Information Commissioner's Office

Consultation:

GDPR consent guidance

Start date: 2 March 2017
End date: 31 March 2017

ICO GDPR guidance:
Consent

Contents (for web navigation bar)

At a glance

- The GDPR sets a high standard for consent.
- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh consents if they don't meet the GDPR standard.
- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- 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. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third parties 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 a precondition of a service.
- Public authorities and employers will find using consent difficult.
- Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

About this guidance

These pages sit alongside our Overview of 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.

However, as the GDPR is a Regulation that applies consistently across the EU, our guidance will need to evolve to take account of future guidelines issued by relevant European authorities, as well as our experience of applying the law in practice from May 2018. We intend to keep this guidance under review and update it in light of relevant developments and stakeholders' feedback.

You can navigate back to the Overview at any time using the link on the left-hand side of this page. We also give links throughout to other relevant guidance and sources of further information.

Key GDPR provisions
See Articles 4(11), 6(1)(a), 7, 8, 9(2)(a), 13(2)(c), 14(2)(d), 49(1)(a) and Recitals 32, 33, 38, 42, 43, 54, 65, 111, 155, 161, 171 (external link)

Further reading
Article 29 Working Party Opinion 15/2011 on the definition of consent (WP187) (external link)

This opinion gives detailed guidance on the key elements of consent under the Data Protection Directive along with recommendations for change – much of this was then codified in the GDPR.

What's new?

In brief…

- 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.
- Consent should be separate from other terms and conditions. It should not generally be a precondition of signing up to a service.
- The GDPR specifically bans pre-ticked opt-in boxes.
- It requires granular consent for distinct processing operations.
- 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 are likely to find it more difficult to get valid 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.

In more detail…

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 (DPA). However, the GDPR builds on the DPA 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 will 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 should 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 granular choices upfront and ongoing control over their consent.

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.

Key GDPR provisions
See Article 8, and Recitals 33 and 38 (external link)

Consent can also legitimise restricted processing. 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.

Key GDPR provisions
See Articles 17(1)(b), 18(2), 20(1)(a), and 22(2)(c), and Recitals 65, 68, and 71 (external link)

What are the key changes to make in practice?

You will 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 granular options to consent separately to different types of processing wherever appropriate.
- **Named**: name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable 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 will 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.

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

Can we carry on using existing DPA consents?

You are not required to automatically 'repaper' or refresh all existing DPA 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 will need to be confident that your 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.

On the other hand, if existing DPA consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

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.

Key GDPR provisions
See Recital 171 (external link)

Why is consent important?

In brief…

- Consent is one lawful basis for processing, and consent (or explicit consent) can also legitimise use of special category data, restricted processing, automated decision-making or overseas transfers.
- Doing consent well should put individuals in control, build customer 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 substantial fines.

In more detail…

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. 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.

Key GDPR provisions
See Articles 6(1)(a), 9(2)(a), 17(1)(b), 18(2), 20(1)(a), 22(2)(c) and

49(1)(a), and Recitals 50, 65, 68, 71 and 111 (external link)

What are the benefits of getting consent right?

Basing your processing of customer 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 customer 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.

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

When is consent appropriate?

In brief…

- Consent is one lawful basis for processing, but there are alternatives. If consent is difficult, you should consider using an alternative basis.
- 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, consent 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.

In more detail…

Do you always need consent?

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

You should 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 'What are the alternatives to consent?' (link).

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 and there is some scope for UK legislation to add more. The alternative conditions for processing special category data are generally more restrictive and tailored to specific situations, but it's worth checking first whether any of them apply.

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

When must you have consent?

You need consent when no other lawful basis 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 are more likely to need to seek explicit consent to legitimise the processing, unless one of the other specific conditions in Article 9(2) applies. If you are a not-for-profit body relying on Article 9(2)(d) instead, you will still need explicit consent to disclose the data to any third parties.

You are also likely to need consent under ePrivacy laws for most marketing calls or 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), but there is a proposal for a new updated ePrivacy Regulation to come into force at the same time as the GDPR. The Regulation has not yet been finalised so this guidance does not consider these issues further.

Further reading
For more about the existing ePrivacy rules, please see our Guide to PECR.

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 your customers 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.

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

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 should 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 should still tell customers this will happen, but this is very different from giving them a choice.

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 better lawful basis for processing is more likely to be that the "processing

is 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 electronic marketing.

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 would usually need to consider 'legitimate interests' under Article 6(1)(f) as your lawful basis for processing instead.

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 is likely to be in a vulnerable position and is unlikely to 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 'performance of a public task' if you are a public authority, or 'legitimate interests' if not.

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. Always check that the consent also meets the GDPR standard, rather than simply assuming it applies. In particular, implied consent won't always 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 use patient data for the purposes of direct care, without breaching confidentiality.

Implied consent for direct care is industry practice in that context. But consent is 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. For the stricter rules on special category data, Article 9(2)(h) specifically legitimises processing for health or social care purposes.

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.

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

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**: if you are a private-sector organisation, you can process personal data without consent if you have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests.

Private-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 ensure there is no unwarranted impact on them, and that you are still fair, transparent and accountable.

Public bodies cannot generally rely on 'legitimate interests' under the GDPR, but should be able to consider the 'public task' basis in Article 6(1)(e) instead. However, you will need to be able to justify why the processing is necessary to carry out your functions – in essence, that it is proportionate and there is no less intrusive alternative. And, as always, you will need to ensure you are fair, transparent and accountable. Note that this basis cannot apply if you are acting for purposes other than your official functions – for example, if you are a hybrid body. In such circumstances you could still consider 'legitimate interests' as a potential basis, as long as the processing is otherwise lawful.

