Data Subject Access Request Policy

1. Background

The General Data Protection Regulation (GDPR) allows individuals to access information from organisations that process their personal data. The process for obtaining this information is known as a subject access request.

2. What is a Subject Access request (SAR)?

A SAR is a request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR.

All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a request is received, it should immediately be reported to the Data Protection Officer (dataprotectionofficer@ifs.org.uk)

3. Identifying a Subject Access Request

The UK GDPR does not set out formal requirements for a value request. It is therefore important that staff knowhow to recognise a SAR.

SARS may be made

- Verbally,
- In writing
- Via social media
- To any part of the IFS (e.g to mailbox, to IT, to specific researchers)

Requests do not specifically have to mention any phrases from the UK GDPR. If a request is made for an individual to access their personal data. If staff are not sure whether a request is a SAR, it should be forwarded to the Data Protection Officer immediately.

4. Staff training

The IFS does not hold identifiable data about the general public. SARs are most likely to be received by the following categories of data subjects:

1. Members of staff or associates
2. Former members of staff or associates
3. Individuals on our mailing list
4. Individuals who have attended IFS events
5. Individuals who have taken part in surveys run by IFS where we hold personal data

For this reason, staff working in HR, communications, IT and data services are given specific training to ensure that they can recognise a Subject Access Request. In addition, research staff who are involved in collecting data are also given additional training.

Research staff are made aware that if the receive a SAR in relation to de-identified data, they should suggest that the data subject gets in contact with the relevant organisation that collected the data.

5. Charging a fee

In general, a fee will not be charged in line with the law. However, if an individual makes an excessive request or a request is repeated after a short period of time, an administrative fee may be charged if appropriate.

6. IFS Procedures: Responding to Subject Access Requests

Action		**Time frame from time request received**
When a request is received, it should be forwarded immediately to dataprotectionpolicy@ifs.org.uk	Staff member who receives the request	immediately
All Subject Access Requests will be logged on the Subject Access Request register with the date received. The Subject Access Request register is located on I:\Data\GDPR\Subject Access Requests and is maintained by the Data Protection Officer	DPO. In the absence of the DPO, responsibility lies with the Head of Operations	Immediately
If you are not sure the requester is who they say they are you should check this by asking questions that only the individual would know. For example, if it is an ex-employee, ask who their line manager was and the dates that they worked for IFS.	DPO	
Read the request carefully and if necessary, confirm with the data exactly which data they wish to access. They may not want access to everything and it is okay to confirm with them.	DPO	immediately
Consider whether the request is complex. If so, send a letter to the requester as contained in section 7 explaining why and stating the extension date	DPO	As soon as possible
Alert key IFS individuals regarding the receipt of the request and timeline. This may include: • Head of Operations • Head of ICT • Director; • Head of Finance; • Senior members of the Computing Committee and; as necessary • Line Manager and Sector Head (employee request) • Head of PR and Head of Communications (external request)	DPO	As soon as possible
Agree (through convening meeting or email correspondence) an owner for the subject access request, responsible for working with others to prepare the response.	DPO with key IFS individuals	
With key IFS individuals, brainstorm all sources of relevant information. This may include (but is not limited to):	DPO with key IFS individuals	

- Email including the jobs@ifs.org.uk inbox - Network files - Hard copies of HR information - Marketing databases - Events databases - Research data collection - Recruitment		
Assign responsibility to searching depending on where the information will be found. E.g historical email will be searched by IT, marketing or events databases will be searched by comms, research data collections will be searched by the relevant member of res	Key individuals	2 weeks
Gather together all the relevant information and review it - Check whether the information really relates to the individual - Redact any information about other people which doesn't relate to the person making the SAR - Ensure that the redaction is done in an irrevsible way. E.g. once redaction has been carried out, print out the file and scan it back to pdf. - Consider whether releasing any information to the Data subject might have a negative impact on another individuals (even after redaction). If is will, consider withholding this piece of information and record this in the SARs log - Consider whether the information needs to be kept for legal reasons	DPO	3 weeks
All details to be logged in the Subject Access Request register. I:\Data\GDPR\Subject Access Requests\SARs log.xls	DPO	3 weeks
Prepare your reply. Check with the requester what format the would be happy to receive the reply in. In addition to the personal information, you also need to include: Why we hold their data How we got it How long we plan on keeping it Who we share it with How they can ask for it to be updated or deleted Consult the templates contained in section 7 of this policy	DPO	Less than one calendar month
Keep a record of the reply in the SARs log	DPO	One calendar month

7. IFS Template letters for responding to Subject Access Requests

Four templates are included on the following pages:

- Letter responding to subject access request providing requested information (compliant with the GDPR)
- Letter responding to subject access request asking for more information (compliant with the GDPR)
- Letter refusing subject access request or asking for an administrative fee (compliant with the GDPR)
- Letter refusing subject access request or asking for an administrative fee (compliant with the GDPR)

Letter responding to subject access request providing requested information (compliant with the GDPR)

Dear [ ]

Thank you for [submitting your form/your email] on [date], making a request for your personal data.

