you need to make sure you keep a record of the script.

## Further Reading

Key GDPR provisions - See Article 4(11) and Recital 43
External link

### How long does consent last?

The GDPR does not set a specific time limit for consent. Consent is likely to degrade over time, but how long it lasts will depend on the context. You need to consider the scope of the original consent and the individual's expectations.

**Example**

A gym runs a promotion that gives members the opportunity to opt in to receiving emails with tips

about healthy eating and how to get in shape for their summer holiday that year.

As the consent request specifies a particular timescale and end point – their summer holiday – the expectation will be that these emails will cease once the summer is over. The consent will therefore expire.

If your processing operations or purposes evolve, your original consents may no longer be specific or informed enough – and you cannot infer broader consent from a simple failure to object. If this happens, you will need to seek fresh consent or identify another lawful basis.

If someone withdraws consent, you need to cease processing based on consent as soon as possible in the circumstances. This will not affect the lawfulness of your processing up to that point.

Parental consent won't automatically expire when the child reaches the age at which they can consent for themselves, but you need to bear in mind that you may need to refresh consent more regularly.

You should keep your consents under review and consider refreshing consent at appropriate user-friendly intervals. See the section on how should you manage consent? for further information.

**Further reading – ICO guidance**

Lawful basis for processing

Right to be informed

Children and the GDPR

## Can a third party give consent on an individual's behalf?

The GDPR does not prevent a third party acting on behalf of an individual to indicate their consent. However, you need to be able to demonstrate that the third party has the authority to do so.

In practice, it is likely to be difficult in most cases to verify that a third party has the authority to provide consent. You also still need to be able to demonstrate that the individual was fully informed and consent was freely given.

This is most likely to be appropriate in cases where the individual lacks the capacity to consent and someone else has specific legal authority to make decisions on their behalf.

## What are the rules on capacity to consent?

The GDPR does not contain specific provisions on capacity to consent, but issues of capacity are bound up in the concept of 'informed' consent.

Generally, you can assume that adults have the capacity to consent unless you have reason to believe the contrary. However, you should ensure that the information you provide enables your intended audience to be fully informed.

It may be that you do have reason to believe that someone lacks the capacity to understand the consequences of consenting and so cannot give informed consent. If so, a third party with the legal right

to make decisions on their behalf (eg under a Power of Attorney) can give consent.

### What are the rules on children's consent?

There are no global rules on children's consent under the GDPR, but there is a specific provision in Article 8 on children's consent for 'information society services' (services requested and delivered over the internet).

In short, if you offer these types of services directly to children (other than preventive or counselling services) and you want to rely on consent rather than another lawful basis for your processing, you must get parental consent for children under 13 (which is the age set by the UK in the Data Protection Bill).

If you choose to rely on children's consent, you will need to implement age-verification measures, and make 'reasonable efforts' to verify parental responsibility for those under the relevant age.

For other types of processing, the general rule in the UK is that you should consider whether the individual child has the competence to understand and consent for themselves (the 'Gillick competence test'). In practice, you may still need to consider age-verification measures as part of this assessment, and take steps to verify parental consent for children without competence to consent for themselves.

Consent is one possible lawful basis for processing children's data, but remember that it is not the only option. Sometimes another lawful basis is more appropriate and provides better protection for the child. For example, you may find it beneficial to consider 'legitimate interests' as a potential lawful basis instead of consent. This will help ensure you assess the impact of your processing on children and consider whether it is fair and proportionate.

## Further Reading

Key GDPR provisions - See Article 8 and Recital 38
External link

**Further reading – ICO guidance**

Children and the GDPR

Legitimate interests

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted Guidelines on consent on 10 April 2018.

### What are the rules on consent for scientific research purposes?

There is no rule that says you have to rely on consent to process personal data for scientific research purposes.

Even if you have a separate ethical or legal obligation to get consent from people participating in your research, this should not be confused with GDPR consent.

