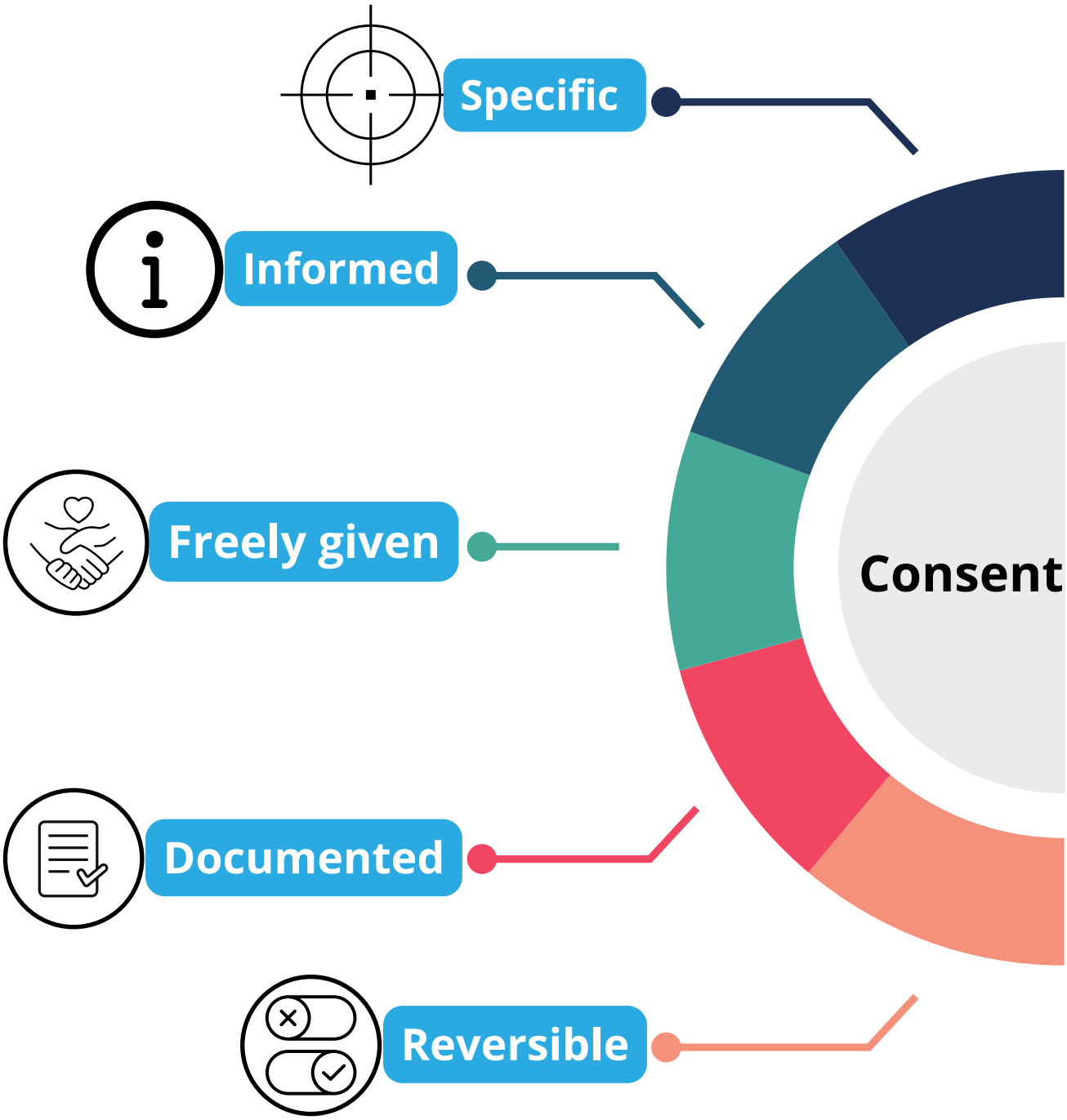
THE OFFICE OF THE
Data Protection
Authority

GUIDANCE: Consent



2024 issue

Consent

Overview

This guidance is for anyone who works with information about people who wants to understand how to use the 'lawful processing condition' known as 'consent' properly.

Consent, in data protection terms, is the act of someone choosing to give you their permission to do something specific with their personal data. It is one of several conditions in *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('the Law') that you can rely on to use someone's information, and it is known as a 'lawful processing condition'. There are many other conditions[1] you can use, and consent is only appropriate in circumstances where you are giving people genuine choice over what you are doing with their information.

The basics of getting consent right

- The Law sets a high standard for consent and it is important that you understand these requirements. Remember, consent is one of a number of conditions and it may be that another of those conditions is more appropriate for your particular processing.
- Consent means offering individuals genuine choice and control. Genuine consent puts individuals in charge, builds customer trust and engagement, and enhances your reputation.
- Check your consent practices and your existing consents. Update your consents if they do not meet the Law's standard – you can do this by using the checklists at the end of this guidance document.
- Consent requires a positive opt-in. Do not use pre-ticked boxes or any other method of default consent.
- 'Explicit consent' requires the person whose information it is to give you a very clear and specific statement of consent.
- Consent requests must be separate from other terms and conditions or other matters – you cannot 'bundle' them together.
- 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.

[1] See here for a full list of lawful processing conditions: https://www.odpa.gg/information-hub/guidance/lawful-processing-conditions.

