Consent in Data Processing

Introduction

Consent is one of the six lawful bases for data processing under the *General Data Protection Regulation* (GDPR). But from 25 May 2018, the GDPR will set higher standards for obtaining and using consent than has previously been required.

This means that to be lawful, consent must be given by clear affirmative action for each separate processing operation. Generic, bundled-up consents, the use of pre-ticked boxes or default opt-ins are not allowed. Also, you must make it clear why consent is requested, that it can easily be withdrawn; and you must be able to evidence, if asked, that consent has been given.

For further reading, please see the Information Commissioners Office (ICO) separate guidance regarding consent which is due to be published in April 2018.

Frequently asked questions

What is the standard for lawful consent?
If consent was "freely given, specific, informed and unambiguous" it will be okay. The ICO has said this means individuals will have actively opted-in, were given a genuine choice and that it was made clear and specific as to what they were consenting. Consent will not be given freely where there is an imbalance of power in the relationship, so local authorities and employers should look for another lawful basis for data processing. Finally, and crucially, individuals must be provided with the opportunity to opt-out.

We have existing data. Do we need to obtain a fresh consent?
The ICO has made it clear in its draft guidance on consent, "If existing DPA consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR compliant consent,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." (But also see below: *Direct marketing and consent*).

We send out an email newsletter to club/group members. Will we need to seek fresh consent?
If you already meet the GDPR requirements on consent, or if your newsletter is solely concerned with news or routine customer service messages (see next question); and does not promote campaigns, events, products or services – including free ones - then you will not need fresh consent. However, if none of these apply, you will need to refresh your consent.

Do we need consent to send emails to existing beneficiaries/members regarding our services?
You do not need to rely on consent (although you will still need another lawful basis for data processing) for routine customer service messages. These are email or text messages to service users, beneficiaries, members etc. to provide information they need about a current or past service/contract etc. However, if you include any "significant promotional material" then consent is needed.

Can we rely on another lawful basis rather than consent?
Consent is one of only six lawful bases for data processing. If there is any doubt regarding consent, then you should consider if another lawful basis for processing can be used (and documented accordingly). However, consent will still be a requirement for electronic direct marketing (see below: *Direct marketing and consent*).

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. If someone withdraws consent, processing must end as soon as possible.

What about someone's 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 otherwise. If you have good reason to believe that someone lacks the capacity to understand the consequences of consenting, a third party with the legal right to make decisions on their behalf (eg. under a Power of Attorney) can give consent.

Does using third party email processors like MailChimp change anything?
Not really. If you use one of the online mailing list providers like *MailChimp*, you will still need to follow the rules regarding consent when collecting email addresses for direct marketing, and ensure that all mailings sent on your behalf make clear an individual's right to withdraw consent by unsubscribing. Most providers such as *MailChimp* have a double opt-in process whereby individuals have also to verify their email address after signing up. Additionally, the mailing list provider will also have to be GDPR compliant; and you should be satisfied that this is apparent in their contract (terms and conditions) with you.

Are there any extra requirements for seeking consent for children?
If you want to rely on consent rather than another lawful basis for your processing, you must get parental consent for children in accordance with your normal policy. However, if you provide online information services then children can give consent themselves if aged 13 or over. Where you 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. (See also Green Pepper's briefing *Processing Children's Personal Data*).

When is consent the only option?
You will need consent when no other lawful basis for processing data applies. You will also need consent for electronic direct marketing under the *Privacy in Electronic Communication Regulations 2003* (see below: *Direct marketing and consent*).

How can we provide evidence of consent?
You must have an effective audit trail of how and when consent was given, so that you can provide evidence if challenged. Good records will also help you monitor and refresh consent. Your CRM system may be able to evidence consent at the moment it is given or withdrawn. Otherwise documents such as copies of completed and time-stamped online data capture forms, or paper copies of signed and dated consent will be acceptable, but a spreadsheet kept by yourself with ticks and dates entered against individual names would not.

Direct marketing and consent

Direct marketing is the promotion of goods, services, aims and ideas. So it will cover, for example, fundraising appeals, event promotions or campaign communications. Non-profit organisations from charities to political parties will therefore need to ensure their direct marketing complies with data protection law. What's more, in addition to GDPR, you will also have to comply with the current *Privacy in Electronic Communications Regulations 2003* (PECR).

Because of PECR, **consent** is required for direct marketing by email, text and automated telephone calls (electronic direct marketing). However, as the ICO points out, under PECR there is an exception to this rule for existing customers, known as the 'soft opt-in'. This means organisations can still send commercial marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; and
- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

However, this soft opt-in does not apply to non-commercial marketing such as campaigning or promoting ideas, even to existing supporters.

Live phone calls, which are covered by PECR, do not require consent, and so are open for you to consider legitimate interest as an alternative lawful basis for processing. However, you must check that the individual is not registered with the Telephone Preference Service.

Postal marketing is not covered by PECR and it is therefore also open to you to consider legitimate interests as your lawful basis for this type of marketing.

Consent checklist

The ICO guidelines contain the following checklist to help organisations comply with the rules on obtaining 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 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.
- ❑ 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.

References: Information Commissioners Office, Data Protection Network