**Example**

The Clinical Trials Regulations apply to clinical trials on a medical product intended for human use. This includes a requirement to obtain 'informed consent' from individuals to participate in the trial.

The GDPR does not alter this requirement. Recital 161 acknowledges that it still applies, but it is an entirely separate requirement about consent to participate in the trial. It should not be confused with consent to process personal data under the GDPR, and it does not override the obligation under Article 6 of the GDPR to identify an appropriate lawful basis.

As a separate exercise, you must also ensure that you have a lawful basis for your processing under the GDPR, as well as a condition for the processing of special category data where necessary (eg clinical trials are highly likely to involve the processing of health data). Even if individuals have consented to participate in the research, you may well find that a different lawful basis (and a different special category data condition) is more appropriate in the circumstances.

In particular, remember that consent under the GDPR can be withdrawn at any time. There is no exemption to this for scientific research. This means that if you are relying on consent as your lawful basis and the individual withdraws their consent, you need to stop processing their personal data - or anonymise it - straight away.

If you would not be able to fully action a withdrawal of consent – for example because deleting data would undermine the research and full anonymisation is not possible – then you should not use consent as your lawful basis (or condition for processing special category data). Consent is only valid if the individual is able to withdraw it at any time.

Please see the section on 'how should you manage the right to withdraw consent?' for further information.

If you do want to rely on consent, the GDPR acknowledges that if you are collecting personal data for scientific research, you may not be able to fully specify your precise purposes in advance.

If you are seeking consent to process personal data for scientific research, this means you don't need to be as specific as for other purposes. However, you should identify the general areas of research, and where possible give people granular options to consent only to certain areas of research or parts of research projects.

## Further Reading

Key GDPR provisions - See Recital 33 and 161
External link

**Further reading – ICO guidance**

For more help on choosing the most appropriate lawful basis for your processing, see the lawful basis pages of our Guide to GDPR, and our lawful basis interactive guidance tool.

Our latest guidance on the conditions for processing special category data is available on the special category data page of our Guide.

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted Guidelines on consent (external link) on 10 April 2018.

## When is consent invalid?

In summary, you do not have valid consent if any of the following apply:

- you have any doubts over whether someone has consented;
- the individual doesn't realise they have consented;
- you don't have clear records to demonstrate they consented;
- there was no genuine free choice over whether to opt in;
- the individual would be penalised for refusing consent;
- there is a clear imbalance of power between you and the individual;
- consent was a precondition of a service, but the processing is not necessary for that service;
- the consent was bundled up with other terms and conditions;
- the consent request was vague or unclear;
- you use pre-ticked opt-in boxes or other methods of default consent;
- your organisation was not specifically named;
- you did not tell people about their right to withdraw consent;
- people cannot easily withdraw consent; or
- your purposes or activities have evolved beyond the original consent.

# How should we obtain, record and manage consent?

## In detail


- How should we write a consent request?
- What information should a consent request include?
- What methods can we use to indicate consent?
- How should we record consent?
- How should we manage consent?
- How should we manage the right to withdraw consent?


### How should we write a consent request?

Consent requests need to be prominent, concise, easy to understand and separate from any other information such as general terms and conditions.

Article 7(2) says:

> "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding."

You should:

- keep your consent request separate from your general terms and conditions, and clearly direct people's attention to it;
- use clear, straightforward language;
- adopt a simple style that your intended audience will find easy to understand – this is particularly important if you are asking children to consent, in which case you may want to prompt parental input and you should also consider age-verification and parental-authorisation issues;
- avoid technical or legal jargon and confusing terminology (eg double negatives);
- use consistent language and methods across multiple consent options; and
- keep your consent requests concise and specific, and avoid vague or blanket wording.

