Webinar: Ask OSCR with the Information Commissioner's Office (ICO) – Data protection for charities

Questions and answers

How long is a reasonable time to keep personal data for if a volunteer is dormant? Is there a minimum time or is it organisation-led? And is it ok to keep a record of their name and date of PVG volunteering etc but with no other personal data?

The storage limitation principle sets out that you must not keep data for longer than you need it. The UK GDPR does not set specific time limits for different types of data. This is up to you, and will depend on how long you need the data for your specified purposes. The charity should consider what is appropriate, considering the normal retention of volunteers, how likely they are to return and any other relevant factors such as the value of the data to the charity over time. The charity should have a clear policy for this data retention. You might want to consult with volunteers about this retention policy and ask for their views, that may help you get an idea of volunteers' reasonable expectations which should inform your decision on an appropriate retention policy.

Can you explain a bit about the main changes in July 2026, and what charities need to do to prepare for them?

The Data Use and Access Act (2025) changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.

Most of the changes offer you an opportunity to do things differently, rather than needing you to make specific changes to comply with the law.

These changes started being phased in from June 2025 and the final changes will come into force in June 2026 such as the complaints process. You can refer to this page for updates: How to deal with data protection complaints | ICO.

In general, DUAA might make things easier for you in the following ways:

- **New 'recognised legitimate interests' lawful basis**: when you use personal information for certain 'recognised legitimate interests', it removes the need for you to balance the impact on the people

whose personal information you use, against the benefits arising from that use. For example, when protecting public security.

- **Disclosures that help other organisations perform their public tasks**: it allows you to give personal information to organisations such as the police, without having to decide whether that organisation needs the information to perform its public tasks or functions. Instead, the organisation making the request is responsible for this decision.
- **Assumption of compatibility**: it allows you to assume that some re-uses of personal information are compatible with the original purpose you collected it for, without having to do a compatibility test. This includes disclosing personal information for the purposes of archiving in the public interest, even if you originally only got consent for a different purpose.
- **'Soft opt in' for charities**: if you're a charity, it allows you to send electronic mail marketing to people whose personal information **you collect** when they support, or express an interest in, your work, unless they object.
- **Subject access requests (SARs)**: it makes it clear that you only have to make reasonable and proportionate searches when someone asks for access to their personal information. Note that 'reasonable' isn't defined in the legislation so it is up for organisations to determine based on the context.
- **Making things clearer**: it improves the way the law is written and structured to make it easier for you to follow and apply, but without materially changing how you can use personal information. For example:
    - it clarifies that direct marketing can be a legitimate interest; and
    - it rewords the test you need to apply when transferring personal information outside the UK.

For a comprehensive overview, please see the ICO website that has plenty of information: [The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations? | ICO.]

What is the guidance around collecting business email addresses from online sites such as Google and Facebook and sending charitable info?

Data protection law and PECR don't necessarily prevent you from doing this but there are restrictions. For example, you **must** tell people that you have their

information and what you want to do with it, as well as ensuring what you want to do is fair and lawful.

You **must** consider whether your direct marketing activities will be unexpected to the people whose information you are collecting from public sources.

For instance, because someone's social media page has not been made private or they are seeking a large audience for their social media post doesn't mean that you are free to use their personal information for direct marketing purposes. They won't expect you to do this.

For more detail, look at our direct marketing guidance on generating leads.

What do we need to tell people if we collect their information from other sources?

It is particularly important to be transparent with people if you don't have a direct relationship with them. This is because people may have no idea that you collect their information from other sources to use for direct marketing unless you tell them.

There is a list of information in the UK GDPR you **must** provide to people if you don't collect their information directly from them. In general, this list is the same as when you collect people's information directly from them, and the requirements for this information to be clear and in plain language still apply. But you also **must** give them details about:

- the categories of their information you hold (e.g. contact details, interests); and
- the source of their information (e.g. the particular organisation it came from).

You **must** give people your privacy information within a reasonable period and at the latest within a month of obtaining their information (unless an exception applies, see below).

There are additional requirements if you plan to use the information to send direct marketing to the person it relates to, or to disclose it to someone else. In that case, the latest point at which you **must** provide your privacy information is when you first communicate with that person or disclose their information to someone else. But the one month time limit still applies, so it is a case of whichever is sooner.

A common issue that arises is when emails are sent to a number of unrelated individuals who are cc'd rather than being bcc'd such that everyone on the distribution list can see others email addresses. Does this constitute a breach and what is a proportionate response to mitigate the breach?

Whether or not this is a data breach would depend on the information being shared. An e mail address is personal information but there may be occasions where it is acceptable to include copies of personal addresses such as if the trustee board have agreed this information can be shared. There will be other occasions where it relates to beneficiaries or donors where this could constitute a data breach. The charity will need to consider the seriousness of a breach, for example what information is revealed, and report accordingly.

- ICO tool - Self-assessment for data breaches | ICO
- ICO guidance - Self-assessment for data breaches | ICO

For our museums collection, do you have any advice on retention of personal data of people who have donated items to our collection? Is this exempt from GDPR or covered by it? (Names, addresses, other identifiable info - some going back to 1840s, but also contemporary as we're still collecting).

Where a person is no longer living then their information is no longer considered to be personal data under GDPR. So for the older collections this will not be covered by GDPR. Any more recent collections will be covered by GDPR. You may want to discuss with other galleries and museums about their approach and policies.

We have a membership subscription scheme as part of our organisation - if a member dies, do we delete their info immediately or are we required to retain for a certain period?

As mentioned above data protection law does not apply to deceased individuals and so we couldn't comment on this. You may want to discuss this with SCVO or other charities and ask their approach.

Would you advise a separate Privacy Notice for children?

If your organisation deals with children, you should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have. The ICO has guidance Using children's information: a guide | ICO which contains a checklist:

Privacy notices

☐ Our privacy notices are clear, and presented in plain, age-appropriate language.

☐ We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.

☐ We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.

☐ As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

☐ We tell children what rights they have over their personal data in language they can understand.

What qualifies as 'large scale processing'?

GDPR does not contain a definition of large-scale processing, but decide whether processing is on a large scale you should consider:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.