Government Internal Audit Agency

Data Subject Access Requests (DSAR) Policy

Version: 01
August 2024

Better insights, better outcomes

Contents

1. Introduction

Policy purpose

1.1. The Government Internal Audit Agency (GIAA) is committed to complying with our legal obligations under Article 15 of UK GDPR and Schedule 1 of the Data Protection Act 2018. This helps us to be transparent on how we process individuals' personal data.

1.2. This policy provides information on how we manage Data Subject Access Requests (DSARs). It outlines the key processes and responsibilities for the handling of DSARs across the organisation.

1.3. This policy applies to all GIAA colleagues who handle personal data on behalf of GIAA and should be applied consistently across the organisation.

1.4. Any enquiries about the policy should be sent to correspondence@giaa.gov.uk.

1.5. This policy works in conjunction with our complaints procedure, which can be read on our website – GIAA Complaints procedure.

Policy statement

1.6. The objectives of this policy are to ensure we deliver:

- **Transparency:** We are committed to the principles of lawfulness, accountability, transparency, and the general right of access to information. This policy outlines how we manage our obligations for compliance.
- **Accessibility:** To help individuals understand how and why we use their data
- **Compliance:** To ensure compliance with Article. 15 of UK GDPR and government standards.
- **Accountability:** To ensure we comply with the accountability principle in Article 5(2) of UK GDPR, which requires us to take responsibility for what we do with personal data.

Definitions

Word/phrase	Definition
Calendar Month	When we receive a DSAR we must respond to it as soon as possible and no later than one calendar month. A calendar month starts on the day we receive the request, even if that day is a weekend or a public holiday. It ends on the corresponding calendar date of the next month. However, if the end date falls on a Saturday, Sunday or bank holiday, the calendar month ends on the next working day.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller referred to in this policy is GIAA.
Data Protection Officer (DPO)	A person in GIAA tasked with monitoring compliance with UK GDPR and other data protection laws. The contact details for our DPO can be found our privacy notice.
Manifestly excessive	We can refuse to comply with a DSAR if the request is clearly or obviously unreasonable. An example of an excessive request is where it only asks for the information that has previously been requested.
Manifestly unfounded	We can refuse to comply with a DSAR if the request is malicious in intent and is being used to harass with no real purpose other than to cause disruption.
Personal Data	Any information relating to an identified or identifiable natural person. This may include special category data, which you can find more information about on the ICO's website.

Word/phrase	Definition
Processing	Any operation performed on personal data, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, or erasure.
Supervisory Authority	An individual authority established to supervise the compliance with a specific regulation. In regard to GDPR, the Information Commissioner's Office (ICO) is the Supervisory Authority for the UK.

2. Data Subject Access Requests

What is a Data Subject Access Request?

2.1. You have the right to ask an organisation if they're using or storing your personal information and ask for copies of the personal data. It helps individuals understand how and why we are using their data, and check we are doing it lawfully.

2.2. As well as a copy of your personal data you have the right to receive the supplementary information that the ICO outlines on their website. The supplementary information is addressed in GIAA's privacy notices. We will include a link to the relevant privacy notice in our response.

Who can submit a request?

2.3. You can submit a DSAR to ask for the personal information we might hold about you, or you can ask a third party (e.g., a relative, friend or solicitor) to make a request on your behalf. However, we may need to ask for evidence that the third party is acting on your behalf. For example, by asking you to confirm your permission in writing.

How can a request be submitted?

2.4. DSARs should be made by email (correspondence@giaa.gov.uk) or post to:

Correspondence Team

Government Internal Audit Agency

7th Floor, 10 Victoria Street

London

SW1H 0NB

2.5. When asking for information please try and be as clear as possible. This will help us understand your request and respond to you promptly.

Fees

2.6. We do not charge a fee for responding to DSARs.

Time limits for responding

2.7. We will respond to your request without delay and within one calendar month of receipt of the request.

2.8. We may need to extend the time limit for responding to your request if it is complex, or you have sent in more than one. We can extend the time limit for a further two months (i.e., we may respond up to three months from the receipt of your request).

Scope and clarification

2.9. When making a request you should supply the following information

- Your name and any other information that will help us identify you e.g., your relationship to GIAA
- If a third party is submitting the request on your behalf, they should explain their relationship to you, along with your full details
- A comprehensive list of the personal data you would like access to and where relevant, what information you don't need
- Any details or dates that will help us identify the information you require

2.10. If the scope of your request is unclear, or if we process a large amount of your information, we can ask you to specify the information you require before we respond to your request.