- Keep evidence of consent – who, when, how and what you told people.
- Keep consent under review and update it if anything changes.
- Avoid making consent to processing a precondition of a service – unless you are genuinely going to stop using someone's data if they withdraw their consent.
- Public authorities and employers need to take extra care to show that consent is 'freely given' and should avoid over-reliance on consent.
- Consent will not be considered as freely given if the data subject (i.e. the person you are asking for consent from) has been deceived or misled by whomever is seeking the consent.
- Consent to the processing of criminal data is strictly controlled[2].

What does the Law require?

The Law sets a high standard for consent and you need to understand what this means in practice for your consent mechanisms.

The Law is clear that an indication of consent must be **unambiguous** and involve a clear affirmative action (an opt-in). You must not use **pre-ticked** opt-in boxes. It also requires **individual** ('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 has been given.

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

Individuals should also not be disadvantaged by withdrawing or refusing consent (for example, you should not offer better payment terms if the person consents to being added to a mailing list).

Public authorities, employers and other organisations in a position of power, and where there may be an imbalance of that power in relation to the person being asked for their consent (this person is called the 'data subject' under the Law), may find it more difficult to show valid freely given consent.

Consent for processing criminal data is only valid if the processing is required or authorised by a law. An example of such a law would be the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 (as amended).

[2] See Section 10(7) of *The Data Protection (Bailiwick of Guernsey) Law, 2017* for details.

You should review existing consents and your consent mechanisms to check they meet the Law's standard (see the checklists at the end of this guidance document). If they do, there is no need to obtain 'fresh' consent. However, if you are relying on consent you gathered **prior to the Law's commencement** (on 25 May 2018) and after having gone through the checklists you think it does not meet the Law's higher standard you will need to take action: either seeking fresh consent from the person or determining an alternative, more appropriate lawful basis for processing[3]. A word of caution here: if you are 'switching' from consent in this way you need to take great care to ensure the person knows about this switch. You will need to handle this appropriately as, depending on the circumstances and your relationship with the person, you may be reducing their control over how their information is used which they may not welcome.

Why is consent important?

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

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

When is consent appropriate?

Consent is one lawful basis for processing, but there are several alternatives. Consent is not inherently better or more important than these alternatives. You should carefully consider which condition is most appropriate for you to rely on.

Consent is only 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 use a person's data without their consent, asking for consent is misleading and inherently unfair, so you should tell people which lawful processing condition you are using instead. An example to illustrate this point: A family are in touch with social services due to their child's non-attendance at school. There is no need for the family members or the child to consent to social services making, storing or sharing information about them as social services can legitimately rely on other lawful processing conditions (such as 'health/social care' or 'public function'). However, whilst they do not need to ask for the family's *permission* to use information about them, they do need to ensure that the family *understands* how their information is being used and on what basis (see data processing notice guidance).

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis and could be deemed as not freely given.

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.

[3] See here for a full list of lawful processing conditions: https://www.odpa.gg/information-hub/guidance/lawful-processing-conditions.

What is valid consent?

Consent must be freely given; this means giving people genuine, ongoing choice and control over how you use their data.

The provision of 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,
- user-friendly and
- age appropriate.

Consent must specifically cover the controller's[4] name, the purposes of the processing and the types of processing activity.

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

The Law does not set a time limit for when consent 'expires'. How long it lasts will depend on the context, and your retention policy periods. It is up to you to ensure you review and refresh consent as appropriate given the circumstances you are working in. Remember that if an individual withdraws their consent for a particular matter you must immediately stop using their data in that specific way, but you could carry on using any other data you have where a different lawful processing condition applies.

An example of this could be: a health insurance provider relies on 'contract' to use information about a person's health in order to service their health insurance policy. The health insurer could legitimately ask the person to consent to receiving direct marketing emails about unrelated insurance products they offer. The person may consent to receiving these marketing emails initially and then grow tired of them and withdraw their consent by unsubscribing. The insurance provider is still able to email them about anything related to the service of their insurance policy but they do have to stop the unrelated direct marketing. This example also illustrates the benefit of not bundling consent into your general terms and conditions, as you are limiting yourself needlessly.

Other times the Law refers to consent

Consent is used in the Law not only as a lawful processing condition but in other contexts too. These include automated decision making, international transfers and data subject rights. When used in these other contexts, it is expected that consent will meet the same high standards as when used as a lawful processing condition.

[4] A 'Controller' is any entity* who is responsible for the decisions made about why and how they use personal data about staff, customers, suppliers, or any other people. * *this entity would normally be an organisation, but it could be a specific human being (e.g. sole traders, landlords, elected officials etc).*

How should you obtain, record and manage consent?

You should make any consent requests prominent, concise, separate from other terms and conditions, easy to understand and age appropriate. 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
- a reminder that individuals can withdraw consent at any time and how to do so.

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

Keep records so you can 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 routine business processes.

Need further help?

If you need further clarity on anything please contact us.

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 or other matters.

☐ We ask people to positively opt in.

☐ We do not use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand and appropriate for the person we are asking for consent from.

☐ We are clear why we want the data and what we are going to do with it.

☐ We give individual ('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 and explain how they can do it.

☐ 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 children under 13 years of age) 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 review and refresh consent at appropriate intervals.
- ☐ 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 promptly on requests to withdraw consent.
- ☐ We do not penalise individuals who wish to withdraw consent.