SSRO

Single Source Regulations Office

Procedure for responding to Subject Access Requests

June 2023

1. Introduction

1.1 The Data Protection Act 2018 (DPA) provides individuals with rights in connection with personal data held about them. Individuals can be internal to the SSRO (employees) or external (including stakeholders) and they have the right to obtain:

- confirmation that the SSRO is processing their personal data;
- a copy of their personal data; and
- other supplementary information set out in section 4 of this procedure.

1.2 This procedure defines the process to be followed by the SSRO when a request for access to personal data (a "subject access request") is received.

1.3 A failure to comply with the provisions of the DPA in responding to requests may render the SSRO, or in certain circumstances the individuals involved, liable to prosecution.

2. Responsibilities and definitions

2.1 Roles and responsibilities relating to subject access requests are defined as follows:

- **Data Protection Officer (DPO)** is responsible for ensuring that statutory and regulatory obligations are adhered to. This role is undertaken by the Director of Corporate Resources.
- **Data Protection Manager** is responsible for handling subject access requests, acting on behalf of the DPO.
- **Information Commissioner's Office** is the UK's independent authority set up to promote access to official information and to protect personal information.
- **Data Controller** is the person or organisation who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. In most cases the SSRO itself is the registered Data Controller for the personal data it holds.
- **Data Processors** are any individual or company who records and/or processes personal data in any form on behalf of the SSRO and therefore subject to the requirements of this policy. It may also include the SSRO, to the extent that it processes personal data on behalf of another (e.g. a contractor).
- **SSRO permanent and temporary employees, contractors and consultants** are responsible for incorporating this procedure and its associated policy into their own working practices.

3. What does a valid Subject Access Request look like?

3.1 There is no prescribed way in which a data subject must make a request, nor form the request must take. The request does not have to be made in writing, and it does not have to specifically refer to a 'subject access request' or the 'right of access'.

3.2 A valid subject access request is one which:

- provides all the information the SSRO requires to locate the information the person wants; and
- provides sufficient information to verify the data subject's identity.

3.3 Before disclosing any personal information, the Data Protection Manager must verify the identity of the data subject. The DPA requires the SSRO to be satisfied as to the identity of the individual making a request.

3.4 If the request is from an employee, their identity will generally be obvious and immediately verifiable. If not, it is unlikely that the first contact will provide sufficient information to verify the identity of the individual, in which case the Data Protection Manager will seek to do so. A template is provided at Appendix 1 to this procedure, which includes a form to be sent to the data subject to complete and return.

3.5 If the evidence provided remains insufficient, such that there are doubts about the identity of the person making the request, there are two options:

- telephone the individual and, based on the information held about them, ask relevant questions to confirm their identity; or
- write to the individual and ask them for further information.

3.6 It is important that only information which is necessary to confirm the individual's identity is requested. The information requested must be proportionate. The Data Protection Manager should keep a record of what measures they take.

3.7 The SSRO must comply with a subject access request **promptly** (i.e. without undue delay) and **in any event within one month** of receipt of the subject access request or information requested to confirm identity (whichever is later). The time limit is calculated from the date of receipt until the corresponding calendar date in the next month.

3.8 The SSRO can extend the time to respond by up to a further two months where necessary, taking into account the complexity or the number of requests from the individual. The Data Protection Manager must let the individual know within one month of receiving their request and explain why the extension is necessary.

3.9 People are able to make requests via a third party, such as a solicitor or family member. This may be the case where, for example, legal action is involved or the person does not feel capable of dealing with the request on their own. In such circumstances the SSRO should make sure that the person acting on their behalf either has the legal authority to do so or has the permission of the data subject.

4. Information to be provided

4.1 Article 15 of the GDPR specifies what must be provided to the data subject in response to their subject access request. These can be put into three groups:

- confirmation of processing;
- a copy of the relevant personal data, and explanatory information; and
- additional information relating to the processing, to the extent it is not already covered in the SSRO's Personal Information Charter.

Confirmation of processing

4.2 The SSRO should confirm that it processes information relating to the person. This should be done at the earliest point following the verification of the request and the determination that the SSRO has information about the person.

