MGroupServices

DATA SUBJECT ACCESS REQUEST PROCEDURE

MGS-PRO-DP-003

Procedure Reference:	MGS-PRO-DP-003	**Version:**	v1.0
Issue Date:	12/03/2024	**Next Review Due:**	11/03/2025
Document Owner:	Ted Sefia, Group Data Protection Officer	**Document Scope:**	All Group companies

Issue, Review and Amendment

This Procedure shall be made available through M Group Services Intranet and its issue notified to relevant companies' employees through an internal memorandum or other appropriate form of communication.

The procedure shall be utilised by the businesses encompassed by the MGS scope.
Where revisions are required, they shall be made by replacement of the applicable page(s). An amended revision number and the date of revision shall identify each revised document; this shall be detailed within the document revision table below.

When changes affect a considerable number of pages, this document shall be re-issued/revised in its entirety, incorporating all previous revisions. A number shall identify issues and each issue shall cancel and replace all previous issues and revisions. Revisions shall be identified by a number and shall replace the previous revision.

Revisions shall be notified to relevant M Group Services companies' employees through an internal memorandum or other appropriate form of communication.

Document Reviews			
Date	**Version**	**Owned By**	**Changes**
12/03/2024	v1.0	Ted Sefia	No document

CONTENTS

1. Introduction

The Data Protection Act 2018 (DPA) provides individuals (known as the data subject) the right to access and receive a copy of their personal data, and other supplementary information. This is the “Right to Access” and it is important we have a process in place to make their data available upon request and within the ambits of the law.

This procedure defines the process to be followed when a request for access to personal data is received. A failure to comply with the provisions of the DPA in responding to requests may cause us to be in breach of the Data Protection Law and can lead to fines to the business. Individuals can face disciplinary action and/or be prosecuted where liability is established.

2. Roles, Responsibilities and Definitions

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Personal Data: any information in any format (emails, texts, videos, hardcopies etc.) relating to an identified or identifiable natural person i.e., a living individual *(see Data Protection Policy for further information on Personal Data).*

Data Subject Access Request: Also commonly referred to as subject access request or the acronyms DSAR or SAR (may be used interchangeably) is a request made by an individual to have a copy of the data we hold about them. A SAR can be made verbally or in writing (either via email, letter in the post or even on any of our social media platforms). A SAR is valid if it is clear that the individual is asking for their own personal data and they don’t need to use a specific form of words, refer to legislation or direct the request to a specific contact.

Personnel: All Personnel are responsible for reporting any subject access request received to the Group DPO. Any employee, worker, contractor, agency worker, consultant, director, member, and others who carry out work for or on behalf of any member of M Group Services Limited or any of its group companies is classed as Personnel.

Group Data Protection Officer (Group DPO) is responsible for ensuring that statutory and regulatory obligations with respect to the UK GDPR are adhered to across all the companies within the business hence it is imperative to report any SAR received to dp@mgroupservices.com.

3. Processing a Data Subject Access Request

Generally, request will be received from three classes of data subjects namely members of public, ex-staff and current staff.

3.1 What does a valid subject access request look like?

A valid SAR is one which the data subject states they wish to have information that relates to them. If in doubt, contact the Group DPO to confirm in the first instance.

It is quite possible that the first contact from the data subject will provide all the relevant information. In certain circumstances, we may need to request for further information to clarify the request and in other scenarios, we may need to verify the data subject. Please refer to the Appendices for standard template letters to use in requesting ID or further information in order to process a SAR.

Once we are confident that we have verified the data subject and sufficient information is received to process the SAR, we must process the SAR and should respond without delay and within one month of receipt of the SAR.

3.2 Identifying the location of information requested.

You must confirm if the requester is a member of public, an ex-staff or a current staff.

Member of public:
The request may come from a member of public for a number of reasons. Most likely it will be following work we have conducted for our contracts in the Energy or Water Divisions. It could be due to CCTVs we have or following a road traffic incident involving one of our vehicles.

Regardless, the request should be forwarded to the Group DPO to ascertain where the data resides and how to deal with the request.

Once the Group DPO has confirmed the location of the data and what team will need to produce the data requested, the request will be sent to the team to provide the information.

Ex-Staff and Existing Staff:
The request may come from an existing employee, an ex-employee or contingent worker. Where they make a request and the request does not identify what team they worked in, this should be clarified from the requester.

They are times an ex-employee/contingent worker may make a request via a solicitor. The information on the team will still be required and the solicitors making the request on behalf of the data subject will provide a written authority from the data subject without which we will not be able to address the request.

The request should be forwarded to the Group DPO to ascertain where the data resides and how to deal with the request.

Once the Group DPO has confirmed the location of the data and what team will need to produce the data requested, the request will be sent to the team(s) to provide the information.

A request may ask for personnel files only and this request should go to People Services. However, some requests will ask also for emails, Teams messages and/or minutes of meetings.
Treat as follows.

a) Personnel file – Send to Peoples Services to provide the data.
b) Emails and Teams Messages – Send to Group DPO who will retrieve the information via Littlefish. The Littlefish portal will need to be used in retrieving the information. Once received, all redactions will need to be made to exclude any information that relates to any other individual.
c) Memos, minutes of meetings – The line manager and HR Business Partner for the relevant team will confirm. All redactions will need to be made to exclude any information that relates to any other individual.

Update the DSAR Log

3.3 Retrieving the information requested.

Member of public:
Where the requester is a member of public, confirm the appropriate team the DSAR refers to. Send the request to the team with the specifics of what needs to be done and advise of the timeframe to respond to the DSAR. The case should be logged in the local team log to ensure corresponding requests have been received and actioned.

Once all data is collated, redact as appropriate and send to the manager or a senior member of the team to second check the redactions have been completed appropriately.

The manager or senior individual in that team will second check the redactions and give approval to deliver to requester before it is sent out to the requester. The Group DPO must be advised the response has been done so the case can be closed in the DSAR Log.

Monthly checks of the DSAR logs should be conducted between the teams and Group DPO to check no DSAR has been missed.

Ex-Staff and Existing Staff
Where the information requested is for Personnel file, the request must be sent to People Services to retrieve the information. People Services may need more information where they are unable to identify the individual, for instance where the NI Number does not match the name. Request for the relevant information from the data subject and advise the timeframe will reset once full identification has been completed.

In the case where identification is confirmed, advise People Services of the timeframe to respond to the DSAR. Once received from People Services, proceed with appropriate redactions before sending to Group DPO to deliver to requester from DP mailbox.

Close in the DSAR Log.

Where the request is for emails and Teams messages, the Group DPO will raise a “Confidential Request” with IT ServiceDesk.

IT ServiceDesk have a 3 to 5 days Service Level Agreement and will conduct the search on

Mimecast Archive. The results of the search will be dropped in the OneDrive of the individual designated to review and redact.

The team member doing the redactions will complete the redactions and send to their line manager of a senior member of the team to second check for accuracy. Once confirmed as accurate redaction, the redacted information will be sent to Group DPO to review and deliver from DP mailbox.

If the request is for both personnel files and emails/Teams' messages, the same processes above will apply, however, in this case the data will only be sent together when both redactions (personnel file and messages) have been received.

Close in the DSAR Log.

EXAMPLE HR SAR PROCESS – MES HR