We confirm that we process the following information about you:

- [List categories of personal data.]

We process this information to [specify the purposes for processing].

[This data was obtained from [specify any third party from whom data was obtained, eg external benefit provider].]

Your information is shared internally, including with [members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles].

We also share your data with third parties that process data on our behalf [, in connection with recruitment, payroll, the provision of benefits and the provision of occupational health services]. [Specify any other third parties with whom data is shared and why.]

[We do not transfer your data to countries outside the European Economic Area.

OR

HR-related personal data may be transferred to countries outside the European Economic Area ("EEA"), specifically, the organisation's management information system, Deltek Vision is a cloud-based service and information in the system may be transferred, sorted or backed up in countries outside the EEA. Appropriate safeguards have been put in place to cover such data transfer, using the standard contractual clauses published by the European Courts for such cases (ref: 2010/87/EU).]

We do not make employment decisions based solely on automated decision-making.

We will hold your personal data for [set out various retention periods].

As a data subject, you have a number of additional rights in relation to your data. You can:

- require us to change incorrect or incomplete data;
- require us to delete or stop processing your data in certain circumstances, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the organisation relies on its legitimate interests as the legal ground for processing.

[If you would like to exercise any of these rights, please contact [name, contact email or address].]

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

We enclose a copy of the information requested [provide information on format and any security features].

[Please note that, as the information that you have requested includes personal information relating to third parties, we have redacted this to protect their identities.]

[Please note that the information you have requested includes data that is subject to legal professional privilege/processed for the purpose of management planning/relates to intentions in negotiations with you/consists of a confidential reference that we have provided for you. This information is exempt from disclosure and has therefore been removed from the data requested by you.]

To confirm, the files included are:

- [List files.]

We trust that this responds sufficiently to your subject access request.

Yours sincerely

[ ]

Letter responding to subject access request asking for more information (compliant with the GDPR)

Dear [ ]

Thank you for [submitting your form/your email] on [date], making a request for your personal data.

In order to respond to your request, we require the following [information/proof of identity] to [locate the requested personal data/identify you]:

[Details of information/proof of identity required]

Please provide the above [information/proof of identity] as soon as possible so that we can respond to your request. The one-month time period for us to respond to your request will not start to run until we receive the requested [information/proof of identity] from you.

If you have any queries about this, please do not hesitate to contact [name].

Yours sincerely

[ ]

Letter extending time to respond to a subject access request (compliant with the GDPR)

Dear [ ]

Thank you for [submitting your form/your email] on [date], making a request for your personal data.

The normal time limit for responding to a personal data access request is one month from the date we receive the request. However, the time limit can be extended by two months if the request is complex.

We believe that your personal data access request is complex and that an extension of time to respond is necessary because of [list the appropriate points and expand on them as necessary]:

- [the amount of your personal data that we process;
- the fact that your personal data is contained in a number of different systems and/or locations, and includes data that has been archived and that will need to be retrieved before it can be searched;
- the fact that some of your personal data is being processed by a third party on our behalf and we will need to liaise with it to respond to your request;
- the number of searches that will have to be carried out to locate the data that you have requested; and
- the fact that some of your data is likely to be mixed with the personal data of other people.]

For these reasons, we will respond to your subject access request within three months of the date we received it. This means that we will respond to your subject access request by [date].

If you have any queries about this, please do not hesitate to contact [name].

Yours sincerely

[ ]

Letter refusing subject access request or asking for an administrative fee (compliant with the GDPR)

Dear [ ]

Thank you for [submitting your form/your email] on [date], making a request for your personal data.

If we receive a personal data access request that is manifestly unfounded or excessive, we can refuse to act on the request or we can charge a reasonable fee for dealing with it.

We believe that your request is manifestly unfounded or excessive, because it repeats the subject access request that you submitted on [date]. We have considered whether or not the nature of your data, the purposes for which it is processed or the frequency with which it changes means that a reasonable interval has passed since your last request. We have concluded that this is not the case.

[We are therefore not going to respond to your personal data access request. If you wish to discuss this further, please contact [name].

OR

We are prepared to comply with your personal data access request if you are willing to pay a fee of £[ ] to reflect the administrative costs we will incur in providing the information to you. [Provide instructions for payment.] We will respond to your request once we have received the fee.]

You can lodge a complaint about our decision with the Information Commissioner or take legal action to compel us to comply with your subject access request.]

Yours sincerely

[ ]

8. Policy review and audit log

8.1 Summary of audit and review findings

Date	Reviewed by	Audited by	Issues found	NC or Obs?	Action taken	Location of audit findings*

*all audit findings are stored in subfolders within ISO27001\Policies and internal audits\7. Internal audit and review\

8.2 Log of changes made

Date	Changes made	Changes made by	Approved by	Major or minor change?	Where archived?* (major changes only)

*all archived documents are stored in subfolders within ISO27001\Working documents and archive\Archive