## Further Reading

Key GDPR provisions - See Article 7(2) and Recital 42
External link

**Further reading – ICO guidance**

Children and the GDPR

### What information should a consent request include?

Consent must be specific and informed. You must as a minimum include:

- the name of your organisation and the names of any other controllers who will rely on the consent – consent for categories of third-party controllers will not be specific enough;
- why you want the data (the purposes of the processing);
- what you will do with the data (the processing activities); and
- that people can withdraw their consent at any time. It is good practice to tell them how to withdraw consent.

This is separate from the transparency requirements of the right to be informed. You must also make sure you give individuals sufficient privacy information to comply with their right to be informed, but you don't have to do this all in the consent request and there is more scope for a layered approach.

There is a tension between ensuring that consent is specific enough and making it concise and easy to understand. In practice this means you may not be able to get blanket consent for a large number of controllers, purposes or processes. This is because you won't be able to provide prominent, concise and readable information that is also specific and granular enough.

If you do need to include a lot of information, take care to ensure it's still prominent and easy to read.

You may need to consider whether you have another lawful basis for any of the processing, so that you can focus your consent request. If you use another basis, you will still need to provide clear and comprehensive privacy information, but – as noted above - this is different from a consent request and there is more scope for a layered approach.

You could also consider using 'just-in-time' notices. These work by appearing on-screen at the point the person inputs the relevant data, with a brief message about what the data will be used for. This will help you provide more information in a prominent, clear and specific way to ensure that consent is informed. However, you will need to combine the notices with an active opt-in and ensure this is not unduly disruptive to the user. There's more on methods of consent below.

See 'What is valid consent?' for more on the requirement for consent to be specific and informed.

## Further Reading

Key GDPR provisions - See Article 7(2) and (3), and Recital 42
External link

**Further reading – ICO guidance**

For more guidance on a layered approach to transparency, and the use of just-in-time notices, see our Right to be informed guidance.

## What methods can we use to obtain consent?

Whatever method you use must meet the standard of an unambiguous indication by clear affirmative action. This means you must ask people to actively opt in. Examples of active opt-in mechanisms include:

- signing a consent statement on a paper form;
- ticking an opt-in box on paper or electronically;
- clicking an opt-in button or link online;
- selecting from equally prominent yes/no options;
- choosing technical settings or preference dashboard settings;
- responding to an email requesting consent;
- answering yes to a clear oral consent request;
- volunteering optional information for a specific purpose – eg filling optional fields in a form (combined with just-in-time notices) or dropping a business card into a box.

If you need explicit consent, the opt-in needs to involve an express statement confirming consent. See 'What is explicit consent?' for more information.

You cannot rely on silence, inactivity, pre-ticked boxes, opt-out boxes, default settings or a blanket acceptance of your terms and conditions.

The GDPR does not specifically ban opt-out boxes but they are essentially the same as pre-ticked boxes, which are banned. Both methods bundle up consent with other matters by default, and then rely to some extent on inactivity. They also increase the likelihood of confusion and ambiguity.

The usual reason for using opt-out boxes is to get more people to consent by taking advantage of inaction – but this is a clear warning sign of a problem with the quality of the consent. You should instead use specific opt-in boxes (or another active opt-in method) to obtain consent.

**Example**

If you don't want us to share your response with ABC company please tick here ☐

If you would like us to share your response with ABC company please tick here ☐

If you want consent for various different purposes or types of processing, you should provide a separate opt-in for each unless you are confident it is appropriate to bundle them together. People should not be forced to agree to all or nothing – they may want to consent to some things but not to others.

If you are asking for consent electronically, consent must be "not unnecessarily disruptive to the use of the service for which it is provided". You need to ensure you adopt the most user-friendly method you can. If your processing has a minimal privacy impact and is widely understood, you may be able to justify a less prominent or granular approach, or a greater reliance on technical settings. But you must still always ensure people have genuine choice and control, and take some positive action. Disruption is not an excuse for invalid consent.

If you need to obtain an individual's consent online, you don't need to force people to create user accounts and sign in just so you can obtain verifiable consent. But you can of course offer this as an option, in case people want to save their preferences. Article 11 makes it clear that you don't have to get additional information to identify the individual in order to comply.