A copy of the relevant personal data, and explanatory information

4.3 Personal data is any information relating to an identified or identifiable living individual. An individual is only entitled to their own personal data, and not to information relating to other people (unless the other individual has consented to the disclosure).

4.4 If the person has specified what personal data they are looking for or which individuals hold it, the search can be limited. In such cases the SSRO would respond to the specific request, rather than interpret it more widely.

4.5 The Data Protection Manager, in consultation with the Data Protection Officer, will identify which individuals are to conduct the search, from whom permission must be sought to search their files and the extent of the search. There may be a need to involve the IT Managed service provider, for which authorisation will be provided by the DPO.

4.6 The extent of the search may, depending on the data subject and nature of request, include:

a. electronic documents held in the SSRO's SharePoint files;

b. electronic documents held by individuals on their laptops and personal one drive files;

c. emails and attachments held by individuals on their SSRO email account;

d. office collaboration platforms (including Skype and Teams);

e. electronic documents held on the SSRO's intranet; paper records, including personnel records and private filing systems;

f. data/information held on mobile phones; and

g. records of individuals or companies who record and/or process personal data in any form on behalf of the SSRO.

4.7 The SSRO may also act as Data Controller in relation to work-related personal data which is held on employees' private devices or accounts. If an employee holds such information, they may be acting as the SSRO's agent and the personal data would be within scope of the subject access request.

4.8 If staff are aware of other business areas that might also hold information about the person concerned, they should inform the Data Protection Manager as soon as possible so that they can arrange for these areas to be searched.

4.9 Once the Data Protection Manager has collected together the information, they must examine it in detail to establish if it should be disclosed. This must be done on a case-by-case basis for each individual piece of information. In some cases only parts of particular documents must be disclosed. The Data Protection Manager should:

a. Check that the record is about the person concerned and not about somebody else with the same name. For example, an email might carry the subject line "Meeting about John Smith" but if the email only contains details about whether people can attend the meeting the email is not about John Smith. The Data Protection Manager should only identify records/documents/emails which are about the person making the subject access request.

b. Screen out any duplicate records. For example, if there has been an e-mail exchange with some colleagues, the Data Protection Manager only needs to provide the last email in the exchange if copies of all the other emails are part of the last email.

c. Only disclose a record created by a member of staff acting in a private rather than an official capacity in exceptional circumstances. If they are not prepared to disclose the record, do not disclose it. Please note however that SSRO staff should act in accordance with the Acceptable Use Policy for SSRO Information and Communications Technology.

d. Only disclose information that is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, they should carefully consider whether to disclose the information about the third parties to the data subject. If the record is primarily about the data subject, with incidental information about others, they could redact the third-party information. If the record is primarily about third parties it should be withheld if redacting is not possible. Alternatively, the third party can be contacted to obtain consent to disclose if possible. All correspondence in these matters should be logged in the relevant folder.

e. Balance the interests of the third party against the interests of the data subject in cases where the records contain correspondence and comments about the data subject from private individuals and external individuals acting in an official capacity. Such third party information can be omitted or redacted.

f. Not disclose information that would prejudice the prevention or detection of a crime. For example, if the Police informed the SSRO that a member of staff is under investigation but the member of staff did not know this, then the information should not be provided to the member of staff while the investigation is in progress. However, if the investigation is closed or if the member of staff has been informed that there is an investigation underway, the information should be disclosed in response to a subject access request.

g. Not disclose any records that contain advice from our lawyers, where we are asking for legal advice or which were written as part of obtaining legal advice.

h. Not disclose information that is being used, or may be used in future, in negotiations with the data subject, if the information gives away the SSRO's negotiating position and disclosing the information would weaken that negotiating position.

4.10 The list of exemptions identified above is an indicative list of those that are most likely to apply to information held by the SSRO. There may be other circumstances in which the subject access request may not be complied with. Examples include where the SSRO is not the Data Controller and has no obligation to respond, where the request is manifestly unfounded (for example, where it is malicious in intent), or where the request is excessive (for example, it repeats the substance of previous requests and a reasonable interval has not elapsed). We will have regard to all exemptions specified in the Data Protection Act. Legal advice should be sought in all cases where it is proposed not to comply with a subject access request.

