Subject Access Request policy

Please refer to our 'GDPR Overview' document for definition of terms, outlines of policies and the context in which this policy is set.

This document is part of our Data Protection Policy Portfolio and is to be used in conjunction with the other documents.

1 – Introduction

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Our business must comply with the requirements of the General Data Protection Regulations (GDPR) and we must be able to demonstrate compliance to the Information Commissioner's Office (ICO).

2 – Responsibility

Our Data Protection Manager is responsible for the handling of Subject Access Requests (SAR) in our business.

Their duties include but are not limited to:

- Log the receipt and fulfilment of all requests received from a requestor to see their personal information.
- Acknowledge the SAR.
- Verify the identity of any person making a SAR.
- Maintain a database on the volume of requests and compliance against the statutory timescale.
- Verify whether we are the controller of the requestor's personal data.
- Check if we are not a controller, but rather a processor. If so, inform the data subject and refer them to the actual controller. This needs to be recorded in writing.
- Where applicable, decide if a request is excessive, unfounded or repetitive and communicate this to the requestor.
- Decide if an exemption applies (Section 4).
- If a SAR is submitted in electronic form, any information should preferably be provided by electronic means as well.

3 – Verification of requestors identity

The requestor must supply valid evidence to prove their identity.

We may verify the requestor's identity either through a phone call where we ask questions that only the requestor will know the answers to or by requesting forms of identification.

The following forms of identification will be allowed:

- Current UK/EEA passport
- UK Driving licence

4 – Processing a SAR

Our aim is to determine what information the requestor is asking for. If the request is not clear, or where we process a large quantity of information about an individual, the GDPR

permits us to ask the individual to specify the information the request relates to. Where this applies, we will proceed with a request for clarification.

We must verify whether we process the data requested. If we do not process any such data, we must inform the data subject accordingly.

We must respond to the data subject within 30 days of receiving the request as valid. This is a requirement under the GDPR.

We will locate and supply all data relating to the SAR, this will be a full exhaustive search of records, this may include but not limited to; emails, documents, spreadsheets, databases and paper records.

The data will then be reviewed to ensure there is no data relating to other data subjects. If there is data relating to another data subject we will either gain their consent to the data be released, or redact the data accordingly.

All the information that has been requested must be provided unless an exemption can be applied (see below). Information must be supplied in an intelligible form and we will explain acronyms, codes or complex terms.

There will be no charge to the requestor, unless there are excessive and/or multiple request. The Data Protection Manager will determine a 'reasonable fee' for excessive and/or multiple requests, which will be based on our administrative cost of providing the information.

Exemptions

The following exemptions will allow us not to undertake a SAR, the requestor will be notified of the reason for the denial of the request:

- **Excessive, unfounded or repetitive requests** – where a SAR is excessive, unfounded or repetitive we may refuse the SAR or charge a reasonable fee.
- **Complex requests** – A SAR is to responded to within 30 days under GDPR, if a SAR is complex and more time is required to respond, we are allowed a two month extension, as long as this is communicated to the requestor within 30 days of their SAR.

5 – Response to the SAR

After processing the SAR, our response to the requestor should include:

- The purpose(s) the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third party countries or international organisations, including any appropriate safeguards for transfer of data;
- The envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with the ICO;
- If the data has not been collected from the data subject: the source of such data;

- The existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the requestor.

6 – Complaints

If a requestor is not happy with the results of a SAR they may make a complaint to our Data Protection Manager, Jonathan Mackie at Jonathan.Mackie@nrb.co.uk. If the requestor is still not satisfied they may complain to the ICO at www.ico.org.uk.