

GDPR1 – SUBJECT ACCESS REQUESTS

1. SUMMARY

Individuals have the right under the Data Protection Act 1998, (to be superseded by the General Data Protection Regulation (GDPR) on 25 May 2018), subject to certain exemptions, to have access to their personal records that are held by the Society of Consulting Marine Engineers and Ship Surveyors (SCMS).

This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individual with whom the SCMS has had dealings with and holds personal data. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or Word documents and may also be in the form of photographs.

Anyone making such a request is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from. Under GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise and objection to the processing altogether.

The following procedure defines the method that will be followed, and the steps to be taken, when handling Subject Access Requests, under the Data Protection Act/GDPR, for information directed to any member of the Society of Consulting Marine Engineers and Ship Surveyors (SCMS) staff. This is based on the Information Commissioner's Office Subject Access Code of Practice: ICO Subject Access Code of Practice.

2. REVISION AND APPROVAL

Rev.	Date	Nature of Changes	Approved By
1	01/05/2018	Original Issue	CEO
2	06/08/2023	Update	CEO
3	13/10/2025	Review and update to paperless	CEO

GDPR1 – SUBJECT ACCESS REQUESTS

3. PURPOSE

To meet the requirements of the Data Protection Act 1998, as amended, and the EU General Data Protection Regulations (GDPR) 2018.

The purpose of this procedure is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests. *Comment: Any requests made for non-personal information must be dealt with as a Freedom of Information (FOI) request Team. It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA or the Environmental Information Regulations (EIR) 2004 is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA or the EIR to the world at large, this could lead to a breach of the data protection principles.*

4. PROCESS OWNERS AND RESPONSIBLE PARTIES

4.1. Staff Member

- To advise individuals on how to apply for access to data when requested to do so
- To note any reason given for the request
- To review the SAR form for completion and details
- To request additional information where required from the requester
- To maintain the SAR log with details of all requests whether they are fulfilled or not.
- To assess requests and ascertain whether they should be progressed as a SAR, FOI request EIR request or referred onwards to the CEO/DPO

4.3. Chief Executive Officer (CEO)/Data Protection Officer (DPO)

- To review all SAR responses and approve prior to release to the requester
- To review and approve all SARs that are to be refused on grounds of an exemption
- To review and approve all SARs where a payment is to be levied
- To ensure that all controversial SAR decisions are duly documented and approved
- To provide support to all staff for responses to SARs

5. PROCEDURE

This procedure is summarised in Form 953 – Procedure for Handling Subject Access Requests Flowchart.

Assisting and Advising Service Users on how to make a request

GDPR1 – SUBJECT ACCESS REQUESTS

- 5.1. Where it is ascertained that an individual is verbally making an SA request, advise them to put the request in writing on Form 950 – Subject Access Request Form, detailing the information they are requesting with as much information as possible to enable it to be located.
- 5.2. Send them Form 952 – Subject Access Information Sheet and Form 950 – Subject Access Request Form.
Comment: These forms can be provided by email for electronic completion of Form 950 or by post.
- 5.3. Request they tell you their reason for making their request and make a note of this reason to add to the Subject Access Request Log once the request is received in writing.
Comments: Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request.
A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. It is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with this procedure and forward immediately to the CEO or DPO.
- 5.4. Advise the applicant to send the request to the CEO/DPO and provide contact details.
Comment: In order to comply with equality legislation, where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct. NOTE: Responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g. braille.

Requests made about or on behalf of other individuals

General Third Party

- 5.5. A third party, e.g. solicitor, may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney, must be provided by the third party.
- 5.6. If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

Responding to requests

- 5.7. On receipt of a completed SAR Form, open the SAR log and complete as many of the following details as possible:
 - Date received,

GDPR1 – SUBJECT ACCESS REQUESTS

- Date response due (within one month under GDPR),
- Applicant details,
- Information requested,
- Any fees levied (information must be provided free of charge under GDPR from 25th May 2018),
- Exemptions applied in respect of information not to be disclosed,
- Details of decisions to disclose information without the data subjects' consent,
- Details of information to be disclosed and the format in which they were supplied,
- When and how supplied, e.g. Paper copy and postal method used to send them.

5.7. Determine whether the person's request is to be treated as a routine enquiry or as a subject access request (SAR).

Comment: If you would usually deal with the request in the normal course of business e.g. confirming appointment times or details of public meetings planned then do so. The following are likely to be treated as formal subject access requests:

- a. Please send me a copy of my Member's file.*
- b. I am a solicitor acting on behalf of my client and request a copy of his Member's records. An appropriate authority is enclosed.*
- c. The police report that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.*

5.8. Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party is obtained before releasing information requested, this may be in the form of documentation as detailed on Form 952 – Subject Access Request Information.

