

1.0 Scope

The General Data Protection Regulations provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This procedure covers rights 3 - 7. (Right 1 to be informed is covered by our published Privacy notice and consultation document template. The access right is covered by our SAR process see IMPR04.

2.0 Responsibility and definitions

Information Access Manager – responsible for handling data subject rights requests.

Data Protection Officer – deputy for Information Access Manager and has responsibility for compliance with Data Protection Legislation.

3.0 Procedure

- 3.1 All requests should be directed to the Information Access Manager or Data Protection Officer in their absence
- 3.2 Requests should be logged on the Subject Access Request (SAR) tracking sheet (found in folder 19871455). A ref. number should be allocated and case folder created in SAR cases folder 19395791).
- 3.3 The identity of the applicant must be verified before any action is taken, refer to SAR process IMPR04 for verification process.
- 3.4 All requests relating to subject rights must be dealt with promptly and be completed within **one month from receipt**.

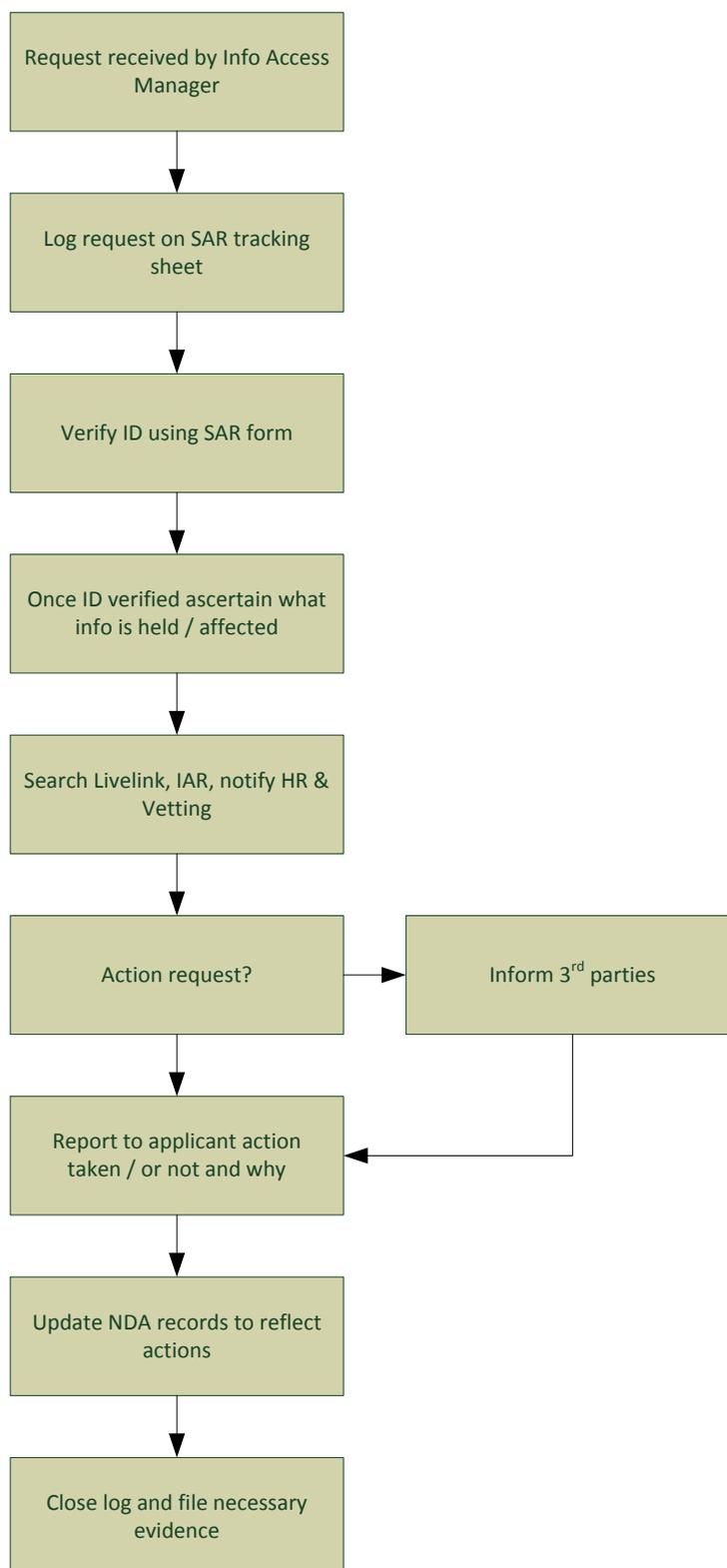
This can be extended by two months where the request is complex or we receive a number of requests from the same applicant. If this is the case the applicant must be informed of the delay within one month of the receipt of the request and we must explain to them why the extension is necessary.

We should keep the applicant up to date re. progress in any case of delay.

Procedure for handling GDPR Data Subject Rights

Doc No IMPR08

Rev 1
Date Feb 2018



3.5 Once ID has been verified, all personal data affected by the request must be identified and the request actioned if appropriate – refer to appendix A. re complying with each specific right to understand when we may or may not be required to take action.

Relevant data can be identified via the Info Asset Register, Livelink search, data processing record spreadsheets. HR and Vetting must be notified as appropriate re. requests affecting data they hold.

3.6 If we have disclosed the personal data in question to third parties, we must inform them re. any necessary action they must take in response to the request.

We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

3.7 We should inform the applicant what action we have taken. If we determine not to take any action in response to a request, we must explain why to the individual, informing them of their right to complain to the ICO.

3.8 Once the request has been dealt with all relevant evidence of compliance should be added to the case file and the SAR tracking sheet updated.

Appendix A. Handling specific rights requests

Right 3. Request for rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

Right 4. Erasure

The right to erasure is also known as ‘the right to be forgotten’.

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

Procedure for handling GDPR Data Subject Rights

Doc No IMPR08

Rev 1
Date Feb 2018

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

If we have disclosed the personal data in question to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Right 5. Restricting processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.

We will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Procedure for handling GDPR Data Subject Rights

Doc No IMPR08

Rev 1
Date Feb 2018

Right 6. Data portability

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

We must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

Records Table

Record Description	Record Owner	Retention Time	Record Format Electronic/Hardcopy	Record Location
	Judith Griffin		Electronic	