Subject Access Request Procedures

Version Control

1. Full Document Number:	OPESOP002
2. Version number:	3.0
3. Superseded version number:	2.1
4. Document owner job title:	Data Protection Officer
5. Department / function:	Strategic Operations
6. Next review date:	01-APR-2024
7. Add document to external LSTM website?	Yes

Modifications from previous version of document

Version	Date of issue	Details of modification
Version	**Date of issue**	**Details of modification from previous version**
1.0	09.02.2018	v0.3 included Senior HR Manager (OD and Engagement) suggested amendments.
2.0	16.05.2019	Updated for DPA2018, updated intranet links, new DPO contact details, SAR gatekeepers, and central log.
2.1	28.05.2019	Target audience defined
3.0	30/03/2021	Updates to bring in line with latest ICO guidance and document template

1 Introduction and Context

1.1 Under the Data Protection Act 2018, data subjects can request access to their personal data. This is known as a "subject access request" (SAR).

1.2 Sometimes, a third party may make on SAR on behalf of the data subject. This may be allowed, for example a lawyer making a SAR on behalf of their client. Before responding to such a request you must ask the third party to provide evidence that they are authorised to make the SAR on behalf of the individual (see paragraph 2.1 below).

1.3 Requests must be made verbally, in writing, from or a valid e-mail address or via social media. If a request is made verbally, ask for written confirmation so that you can check the identity of the person making the request to avoid a data security breach. The individual making the request must receive a response within one month of receipt although the time limit can be paused if you need to ask for clarification.

1.4 There is generally no charge for a SAR – see paragraph 2.5 for when you can charge for a manifestly excessive or unfounded request.

1.5 Normally, requests will be directed to the department who holds the personal data, e.g. Human Resources or Education. A SAR "gatekeeper" has been identified in each department that has received a SAR. Where there is no available gatekeeper the Data Protection Officer (DPO) will deal with the request and seek the relevant information to respond to the SAR from the appropriate department (s)

1.6 For simple, routine requests, department gatekeepers can deal directly with the data subject provided they follow these procedures and keep the necessary records. It is not necessary to inform the DPO in advance of answering a SAR unless it is complex, exemptions may apply, or the department gatekeeper(s) has other concerns about the SAR. To ensure that processes are being followed correctly the DPO maintains a central log of SARs which gatekeepers must update. The DPO will carry out periodic audits.

1.7 The Data Protection Act 2018 gives the data subject a "right of access" and they do not have to explain why they want the data[1]. The Act states a preference for self-service access to this data e.g., via "remote access to a secure system". An example of this currently within LSTM, would be the ability to view and alter personal data within the Employee Self-Service (ESS) system. While this may not be possible for all current systems which process personal data about staff and students, it should be considered when procuring or designing new systems to reduce the administrative burden of responding to SARs. Departments can also further reduce the number of SARs they receive by responding promptly

[1] Recital 63

to request for access to individual pieces of personal information. This will reduce the number of SARs since in most cases individuals will only make SAR when their initial request has not been dealt with.

2 Actions to take

2.1 Firstly, ensure that it is a valid request, and that the individual is asking for a copy of their own personal data. The request can be made verbally or in writing, including by email and via social media. Internal requests may be considered valid if they come from an lstmed.ac.uk account, although if the request seems suspicious further checks should be made to verify no hacker or intermediary is involved. For third party requests (see paragraph 1,2 above) there needs to be a record of the consent in writing of the data subject that the third party is entitled to make a SAR on the individual's behalf.

2.2 The Data Protection Act 2018 also states that the controller "…should use all reasonable measures to verify the identity of a data subject who requests access…"[2]. This could be from their address or their signature, if you have a record of these. If this is not possible, seek further verification by telephone. To confirm their identity, ask two questions based on information you have about them.

2.3 You need to be satisfied that you know the identity of the individual making the request (or the identity of the data subject on whose behalf the third party is making the request) If you are unsure of the identity of the data subject you can ask for further verification which could be a photocopy of their passport or driving licence. Consider the possible harm and distress caused to the individual in the case of inappropriate disclosure of the information requested in deciding what identity checks may be required. Do not request further verification if the requester's identity is obvious to you, for example they are a staff or a student member of LSTM. The calendar month period in which you must respond to the request starts from when you receive the verification documentation. Request further verification promptly and do not use this as a technique to delay a response to the request.