4.11 As the Data Protection Manager puts the information together they may discover material which does not reflect favourably on the SSRO. For example, they may find documents that show that standard procedures have not been followed, or documents that may cause offence to the data subject. We recognise that these are not valid reasons for withholding the documents. However, the Data Protection Manager should bring their contents to the attention of the relevant manager and ensure that appropriate action is taken to address any issues they raise.

4.12 Staff must not destroy, or refuse to disclose, records. This is a criminal offence if it is done after the subject access request has been made.

4.13 Once the Data Protection Manager has identified all information that can be sent in response to a subject access request, one final review of this information as a collection must be made, under the supervision of the Data Protection Officer. This is to offset the risks often discovered through the aggregation of information that additional information could be disclosed or at least interpreted.

Additional information related to the processing:

4.14 The Data Protection Manager should refer the data subject to the SSRO's Personal Information Charter, which sets out the information that the response will provide.

4.15 If an individual makes a request electronically, the SSRO should provide the information in a commonly used electronic format, unless the individual requests otherwise. Required information can also be directly communicated in paper form.

5. How to log the requests and responses.

5.1 The Data Protection Manager should log subject access requests and allocate a unique reference number to the subject access request. This number should be used in all correspondence.

5.2 The Data Protection Manager should create a folder for each subject access request. The filename should be made up from the reference number and surname of the applicant e.g. SAR001 – Smith. Each file should include the following:

- Copies of the correspondence between the Data Protection Manager and the data subject and between the Data Protection Manager and any other parties.
- A record of any correspondence, telephone conversation or other means used to verify the identity of the data subject.
- A record of searched documents and locations.
- A record of the Data Protection Manager's decisions (for example on redactions) and how they came to those decisions.
- Copies of the information sent to the data subject, for example if the information was anonymised keep a copy of the anonymised or redacted version that was sent.

5.3 The folder should be kept for five years and then securely destroyed within the SSRO's records management programme.

Appendix 1

Dear [ ]

The Data Protection Act 2018 grants you the right to access your personal data held by the SSRO, including the right to obtain confirmation that we process your personal data, receive certain information about the processing of your personal data and obtain a copy of the personal data we process. In order for us to respond to your request, we ask that you submit this request either:

- In writing by post to Data Protection Manager, Single Source Regulations Office, G51/G52 100 Parliament Street, London, SW1A 2BQ.
- Electronically via email to [EMAIL ADDRESS].
- By using [our secure portal] **OR** [OTHER SUBMISSION MECHANISM]], after authenticating your identity with your [username and password **OR** [OTHER AUTHENTICATION MECHANISM]].

We expect to respond to your request within one month of receipt of a fully completed form and proof of identity. You do not have to use this form but using this form should make it easier for you to make sure you have provided us with all relevant information, and for us to process your request.

For more information on your rights, see the SSRO's Personal Information Charter at https://www.gov.uk/government/organisations/single-source-regulations-office/about/personal-information-charter.

1. Requested name (data subject) and contact information

Please provide the data subject's information below. [If you are making this request on the data subject's behalf, you should provide your name and contact information in *Paragraph 3*.]

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, to respond to your request and to keep a record of your request and our response.

First and last name:	
Any other names that you have been known by (including nicknames and previous sur-names):	
Home address:	
Date of birth:	
Telephone number:	

Email address:	
Are you a current or former employee of the SSRO?	
If so, please provide your approximate dates of employment:	

2. Proof of data subject's identity

We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth and current address. We accept a photocopy or a scanned image of one of the following as proof of identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.
- [OTHER PROOF OF IDENTITY].

[Please also attach a copy of a bank or credit card statement or utility bill showing your current address and dated within the last three months.] If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact [NAME AND TITLE] at [TELEPHONE NUMBER] or [EMAIL ADDRESS] for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you. We reserve the right to refuse to act on your request if we are unable to identify you.