2.11. The time limit for responding to the request is paused until we receive clarification. We will confirm this to you when we request the clarification.

Confirming the identity of the requestor

2.12. To avoid personal data being sent to another individual, either accidentally or as a result of deception, it may be necessary for us to confirm your identity.

2.13. Examples of the information we may request include:

- Date of birth
- Other known names or aliases
- Confirmation of postal or email addresses
- A copy of a passport or driving license

- A photographic government building pass that includes your name (if you are an employee of a government body)
- Information relating to your civil service employment (if you are an employee of a government body)
- Investigation reference number (if you are an employee of a government body)

2.14. The timescale for responding to a DSAR does not begin until we have confirmed your identity.

Searches for the relevant information

2.15. We will perform a reasonable and proportionate search to find the personal data that we hold about you at the time of your request.

2.16. We may contact relevant individuals or teams in GIAA for the information we require to respond to the DSAR. Those persons are required to search the systems in scope for all relevant records.

2.17. If the DSAR is complex or involves searching through a large number of systems, we can request a system-wide search to be carried out by HM Treasury officials on our behalf (as we are an executive agency of HM Treasury, they manage our shared IT services). This will include searching all cloud-based systems including email.

2.18. If the request involves disclosing personal data that we have received from our customers, we will notify them about the request. A list of our customers can be found here.

Removing other information from the records

2.19. A DSAR gives you the right to access your personal information that we are processing. It does not give you access to documents or information outside of the scope of your request. We will redact information that is out of scope of the DSAR by ‘blocking out’ the material on the record.

Requests that involve information about other individuals

2.20. Personal data can relate to more than one person. Therefore, responding to a DSAR may involve providing information that relates to you and another individual. If we are unable to remove the information about the other individual and still comply with the request, there is

an exemption that says we do not have to comply with a DSAR. This can be used if doing so means disclosing information that identifies another individual, unless:

- The other individual has consented to the disclosure (we are not obliged to ask for consent); or
- It is reasonable to comply with the request without the individual's consent, e.g., the information is already known to you.

Issuing Responses

2.21. The Data Protection Officer (DPO) or their deputy will review our response prior to it being issued.

2.22. All responses will be issued with a link to the relevant privacy notice. The privacy notice will provide the supplementary information you have a right to receive along with a copy of your personal information as outlined by the ICO on their website.

2.23. As outlined in Article 12 GDPR we will respond to requests using clear and plain language. We will issue the response electronically by email unless a reasonable adjustment is required.

2.24. We will add a watermark to the information we provide. This will allow us to identify the source of any further disclosure of the information, should the need arise.

3. Refusing to comply with a request

3.1. We may refuse to comply with a request if an exemption applies, or if the DSAR is manifestly unfounded or manifestly excessive.

3.2. Schedules 2 and 3 of the Data Protection Act 2018 provides circumstances where we can apply an exemption when dealing with a DSAR. There are several different exemptions, and we will consider these on a case-by-case basis. We will justify and document our reasons for relying on an exemption(s).

4. Complaints

4.1. If you are unhappy with our response to your request, you can submit a complaint to us within three months of receiving our response. In exceptional circumstances we may be able to extend the time limit.

4.2. We must respond to the complaint without delay and no later than 20 working days from the date of receipt.

4.3. We will follow our usual complaints process, please see our Complaints procedure for more information.

ICO Complaints

4.4. If you are still unhappy with our response, you have the right to make a complaint to the Information Commissioners Office (ICO), the UK supervisory authority for data protection issues.

4.5. The ICO recommends that you should first give us a chance to respond to your complaint before contacting them, they will not normally review a complaint unless you have done so.

4.6. You should submit a complaint to the ICO within three months of your last contact with us.

5. Compliance and monitoring

5.1. We take our obligations under the UK General Data Protection Regulations (GDPR) and Data Protection Act 2018 seriously. We will comply with the rights of data subjects in line with the the requirements of data protection legislation and the Information Commissioner's Office (ICO). We have an appointed Data Protection Officer, and all our staff are provided with appropriate training on security and data protection.

5.2. The policy will be reviewed periodically, either as part of lessons learned or at least every two years.

Equality impact assessment

5.3. As part of its development, this policy and its impact on equality have been reviewed in line with the Public Sector Equality Duty. You can read more about the Public Sector Equality Duty here.

5.4. The purpose of the assessment is to minimise and, if possible, remove any disproportionate impact on employees and service users in relation to the protected characteristics: race, sex, disability, age, sexual orientation, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity.

5.5. No detriment was identified.

Version number	Date	Summary of changes
01	Oct 2024	Signed off