SFA 8 step guide to managing data access requests

1. Educate your staff

It is essential that all your staff know what a data access request looks, how it can be received in your business and the name of the people who are responsible for dealing with data access requests.

Ideally your business should have a dedicated email, address or web form whereby individuals can send in their data access requests. If your business does not have this in place consider setting up a dedicated email for data access requests.

Be aware that data access requests can come via the following channels:

- E-mail
- Web forms
- Social media such as twitter direct messages, Facebook messenger or LinkedIn
- Letter
- Over the phone or in person
- Via a solicitor who is representing the data subject

Ensure that **all staff** are aware of how data access requests can come in to your business and **most importantly** ensure that they immediately forward it to the person responsible for managing data access requests or someone else in their absence.

2. Ensure the data access request is valid and verify identify of data subject

It is recommended that businesses verify the identity of the data subject. This could be a request for ID or other means to verify the identity of the data subject.
If the data access request has come from a solicitor, it is essential they send you proof that their client has consented to them receiving their personal data. If this has not been received do not send over any personal data until you receive documented proof that the data subject has agreed to this.

3. Acknowledge receipt of the data access request

Let the data subject know that you have received their data access request and who they can contact should they have any further questions. If you have a data access request policy you can send the individual a copy of it. You could also ask the individual if they are looking for a specific piece of personal data, however, they may decide they want all of their personal data and this must be complied with.

4. Gather all the personal data

Collect all the personal data that is relevant to the data access request. If you have mapped out where personal data comes in from and where it is held, it is much easier to gather all this personal data when a request comes in.

It is important to know that “Personal data” is any information that is related to an identified or identifiable living individual. This personal data, which is either in electronic or hard copy format, is most likely held in various parts of your business such as:

- Employee HR files
- Accounting systems
- Documents where the data subject is identified/referenced
- Emails/letters/messages where the data subject is identified/referenced
- CCTV images/recordings
- Call recordings where the data subject is identified/referenced
- Biometric data
- CRM systems
- Newsletter systems
- Marketing tools and other digital tools including web forms
- Third party providers

5. Consider if any exemptions may apply to the data access request

There are limited circumstances in which personal data can be withheld, these exemptions include:

- In contemplation of or for the establishment, exercise or defence of a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings either before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
- For the enforcement of civil law claims, including matters relating to any liability in respect of damages, compensation or other liabilities or debts
- For the purpose of estimating the amount of liability on foot of claim for damages or compensation, if access would prejudice the data controller’s commercial interests
- To safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State
- For the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- For the administration of tax, duty or other money due to the State or a local authority in any case where access would be likely to prejudice such administration
- Where the personal data consists of an expression of opinion which was given in confidence or on the understanding it would be treated as confidential. **NB:** *A high threshold of confidentiality is required to apply this exemption and business owners are not normally able to rely on this exemption*
- Where the personal data is kept by the Data Protection Commission, the Information Commission or the Comptroller or Auditor General for the performance of their functions
- Where processing of data is for archiving, scientific, historic or statistical purposes in the public interest and restrictions are necessary to the extent that exercise of the right of access would seriously impair the achievement of those purposes.

6. Ensure all personal data relating to other persons is redacted

You will need to ensure that the personal data relating to the data subject is separated from the personal information of others. You will need to redact (block or blacken out) all information that has personal data that is not related to the data subject and which identifies others. This is a particularly tricky issue for e-mails and CCTV footage.

It might be useful as a practice going forward to start a new e-mail if an individual is named in the e-mail and store personally identifiable emails into a central location.

7. **Have the collected personal data reviewed before sending it to the data subject**

Once all relevant information has been collected, it should be reviewed by a legal advisor or whoever is responsible for GDPR in your business.

8. **Issue a letter to the individual and include the mandatory information**

When issuing the response letter to the data subject ensure the following mandatory information is included:

- The purposes of the processing
- The categories of personal data involved
- To whom the personal data has been or will be disclosed
- Whether the data will be or has been transferred outside of the EEA
- The period that the data will be stored, or the criteria to be used to determine retention periods
- The right to make a complaint to the Data Protection Commission
- The right to request rectification or deletion of the personal data
- The right to restrict or object to the processing of the personal data

In addition, you will need to include the following if it applies:

- Where the personal data has not been collected from the data subject, information as to its source
- Whether the data has been subject to automated decision making together along with information regarding that processing