2.4 Calculate the response due date. This should be calculated as a calendar month, so includes non-working days such as weekends and Bank Holidays. The ICO advises that Consider a calendar month as being 28 days long.

2.5 In most cases you cannot charge a fee for responding to a SAR. However, you can charge a fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. If you believe that a SAR is manifestly unfounded or excessive then please consult with the Data Protection Officer.

[2] Recital 64

2.6 Make reasonable efforts to find and retrieve the information requested. You are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing the data subject with access to the information. If you process a large amount of personal information about an individual, you may be able to ask them to specify the personal information you hold or processing activities if it is not clear what their request for access relates to. In a lot of cases individuals may just be after access to a specific set of personal information. This benefits you as it means you only have to disclose a specific set of information. It also benefits the individual as they get access to exactly the personal information that they want rather than having to wade through all the personal information you hold about them. The individual may still want access to all the personal information you hold about them and if that is the case, then you have to respect their wishes. If you ask the individual to specify/clarify the request, then the time limit for responding to the request is paused. Once you receive the specification/clarification the time limit will start running again.

2.7 If the information requested contains information about other individuals (for example an email conversation involving multiple individuals), you will need to follow this three-step process:

1) Does the request require disclosing information that identifies another individual?

Consider whether it is possible to comply with the request without revealing information that relates to and identifies another individual(s). Consider the information you are disclosing in response to the request and any information your reasonable believe the individual making the request may have or may get hold of that would identify the other individual(s)

Remember that your obligation is to provide information not documents, so you may delete names or edit documents if the information about the other individual(s) if it does not form part of the requested information.

If it is impossible to take out the information about the other individual(s)and still comply with the request, then you need to move on to the next step.

2) Has the other individual provided consent?

The clearest legal basis for disclosing information about the other individual(s) in response to a request made by an individual is that the other individual(s) has given their consent. Where possible ask the relevant individual(s) for their consent to the disclosure of their personal information in your response to the individual making the SAR.

However, you are not obliged to use the consent legal basis for disclosing information about the other individual(s) in response to a SAR. Indeed. in some circumstances it may not be appropriate to use the consent legal basis. These include where:

(i) You do not have contact details for the other individual(s)
(ii) Asking the other individual(s) could potentially disclose personal information of the requester to the other individual(s) they were not already aware of
(iii) It would be inappropriate for the other individual(s) to know that the requester had made a SAR

3) Is it reasonable to disclose without consent

The DPA 2018 says that you must consider all the relevant circumstances including but not limited to the following factors:

(i) the type of personal information about the other individual(s) that you would disclose to the requester
(ii) any duty of confidentiality owed to the other individual(s)
(iii) any steps taken by you to try to get the other individual(s) consent
(iv) whether the other individual(s) is capable of giving consent, for example if the other individual was a child
(v) if the other individual(s) had refused consent[3].

2.8 Screen the information to see which parts can be disclosed and if any areas need to be redacted. If the work to process the data will take longer than a month you must notify the data subject as soon as possible. You can extend for up to a further two months.

2.9 Redaction should be carried out in the following ways:

(i) If you are dealing with hard copy documents and need to redact the information:

- Make a photocopy;
- Redact the exempt information using a black marker pen;
- Make a photocopy of the redacted version. This is the copy which will go to the person making the SAR.

(ii) For electronic documents, specialist software is available for complex requests and can also provide a secure portal for sharing the results. For simple requests comprising up to ten or so documents it is recommended that you use Adobe software for PDFs, or a freely available plug-in for MS Word called "Redaction" which you can obtain from this website: https://redaction.codeplex.com/

2.10 The response to the SAR must consist of the personal data relating to the requesting individual and other supplementary information which are:

The other supplementary information is:

A) The purpose(s) of the processing.

B) The lawful basis for the processing.

[3] This section is taken from the ICO detailed guidance on the right to access – "What should we do if the request involves information about other individuals?"

C) The legitimate interests for the processing (if applicable).

D) The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

E) The recipients or categories of recipients of the personal data.

F) The details of transfers of the personal data to any third countries or international organisations (if applicable).

G) The retention periods for the personal data.

H) The rights available to individuals in respect of the processing.

I) The right to withdraw consent (if applicable).

J) The right to lodge a complaint with a supervisory authority.

K) The source of the personal data (if the personal data is not obtained from the individual it relates to).

L) The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

M) The details of the existence of automated decision-making, including profiling (if applicable).