Instead, you could for example link the consent to a temporary session ID. Clearly, after the session ends and the link between the individual and the session is destroyed, you will need to seek fresh consent each time the individual returns to your website.

If you are offering online services to children and want to rely on consent for your processing, you need to adopt age-verification measures and seek parental consent for children under 13. See What are the rules on children's consent?

See 'What is valid consent?' for more on what the GDPR says about unambiguous indications of consent by clear affirmative action.

## Further Reading

Key GDPR provisions - See Article 4(11) and Recitals 32 and 43 and Article 11 (for processing that does not require identification)

External link

**Further reading – ICO guidance**

Right to be informed

### How should we record consent?

Article 7(1) says:

> "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."

This means you must have an effective audit trail of how and when consent was given, so you can

provide evidence if challenged. You should keep this evidence for as long as you are still processing based on the consent, so that you can demonstrate your compliance in line with accountability obligations.

Good records will also help you to monitor and refresh consent as appropriate. You must keep good records that demonstrate the following:

- **Who consented:** the name of the individual, or other identifier (eg, online user name, session ID).
- **When they consented:** a copy of a dated document, or online records that include a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation.
- **What they were told at the time**: a master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy or other privacy information, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time.
- **How they consented:** for written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation - it doesn't need to be a full record of the conversation.
- **Whether they have withdrawn consent:** and if so, when.

**Example**

You keep a spreadsheet with 'consent provided' written against a customer's name.

You keep a copy of the customer's signed and dated form that shows they ticked to provide their consent to the specific processing.

**Example**

You keep the time and date of consent linked to an IP address, with a web link to your current data-capture form and privacy policy.

You keep records that include an ID and the data submitted online together with a timestamp. You also keep a copy of the version of the data-capture form and any other relevant documents in use at that date.

**Example**

You put a tick next to a customer's name to indicate that they told you verbally that they consent.

You keep records that include the time and date of the conversation, the name and date/version of the script used.

Consent should be specific and granular, so your records also need to be specific and granular to demonstrate exactly what the consent covers.

For online consent, you may be able to use an appropriate cryptographic hash function to support data integrity.

## Further Reading

Key GDPR provisions - See Article 7(1) and Recital 42
External link

### How should we manage consent?

Your obligations don't end when you get consent. You should view consent as a dynamic part of your ongoing relationship of trust with individuals, not a one-off compliance box to tick and file away. To reap the benefits of consent, you need to offer ongoing choice and control.

It is good practice to provide preference-management tools like privacy dashboards to allow people to easily access and update their consent settings.

If you don't offer a privacy dashboard, you need to provide other easy ways for people to withdraw consent at any time they choose. See 'How should you manage the right to withdraw consent?'

You should keep your consents under review. You will need to refresh them if anything changes – for example, if your processing operations or purposes evolve, the original consent may not be specific or informed enough. If you rely on parental consent, bear in mind that you may need to refresh consent more regularly as the children grow up and can consent for themselves. If you are in any doubt about whether the consent is still valid, you should refresh it. See 'How long does consent last?' for more on this.

You should also consider whether to automatically refresh consent at appropriate intervals. How often it's appropriate to do so will depend on the particular context, including people's expectations, whether you are in regular contact, and how disruptive repeated consent requests would be to the individual. If in doubt, we recommend you consider refreshing consent every two years – but you may be able to justify a longer period, or need to refresh more regularly to ensure good levels of trust and engagement.

If you are not in regular contact with individuals, you could also consider sending occasional reminders of their right to withdraw consent and how to do so.

**Further reading – ICO guidance**

For more on preference-management tools, see our guidance on the Right to be informed.

## How should we manage the right to withdraw consent?

The GDPR gives people a specific right to withdraw their consent. You need to ensure that you put proper withdrawal procedures in place.

