For organisations / Guide to Data Protection / Guide to the General Data Protection Regulation (GDPR) / Right of access / How should we prepare?

How should we prepare?

Share Download options

Contents

In more detail

Why is it important to prepare for the right of access?

Whether or not you receive SARs on a regular basis, it is important that you are prepared and take a proactive approach. This helps you to respond to requests effectively and in a timely manner. It also helps you to:

- comply with your legal obligations under the UK GDPR and Data Protection Act 2018 (DPA 2018) – and show how you have done so;
- streamline your processes for dealing with SARs, saving you time and effort;
- increase levels of trust and confidence in your organisation by being open with individuals about the personal data you hold about them;
- enable customers, employees and others to verify that the information you hold about them is accurate, and to tell you if it is not;
- improve confidence in your information handling practices; and
- increase the transparency of what you do with individuals' data.

What steps should we take?

There are a number of ways that you can prepare for SARs. What is appropriate for your organisation depends on a number of factors, including the:

- type of personal data you are processing;
- number of SARs you receive; and
- size and resources of your organisation.

- **Awareness** – Make information available about how individuals can make a SAR (eg on your website, in leaflets or in your privacy notice).
- **Training** – Provide general training to all staff to recognise a SAR. Provide more detailed training on handling SARs to relevant staff, dependent on job role.
- **Guidance** – Create a dedicated data protection page for staff on your intranet with links to SAR policies and procedures.
- **Request handling staff** – Appoint a specific person or central team that is responsible for responding to requests. Ensure that more than one member of staff knows how to process a SAR, so you have resilience against absence.
- **Asset registers** – Maintain information asset registers which state where and how you store personal data. This helps speed up the process of locating the required information to respond to SARs.
- **Checklists** – Produce a standard checklist that staff can use to ensure you take a consistent approach to SARs.
- **Logs** - Maintain a log of SARs you have received and update it to monitor progress. The log may include copies of information you've supplied in response to a SAR, together with copies of any material you've withheld and why.
- **Retention and deletion policies** – Have documented retention and deletion policies for the personal data you process. This helps to ensure that you don't keep information longer than you need to and therefore potentially reduces the amount of information you need to review when responding to a SAR.
- **Security** – Have measures in place to securely send information. For example, by using a trusted courier or having a system to check email addresses and review responses before sending.

What about our information management systems?

You will find it difficult to deal with SARs effectively without adequate information management systems and procedures. Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs. They should enable you to easily locate and extract personal data and allow you to redact third-party data where necessary.

If you are implementing a new information management system, you need to take a data protection "by design and default" approach and ensure that the system facilitates dealing with SARs.

You should also have effective records management policies, such as:

- a well-structured file plan;
- standard file-naming conventions for electronic documents; and
- a clear retention policy about when to keep and delete documents.

> Relevant provisions in the UK GDPR - see Articles 5(1)(c), 5(2), 25, 30, 32, 26, 28 and Recitals 39, 78, 82, 83
> External link

Further reading

- Data protection by design and default
- Accountability and governance
- Documentation

Previous Next

English

Subscribe to our e-newsletter

English

The ICO exists to empower you through information.

Contact us Privacy notice Cookies Disclaimer © Copyright
Accessibility Cymraeg Publications

☎ 0303 123 1113