3. [Requests made on a data subject's behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name:	
Home address:	
[Date of birth:]	
Telephone number:	
Email address:	

What is your relationship to the data subject (for example, solicitor, other adviser, parent, carer)?	
Do you have legal authority to request the data subject's information?	
If the data subject is under 13, do you have parental authority to act for them?	

We accept a photocopy or a scanned image of one of the following as proof of your identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.
- [OTHER PROOF OF IDENTITY].

If you do not have any of these forms of identification available, please contact [NAME AND TITLE] at [TELEPHONE NUMBER] or [EMAIL ADDRESS] for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We also require proof of the data subject's identity before we can respond to the request. To help us establish the data subject's identity, you must provide identification that clearly shows the data subject's name, date of birth and current address. We accept a photocopy or a scanned image of one of the following as proof of identity:

- Passport or photo identification such as a driving licence.
- Birth or adoption certificate.
- [OTHER PROOF OF IDENTITY].

[Please also attach a copy of a bank or credit card statement or utility bill showing the data subject's current address and dated within the last three months.] If the data subject has changed [his **OR** her] name, please provide the relevant documents evidencing the change.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf:

- A written consent signed by the data subject.
- A certified copy of a power of attorney.
- Evidence of parental responsibility.
- [OTHER PROOF OF AUTHORITY].

We may request additional information from you to help confirm the data subject's identity. We reserve the right to refuse to act on your request if we are unable to identify the data subject or verify your legal authority to act on the data subject's behalf.]

4. Information requested

To help us process your request quickly and efficiently, please provide as much detail as possible about the personal data you are requesting access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help us locate your personal data.

[For example, you may specify that you are seeking:

- Employment records or personnel records.
- Pensions or other benefit records.
- Personal data held by [DEPARTMENT].
- Medical records.
- Email or other electronic communications (specify the approximate dates, times and correspondents).
- Billing information.
- Photographs.
- Video footage.
- User activity logs.
- Transaction histories.
- Correspondence between [NAME] and [NAME] between [DATE] and [DATE].]

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request “all information about me”). We will begin processing your access request as soon as we have verified your identity and have all the information we need to locate your personal data.

In response to your request, we will provide you with the information we are required to provide, including information on:

- The purposes of processing.
- Categories of personal data processed.
- Recipients or categories of recipients who receive personal data from us.
- How long we store the personal data, or the criteria we use to determine retention periods.
- Any available information on the source of the personal data if we do not collect it directly from you.
- Whether we use automated decision-making, including profiling, meaningful information about the auto-decision logic used, and the significance and consequences of this processing.
- Your right to:
    - request correction or erasure of your personal data;
    - restrict or object to certain types of processing with respect to your personal data; and
    - make a complaint to the local data protection authority.

If the information you request reveals personal data about a third party, we will either seek that individual’s consent before responding to your request, consider if it is otherwise reasonable to provide it to you or we will redact third parties’ personal data before responding. If we are unable to provide you with access to your personal data because disclosure would infringe the rights and freedoms of third parties, we will notify you of this decision.

Applicable law may allow or require us to refuse to provide you with access to some or all the personal data that we hold about you, or we may have destroyed, erased or made your personal data anonymous in accordance with our record-retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Signature and acknowledgement

I, [NAME], confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that:

- the SSRO must confirm proof of identity and may need to contact me again for further information.
- My request will not be valid until the SSRO receives all the required information to process the request.
- I am entitled to one free copy of the personal data I have requested.

The SSRO's preferred way of providing information is through electronic copy. If you would like to receive the personal data you are requesting in hard copy, please indicate this, and the reasons why, in the box below.

	Electronic copy.
	Hard copy (including explanation in box below).

……

Signature

……

Date

[AUTHORISED PERSON SIGNATURE

I, [NAME], confirm that I am authorised to act on behalf of the data subject. I understand that the SSRO must confirm my identity and my legal authority to act on the data subject's behalf, and may need to request additional verifying information.

……

Signature

……

Date]