

ASSOCIATION OF BRITISH INVESTIGATORS

Subject Access Requests

Guidance Document

DOCUMENT OWNER
Association of British
Investigators

VERSION
v.2026-06

WEB
www.theABI.org.uk

Intended Audience: This Guide is intended for members of the Association of British Investigators (ABI) who are acting in the UK GDPR role of Controller. Members who are acting as Processors must not respond directly to a Data Subject Access Request (DSAR or SAR) but must immediately refer the request to the relevant Controller.

While the right of access, commonly referred to as a SAR or DSAR, is intended to empower individuals to obtain a copy of their personal data and understand how it is being used, it must also be acknowledged that this right may be misused. In contentious matters, such as those frequently handled by ABI members, SARs may be deployed as tools for intimidation, disruption, or other improper purposes. This can create additional pressure for ABI members and may complicate already difficult professional relationships and interactions.

Recognising the potential for abuse is therefore important when handling SARs, so that legal rights are upheld while appropriate safeguards are applied against manipulation. However, suspected misuse is not, in itself, a reason to ignore the obligation to respond lawfully and appropriately.

A SAR may initially appear daunting or intimidating. However, if handled correctly and promptly, the ABI member should be able to discharge their responsibilities without significant inconvenience, unnecessary expense, or regulatory intervention.

1. Introduction

- 1.1** This guidance outlines practical steps for ABI members acting as Controllers under the UK General Data Protection Regulation (UK GDPR) to manage Subject Access Requests (SARs). A SAR enables individuals to exercise their right to access personal data held about them.

2. Roles and Responsibilities

- 2.1 Controller:** In specific situations, an ABI member's organisation/agency acts as the Controller when processing personal data. This is detailed in the [ABI UK GDPR Code of Conduct for Investigative and Litigation Support Services](#). When this applies, you must ensure:
- **GDPR compliance for SARs:** Always clearly document roles and communicate them to relevant stakeholders.
 - **Data Protection Officer (DPO):** If applicable, the DPO for the agency oversees the SAR process, provides guidance on data protection law, and ensures compliant handling of requests.

3. Handling Subject Access Requests

- 3.1 Understanding the Right of Access:** Individuals have the right to request access to their personal data held by the Controller. Requests must be dealt with promptly and, in any event, within one month of receipt.
- 3.2 Verification of Identity:** Before processing, verify the requester's identity to prevent the disclosure of personal data to the wrong person. Where you have reasonable doubts about the requester's identity, you may ask for further information to confirm it, but any such request must be proportionate to the nature of the data held. In those circumstances, the one-month period does not begin until you have received the information reasonably required.
- 3.3 Documenting Requests:** Record each SAR, including:
- Date of receipt
 - Identity verification details
 - Nature of the request
 - Actions taken
 - Date of response
- 3.4 Assessing the Request:** Check the validity of the SAR and assess possible exemptions and other grounds that may limit your response under the UK GDPR, such as:
- Manifestly unfounded or excessive requests
 - Requests concerning other individuals' data
- For detailed guidance see ICO website:*
- *When can an exemption apply*
 - *Manifestly unfounded or excessive*
- 3.5 Gathering Relevant Information:** Compile and prepare the response, ensuring it includes:
- Confirmation of whether personal data is being processed

- A copy of the personal data
- Information on the purposes of processing
- Data categories
- Recipients to whom data has been disclosed
- The retention period for the data, or the criteria used to determine it
- The source of the data, where it was not collected from the individual
- The existence of any automated decision-making, including profiling, and meaningful information about the logic involved
- The individual's right to request rectification or erasure, or to restrict or object to processing
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

4. Response to the Request

- 4.1 Timely Response:** Respond without undue delay and within one month of receipt. If more time is needed due to complexity or volume, inform the requester within the initial month and keep them updated. The time for responding may be extended by up to a further two months where the request is complex or where a number of requests have been received from the individual. You must tell the requester within one month of receipt and explain why the extension is necessary.
- 4.2 Fees:** A SAR must normally be dealt with free of charge. A reasonable, administration-based fee may only be charged where the request is manifestly unfounded or excessive, or where the individual requests further copies of data already provided.
- 4.3 Format of Response:** Provide a clear, concise response in a commonly used electronic format unless the individual requests otherwise. Consider the individual's ability to access the data in the provided format.
- 4.4 Assistance:** Various factors may influence how best to structure the response and determine its format. If you require assistance, please contact the ABI Secretariat.

5. Providing Information

5.1 The response should include:

- The requested personal data
- An explanation of how the data is processed
- Information on the individual's rights regarding their data

5.2 Exemptions and Limitations

If a part of the request cannot be fulfilled due to exemptions, explain the limitation and the reasons for the refusal or restriction.

6. Record Keeping and Accountability

- 6.1 Maintaining Records:** Keep thorough records of SARs to demonstrate compliance. Include actions taken, correspondence, and any exemptions applied.
- 6.2 Regular Review:** Periodically review the SAR process and this guidance to ensure ongoing effectiveness and legal compliance.
- 6.3 Training:** Ensure all relevant staff are trained on SAR handling, data protection principles, and individuals' rights under the UK GDPR.
- 6.4 Awareness Campaigns:** Inform individuals about their rights and the SAR process, promoting transparency and accessibility.
- 6.5 Cooperation with Regulator:** Cooperate with the ICO in any concerns or investigations related to SARs and be prepared to demonstrate compliance with this guidance.

7. Conclusion

- 7.1** This guidance provides a structured approach for ABI members acting as Data Controllers to manage Subject Access Requests in line with the UK GDPR, promoting transparency, accountability, and respect for individuals' rights. Members are encouraged to implement and regularly review these practices to uphold high standards of data protection.