5.9. Ensure adequate information has been received to facilitate locating the information requested. Where insufficient information has been received, contact the requester and ask for the missing details.

5.10. Locate the required information from all sources and collate it ready for review by the CEO/DPO.

Comment: This review is to ensure that the information is appropriate for disclosure, i.e. to ascertain whether any exemptions apply e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed, or is information to be withheld due to on-going formal investigations

Payment

5.11. Determine whether a fee is to be charged for the information to be provided.

Comments: GDPR does not allow for a standard fee however, a reasonable fee may be charged under GDPR for any further copies of the information that has already been requested or when a request is 'manifestly unfounded or excessive'. However, any fee must be based on administrative costs only.

GDPR1 – SUBJECT ACCESS REQUESTS

It is possible to refuse to respond to ‘manifestly unfounded or excessive requests’ under GDPR but the SCMS must explain to the individual about their right to complain to the Information Commissioners Office as soon as possible and at the latest within one month if they feel this refusal is unfounded.

- 5.12. Determine whether the information is likely to change between receiving the request and sending the response and make appropriate arrangements for the latest information to be made available to the requester.

Comment: Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the Data Protection Act 1998 (to be superseded by the General Data Protection Regulation (GDPR) on 25th May 2018).

Third Party Checks

- 5.13. Check whether the information collated contains any information about any other individuals. If so, consider:

Is it possible to comply with the request without revealing information that relates to the third party? (Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party).

- 5.14. Where it is not possible to remove third party identifiers you must consider the following:
1. Has the third party consented to the disclosure?
 2. Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?

Comment: The following must be considered when trying to determine what reasonable circumstances are:

- *Duty of confidence owed to the third party,*
- *Steps taken to try and obtain consent,*
- *Whether the third party is capable of giving consent, and*
- *Any express refusals of consent from the third party.*

- 5.15. A record of the decision as to what **third party** information is to be disclosed and why should be made on the SAR Log Form.

Check for Exemptions

- 5.16. Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes,
- Negotiations with the requestor,
- Management Forecasts,
- Confidential References given by you,

GDPR1 – SUBJECT ACCESS REQUESTS

- Information used in research, historical or statistical purposes; and
- Information covered by legal professional privilege.

5.17. If the information requested, is held by the SCMS and exemptions apply then a decision must be made as to whether you inform that applicant that the information is held but is exempt from disclosure or whether you reply stating that no relevant information is held.

Comment: A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided. NB. It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

Decoding/Explanations

5.18. If the information contains complex terms or codes, you must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms.

Preparing the Response

5.20. When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case, by the due date (one month from the request date or that date all information needed/fees were provided by the requester).

5.21. Prepare a copy of the information requested in a permanent form except where the individual agrees or where it is not possible in the format requested or would involve undue effort.

Comment: This could include very significant cost or time taken to provide the information in hard copy form, but advice should be taken from the CEO/DPO before refusing on these grounds.

NOTE: Under no circumstances should original records be sent to the applicant

5.22. Where a hard copy cannot be provided an alternative is to allow the individual to view the information at an arranged date and time.

5.23. Pass the prepared copy of information to the CEO/DPO for final approval for release to the individual. SCMS have a maximum of one month under GDPR to comply with the SAR starting from the date that SCMS receive all the information necessary to deal with the request and any fee that is required.

5.24. Once the CEO/DPO confirm that the information can be released, complete the entry in the SAR Log with:

1. The date of approval for release and by whom
2. The date the documents are posted, emailed or viewed
3. The way the documents are released to the individual e.g. recorded delivery post

GDPR1 – SUBJECT ACCESS REQUESTS

- 5.25. Ensure all electronic documents relating to the SAR are filed in the appropriate folder in the Data Protection/SAR/Request number on the SCMS Shared Documents drive.

Comment: It is an offence under the Data Protection Act 1998 (GDPR from 25 May 2018) and individuals can complain to the Information Commissioners Office or apply to a court if SCMS do not respond within this time limit.

6. RECORDS/REFERENCES

QS Form Ref.	Document Title
Form 950	Subject Access Request Form
Form 951	Subject Access Requests Log
Form 952	Subject Access Request Information Sheet
Form 952	Subject Access Request Procedure Flowchart