Article 7(3) says:

> "The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

As the right to withdraw is 'at any time', it's not enough to provide an opt-out only by reply. The individual must be able to opt out at any time they choose, on their own initiative.

It must also be as easy to withdraw consent as it was to give it. This means the process of withdrawing consent should be an easily accessible one-step process. If possible, individuals should be able to withdraw their consent using the same method as when they gave it.

**Example**

An individual gives their consent using Company A's online form. At a later date they decide they wish to withdraw their consent. Company A provides a phone number for withdrawing consent.

An individual gives their consent using Company B's online form. At a later date they decide they wish to withdraw their consent. Company B provides an online form for withdrawing consent, available from an opt-out link at the bottom of every page.

**Example**

Company C gets consent over the phone. The individual decides at a later date they wish to withdraw their consent. Company C provides a postal address for the individual to use to withdraw their consent.

Company D also gets consent over the phone. The individual decides at a later date they wish to withdraw their consent. Company D provides a phone number for anyone wishing to withdraw their consent.

It is good practice to publicise both online preference-management tools and other ways of opting out, such as customer-service phone numbers. You should bear in mind that not everyone is confident with technology or has easy access to the internet. If someone originally gave consent on paper or in person, it may not be enough to offer only an online opt-out.

It is also good practice to provide both anytime opt-out mechanisms, such as privacy dashboards, and opt-out by reply to every contact. This could include an unsubscribe link in an email, or an opt-out phone number, address or web link printed in a letter.

The GDPR does not prevent a third party acting on behalf of an individual to withdraw their consent, but you need to be satisfied that the third party has the authority to do so. This leaves the door open for sectoral opt-out registers or other broader shared opt-out mechanisms, which could help individuals regain control they might feel they have lost. It might also help to demonstrate that consent is as easy to withdraw as it was to give.

**Example**

The Fundraising Regulator has set up the Fundraising Preference Service (FPS). The FPS operates as a mechanism to withdraw consent to charity fundraising. If an individual wishes to stop receiving marketing from particular charities, they can use the FPS to withdraw consent from those specific charities.

Individuals must be able to withdraw their consent to processing without suffering any detriment. If there is a penalty for withdrawing consent, the consent would be invalid as it would not be freely given. See 'When is consent valid?' for more on freely given consent.

If someone withdraws their consent, *this does not affect* the lawfulness of the processing up to that point. However, it does mean you can no longer rely on consent as your lawful basis for processing. You will need to stop any processing that was based on consent. You are not be able to swap to a different lawful basis for this processing (although you may be able to retain the data for a different purpose under another lawful basis if it is fair to do so – and you should have made this clear from the start). Even if you could originally have relied on a different lawful basis, once you choose to rely on consent you are handing control to the individual. It is inherently unfair to tell people they have a choice, but then continue the processing after they withdraw their consent.

If someone withdraws consent, you should stop the processing as soon as possible. In some cases it will be possible to stop immediately, particularly in an online automated environment. However, in other

cases you may be able to justify a short delay while you process the withdrawal.

Withdrawals of consent also apply to special category data where explicit consent is being used. Therefore if you are using explicit consent as your Article 9 condition and the individual withdraws their consent you can no longer use this as your condition. However, unlike Article 6, it could be possible for you to use a different Article 9 condition instead but you still need to ensure that this is communicated to the individual and is fair.

You must include details of the right to withdraw consent in your privacy information and consent requests. It is good practice to also include details of how to withdraw consent.

In some cases you may need to keep a record of the withdrawal of consent for your own purposes – for example, to maintain suppression records so that you can comply with direct marketing rules. You don't need consent for this, as long as you tell individuals that you will keep these records, why you need them, and your lawful basis for this processing (eg legal obligation or legitimate interests).

## Further Reading

Key GDPR provisions - See Articles 7(3), Articles 13(2)(c) and 14(2)(d) (for the right to be informed), and Recital 42
External link