If you are looking for another basis for processing special category data, these are set out in Article 9(2). They are more limited and specific, and for example they include provisions covering employment law, health and social care, and research – see our Overview of the GDPR for the full list.

The Overview 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 will still need to provide clear and comprehensive information about how you use personal data, in line with our privacy notices code.

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

Further reading – ICO guidance
Privacy notices, transparency and control

What is valid consent?

In brief…

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.
- Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.
- Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
- Consent should be obvious and require a positive action to opt in.
- 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.

In more detail…

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.

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

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 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. The store may ask customers to consent to passing their data to named third parties – but 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 it still not be the most appropriate lawful basis.

In some limited circumstances you might be able to overturn this presumption and argue that consent might be valid even though it is a precondition and the processing is not strictly necessary, but this would be unusual. You might, for example, be able to argue that consent should still be considered freely given if:

- there is a legitimate reason for the processing that is consistent with the underlying purpose of the service on offer;
- it is reasonable for it to be bundled with the service;
- there is a minimal privacy impact;
- consent is clearly specific, informed and unambiguous;
- you would stop the processing altogether if the individual withdrew their consent; and
- there is no alternative to consent.

However, 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 a clear and transparent privacy notice.

The GDPR is also clear that people must be able to opt out without being penalised:

Recital 42 says:

"*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.*"

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 very 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…..*"

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

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

Specific and informed

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

- **The controller's identity**: you must identify yourself, and also name any third parties who will be relying on consent.

- **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. As a minimum, consent must specifically cover all purposes.

- **The processing activities**: again, where possible you should provide granular consent options for each 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.

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 will 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.

You will 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.

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

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

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 action to opt in, 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 – there is no such thing as 'opt-out consent'. Failure to opt out is not consent. 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.

The idea of an affirmative act does still leave room for implied consent in some circumstances, particularly in more informal offline situations. The key issue is that there must 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 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 would not extend to using those details for marketing or any other purpose.

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 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.

Key GDPR provisions
See Recital 32 (external link)

What is 'explicit consent'?

Explicit consent is not defined in the GDPR, but 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). Implied consent which 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.

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

Company A provides the following information to individuals:

"Email address (optional): [ ]

"We will use this to send you emails about our products and special offers."

If someone enters their email address, this is likely to be specific, informed and an unambiguous affirmative act agreeing to such emails – but is arguably still implied rather than explicit consent.

Company B uses the following statement instead:

I consent to receive emails about your products and special offers ☐

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

An explicit consent statement will also need 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.

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 will 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 will need to cease processing as soon as possible in the circumstances unless you have another lawful basis. This will not affect the lawfulness of your processing up to that point.

Parental consent will always expire when the child reaches the age at which they can consent for themselves. You need therefore to review and refresh children's consent at appropriate milestones.

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

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 16 – although the UK may choose to lower this, to a minimum age of 13.

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.

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.

We'll be developing further specific guidance on children's privacy. It will include more detail on identifying an appropriate lawful basis for processing children's data, and issues around age verification and parental authorisation.

Key GDPR provisions
See Article 8 and Recital 38 (external link)

What are the rules on consent for scientific research purposes?

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, 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.

Key GDPR provisions
See Recital 33 (external link)

When is consent invalid?

In summary, you will not have valid consent if:

- 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.

How should you obtain, record and manage consent?

In brief…

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include the name of your organisation and any third parties, why you want the data, what you will do with it, and the right to withdraw consent at any time.
- You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.
- Wherever possible, give granular options to consent separately 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.

In more detail…

How should you 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.

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

Further reading – ICO guidance
Privacy notices, transparency and control

What information should you include?

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

- the name of your organisation and the names of any third parties who will rely on the consent – consent for categories of third-party organisations 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.

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 parties, 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 a clear and comprehensive privacy notice but 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.

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

Further reading – ICO guidance
Privacy notices, transparency and control – for more guidance on a layered approach to transparency, and the use of just-in-time notices.

What methods can you 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 on inactivity. 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.

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 will 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.

If you need to obtain a user'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 user and the session is destroyed, you will need to seek fresh consent each time the user 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 16 (or the age specified in UK law). 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.

Key GDPR provisions
See Article 4(11) and Recitals 32 and 43 (external link)

Further reading – ICO guidance
Privacy notices, transparency and control

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

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, 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' 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.

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

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

How should you 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. Our Privacy notices Code says more about using these tools.

If you don't offer a privacy dashboard, you will 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, you will also need to refresh consent 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.

How should you manage the right to withdraw consent?

The GDPR gives people a specific right to withdraw their consent. You will 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 a company's online form. At a later date they decide they wish to withdraw their consent. The company provides an online form for withdrawing consent, available from an opt-out link at the bottom of every page.

Another company gets consent over the phone. They should provide a phone number for anyone wishing to withdraw 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 will 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 sector-wide withdrawal of consent to charity fundraising. If an individual wishes to stop receiving marketing from charities, they can use the FPS to withdraw consent from all charities at once.

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 either need to stop the processing or identify another lawful basis and be able to justify why continued processing is fair.

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.

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

Key GDPR provisions

See Articles 7(3), 13(2)(c) and 14(2)(d), and Recital 42 (external link)

Checklist

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 consent by default.
- ☐ 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 granular options to consent to independent processing operations.
- ☐ We have named our organisation and any third parties.
- ☐ We tell individuals they can withdraw their consent.
- ☐ We ensure that the individual can refuse to consent without detriment.
- ☐ We don't make consent a precondition of a service.
- ☐ If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures 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.