Data Subject Access Request (DSAR) Policy

Together

We are **Clemark Group**,

Registered in England & Wales under **Associate Enterprises Limited** and including all wholly owned subsidiaries. We also trade as Assent, Lorators, Clemark.

Our integrated management system covers the provision of consultancy, auditing, training, creative, technology and other professional services delivered in-person and remotely to ensuring the quality of products/services and the security of all information.

1. Introduction

This policy sets out how Clemark Group handles Data Subject Access Requests (“DSARs”) in accordance with:

- UK GDPR
- Data Protection Act 2018

It ensures that personal data is processed lawfully, transparently, and securely, and that individuals can exercise their rights effectively.

2. About Us

Associate Enterprises Limited also trades as Assent, Lorators, Clemark.

We provide consultancy, auditing, training, creative, and technology services.

For the purposes of this policy, we act as a **data controller** when processing personal data for our own business purposes.

3. Scope

This policy applies to:

- All personal data processed by us.
- All individuals whose personal data we hold, including:
    - Clients
    - Employees
    - Candidates
    - Suppliers
    - Website users
- All staff responsible for handling personal data
- All systems and records containing personal data

4. What is a Data Subject Access Request (DSAR)?

A DSAR is a request made by an individual (“data subject”) to:

- Obtain confirmation that their personal data is being processed

- Access their personal data
- Receive a copy of that data
- Understand how their data is used

Requests:

- Do **not** need to be in writing
- Do **not** need to mention “GDPR” or “DSAR”
- Can be made verbally or in any format

5. How to Submit a Request

DSARs can be submitted via:

📧 **Email:** desk@assent1.com

Staff must treat **any request for personal data** as a potential DSAR and escalate it.

6. Identity Verification

To protect personal data, we will:

- Take reasonable steps to verify the identity of the requestor
- Request additional information (e.g. ID or account details) where necessary
- Ensure verification is **proportionate to the sensitivity of the data**

The response timeframe will be paused until sufficient verification is received.

7. Handling Requests

Upon receipt of a DSAR, we will:

- Log the request promptly
- Escalate it to the Data Protection Officer within **1 working day**
- Acknowledge receipt where appropriate
- Identify relevant systems and data sources
- Retrieve relevant data
- Review and redact third-party or sensitive data where required

8. Response Timeframes

We will respond:

- Within **one month** of receiving the request

This period may be extended by up to **two further months** where:

- Requests are complex
- Multiple requests are received

If extended:

- The data subject will be informed within the initial one-month period
- Reasons for the delay will be explained

9. Information Provided

The response will include:

Confirmation and access:

- Confirmation that personal data is being processed
- A copy of the personal data

Mandatory disclosures:

- The purposes of processing
- The categories of personal data concerned
- The recipients or categories of recipients (including third parties)
- The retention period, or criteria used to determine it
- The lawful basis for processing
- The source of the data (where not collected directly)
- Details of any automated decision-making or profiling (if applicable)

Rights information:

- The right to rectification, erasure, or restriction
- The right to object to processing
- The right to data portability (where applicable)
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

---

10. Format of Response

Responses will:

- Be provided in a secure format
- Be clear and easy to understand
- Use plain language

Where a request is made electronically, the response will normally be provided electronically unless otherwise requested.

11. Fees

DSARs are generally **free of charge**.

A reasonable fee may be charged where:

- Requests are manifestly unfounded or excessive
- Additional copies are requested

12. Refusal or Restriction of Requests

We may refuse or restrict a request where:

- It is manifestly unfounded or excessive
- It involves third-party data that cannot be disclosed
- Legal exemptions apply

In such cases, we will:

- Provide a clear explanation
- Inform the individual of their right to complain to the ICO

13. Communication Standards

All communication will be:

- Clear and professional
- Transparent
- Free from unnecessary technical language

14. Record Keeping

We maintain records of all DSARs, including:

- Request details
- Identity verification steps

- Data provided
- Actions taken and timelines

15. Staff Responsibilities

All staff must:

- Recognise potential DSARs
- Escalate requests promptly
- Maintain confidentiality

Management must ensure:

- Requests are handled within required timeframes

The **Data Protection Lead** oversees compliance.