This list largely corresponds to the information contained in the relevant LSTM privacy notice/policy. Either include the relevant LSTM privacy notice or list the above information in your SAR response.

2.11 If the SAR was made electronically then the response and documents should be provided in a commonly used electronic format unless the individual requests a different format. Consider both the circumstances of the request and whether the individual has the ability to access the SAR response in that format. Find out the individual's preferred format before sending out the SAR response. You can also provide remote access to the individual of their personal data and the ability for them to download a copy in the appropriate format. An LSTM example would be through the Employee Self Service system (ESS). LSTM as the controller has the responsibility to comply with the security principle under the DPA 2018. If you are sending the SAR response by email, then you must comply with the IT Acceptable Use Policy. If you are sending the SAR response by hard copy, then Consider using Royal Mail Recorded Delivery or equivalent service. If the SAR response is very large then Consider using a courier company. Information sent to the requester must be in a suitable and secure manner. Refer to the LSTM Information Classification Matrix for assistance.

3 Exemptions and Special Cases

3.1 The SAR exemptions are:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege

- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks

If you think any of these exemptions apply, then please consult with the Data Protection Officer.

3.2 The special cases are:

- unstructured manual records;
- credit files;
- health data;
- educational data; and
- social work data.

If you think any of the special cases apply, consult with the Data Protection Officer

3.3 You can refuse to comply with a request if it is manifestly unfounded or excessive. If you think this is the case, consult with the Data Protection Officer.

3.4 You may refuse to provide all or some of the requested information depending on the circumstances if you have checked with the Data Protection Officer that

- an exemption/ special case applies and/or
- the request is manifestly excessive or unfounded.

3.5 If you refuse to comply with a request in whole or part you must inform the individual of:

- the reasons why

- their right to make a complaint to the ICO or another supervisory authority if they are resident in another country under that country's national data protection law
- their ability to seek to enforce their right of access through the courts

4 Regulatory and or legal action to comply with the right of access

4.1 The ICO may take action against a controller or processor if they fail to comply with the right of access. The ICO took action against a housing developer in 2019 for failures in this respect[4]. The ICO will exercise these enforcement powers in accordance with its Regulatory Action Plan[5].

5 Prohibition on forcing an individual to make a SAR

5.1 LSTM cannot force a prospective staff member or student to make a SAR so that LSTM can gain access to information about them, for example their convictions or health information. This is a criminal offence. Where it is possible and necessary to make these requests in respect of criminal convictions LSTM can obtain the information through the Disclosure and Barring Service[6] by requesting either standard or enhanced checks. If LSTM requires detailed health information about a prospective staff member or student or current staff member or student, then it must use the provisions under the Access to Medical Records Act 1988.

6 Record keeping and logging requests

6.1 Controllers and processors must be able to demonstrate compliance with the accountability requirement of the DPA 2018 through records of decisions made and actions carried out. LSTM must therefore keep records and information relating to all SARs.

6.2 Any electronic records that are kept, should be on central, IT-approved systems e.g. P:/ or S:/ drives or SharePoint. On occasions, there will be hard copy documents kept in central filing systems such as those administered by Human Resources. These must be kept securely as per guidance in LSTM's "Information Classification Matrix" and should be kept for the length of time determined by LSTM's corporate retention schedules.

6.3 The information kept should include:

[4] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/02/housing-developer-fined-for-ignoring-data-request/ Reference checked 11/01/2021
[5] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf Reference checked 11/01/2021
[6] https://www.gov.uk/government/organisations/disclosure-and-barring-service Reference checked 11/01/2021

- Copies of the correspondence between you and the data subject, and between you and any third parties;
- A record of any telephone conversation used to verify the identity of the data subject;
- A record of your decisions and how you came to those decisions;
- Copies of the information sent to the data subject, e.g. if the information was anonymised or redacted, keep a copy of the anonymised or redacted version that was sent in response to the request.

6.4 Details of every SAR received must be reported to the Data Protection Officer via Teams.

7 Related documents and further information

LSTM Information Classification Matrix
GDPR articles 12 and 15
LSTM Privacy Notices
IT Acceptable Use Policy
Right of access section from the ICO Guide to the UK General Data Protection Regulation

Further information about data protection is on the Knowledge Exchange. If you have any queries or concerns, please contact the Data Protection Officer: dataprotection@lstmed.ac.uk