UK GDPR Data Subject Access Request (DSAR) Policy

1. Purpose

This policy outlines the process for handling Data Subject Access Requests (DSARs) under the UK General Data Protection Regulation (UK GDPR). It ensures transparency for both the business and the requestor, and sets out clear expectations, timeframes, responsibilities, and exemptions.

2. Scope

This policy applies to all employees, contractors, and third parties who process personal data on behalf of the organisation. It covers all DSARs received from individuals seeking access to and/or information about their personal data and how it is processed.

3. Recognising a DSAR

A DSAR is a request made by an individual to access personal data that the organisation holds about them. It does not need to mention "DSAR" or "UK GDPR" to be valid. Staff should treat any request that includes the following as a potential DSAR:

- A request to see or obtain a copy of personal data.
- A question about what personal data is held or how it is used.
- A request to know the source of personal data.
- A request to know who personal data has been shared with.
- A request to confirm whether personal data is being processed.

Examples of valid DSARs include:

- "Can you send me all the information you have about me?"
- "I want to know what data you hold on me and why."
- "Please provide a copy of my personnel file."
- "Who have you shared my data with?"

Unique Reference N°	Classification	Created	Version	Reviewed	Next Review
GDPR61	C1	12/2025	V1		12/2026

All staff must be trained to **recognise** these requests and forward them immediately to the DPO.

4. Submitting a DSAR

- All DSARs **must be directed to the Data Protection Officer (DPO)** in the first instance.
- The DPO will **coordinate the response**, liaise with the requestor, and manage the process in accordance with the organisation's DSAR Procedure, Guidance & FAQs (see separate document).
- DSARs may be submitted via email, post, or any other official communication channel.

5. Identity Verification

- Before any DSAR can be actioned, **the identity of the requestor must be verified**.
- The DPO may request official documentation (e.g., passport, driving licence) to confirm the identity of the data subject.
- If identity cannot be verified, the DSAR will be paused until sufficient evidence is provided.

6. Timeframes

- The organisation will respond to DSARs **without undue delay** and **within one calendar month** of receipt.
- This period may be extended by **up to two additional months** if the request is complex or numerous.
- **The DPO will determine whether an extension is justified** and will notify the requestor within the initial one-month period, including the reasons for the extension.

7. Exemptions and Rejections

Under UK GDPR, certain exemptions may apply. These include:

- Data that includes information about other individuals (unless consent is obtained or it is reasonable to disclose).
- Data subject to legal privilege.

- Data processed for crime prevention or investigation.
- Data that would prejudice negotiations or confidential business information.

The DPO is responsible for assessing and applying any exemptions in accordance with UK GDPR and relevant guidance. If a DSAR is deemed to fall under an exemption, the DPO will inform the requestor and explain the basis for the decision.

In rare cases, a DSAR may be **rejected** if:

- It is manifestly unfounded or excessive.
- The identity of the requestor cannot be verified.
- The request does not relate to personal data held by the organisation.

The DPO will make the final determination on whether a DSAR can be lawfully rejected and will provide written justification to the requestor.

8. Acknowledgement and Action of Valid DSARs

- The organisation will **acknowledge and act upon all DSARs where no exemption applies**.
- Once identity is verified and no exemption is determined, the DPO will proceed to gather and prepare the relevant personal data.
- The organisation is committed to fulfilling its legal obligations under UK GDPR and will ensure that valid DSARs are completed within the statutory timeframe.

9. Sharing of Data

Once the DSAR has been validated and the relevant data compiled, **the DPO will be responsible for sharing the required personal data with the requestor**.

- Data will be shared using a **secure method**, such as encrypted email or secure file transfer.
- If password protection is used, **passwords must be sent separately** from the data file, using a different communication channel (e.g., SMS or separate email).

- The DPO will ensure that only the data subject's personal data is disclosed, and that no third-party data is included unless lawful to do so.

10. Independence of DSARs

- The organisation will **act on all DSARs regardless of any related or separate issues**, such as grievances, complaints, disciplinary matters, or disputes.
- DSARs are treated as **independent legal rights** and will not be delayed, denied, or deprioritised due to other ongoing matters.

11. Internal Cooperation

- All staff, departments, and third parties who hold or process personal data relevant to a DSAR **must cooperate fully and promptly** with the DPO.
- Delays or failure to provide requested data may result in non-compliance with UK GDPR and could lead to regulatory action.

12. Format of Response

- Responses will be provided in a **structured, commonly used, and machine-readable format** (e.g., PDF, Excel).
- Where feasible, data will be provided electronically unless the requestor specifies otherwise.

13. Record Keeping

- All DSARs and related correspondence will be **logged and retained** for audit and compliance purposes. The DPO maintains this log.
- The log will include dates, nature of request, actions taken, and any exemptions or rejections applied.

Updates to document:

Review Date	Changes or Modifications	Approved by	Published

Unique Reference N°	Classification	Created	Version	Reviewed	Next Review
GDPR61	C1	12/2025	V1		12/2026