Data Subject Rights Request Policy

1. Scope

* 1. Under the UK General Data Protection Regulation, all individuals have rights over their data and are entitled to request information from organisations about how they process their data, including access to or a copy of any personal data. If an individual contacts us requesting this information, this is called a subject access request.
  2. All individuals who are the subject of data held by us are entitled to:
     1. information on how their personal data is processed;
     2. **access to and copies of** their personal data;
     3. request incorrect data be rectified;
     4. **erasure** of their data in certain circumstances;
     5. have the processing of their data **restricted;**
     6. be provided their data in a **portable** format;
     7. **object** to the processing of their personal data for any purpose; and
     8. object to their personal data being subjected to a**utomated decision-making or profiling.**
  3. We accept subject access requests in any format, be it electronically, in writing, or in direct conversation with staff. Data subjects should be encouraged to avail of the self-service form on our website.
  4. Where made in person or in writing, the employee who receives the request should complete a request through the same self-service tool to ensure this is logged appropriately.
  5. All information under a request will be provided free of charge. However, where following a request the data subject requests further copies of personal data, a reasonable sum may be charged to cover administrative costs of fulfilling the request.
  6. The Data Protection Lead, Alex Craig, the Head of Knowledge and Risk and the COLP are responsible for responding to and managing all requests under this policy and may allocate these duties from time to time as necessary.

1. Process for Response
   1. All rights requests must be dealt with and responded to **without undue delay**, and in any event within **1 calendar month**. The following general process must be followed.
      1. Immediately record the contact and notify the Data Protection Lead who will take responsibility for ensuring that the request is actioned.
      2. The Data Protection Lead will confirm the identity of the requestor by requesting photographic identification before sharing any information. **Only a current valid driving license or passport will be accepted.**
      3. Where confirming the identity of the requestor proves impossible, the Data Protection Lead may refuse to comply with the request:
         1. where a request is made by a third-party on behalf of a data subject, in addition to valid ID the requestor must also provide written confirmation of consent of the data subject to make the request; or
         2. where the requestor does not provide valid ID, the Data Protection Lead will treat the request as abandoned and refuse to comply with the request.
      4. The Data Protection Lead will then consider the request, checking if there are any exemptions which prevent us complying with the request. Where it is clear an exemption applies to the request meaning the request must be refused, the Data Protection Lead will communicate this to the requestor and document the refusal in the **Subject Access Request Register**. The request may also be refused where the Data Protection Lead considers the request to be manifestly excessive or unreasonable. If refused on this basis the Data Protection Lead must record their reasoning in the Subject Access Request Register.
      5. The Data Protection Lead will complete and provide a full response or communicate a refusal without delay and within one calendar month of receipt of request. Where a request is particularly complex, the deadline may be extended by a further 2 calendar months. Where this is necessary, the Data Protection Lead will communicate this to the subject within 1 month of receipt of the request along with the reasons for the delay.
      6. The Data Protection Lead will monitor our performance in responding to subject access requests within the one-month limit and will provide the Senior Management Team with a monthly report.
2. Form of Response
   1. When responding to subject access requests, the Data Protection Lead must ensure:
      1. all responses are given in clear, concise, transparent and intelligible language, in a form which is easily accessible to the data subject;
      2. in the event that documentation is to be provided to the data subject, this must be provided in a **secure format.** Where possible this should be by way of secure self-service option, such as OneDrive or Firmex. In the alternative, password protected documents may be sent by email; and
      3. where the request is made by electronic means, the response should likewise be via electronic means in a commonly used and accessible format, **unless otherwise specified by the data subject**.
3. Data Subject Rights: Specific Steps

In addition to the general response process outlined above, further specific steps must be adhered to when responding to requests under each data subject right outlined in UK GDPR.

* 1. Right of Access

The Data Protection Lead should follow the process above for managing requests under this right. Under Article 15 UK GDPR, when responding to the data subject the following information must also be provided:

* + 1. the purposes of the processing;
    2. the categories of data concerned;
    3. the recipients or categories of recipient to whom the data have been or will be disclosed, in particular recipients in third countries or international organisations;
    4. where possible, the envisaged period for which the data will be stored, or, if not possible, the criteria used to determine that period;
    5. the existence of the right to request from the controller rectification or erasure of data or restriction of processing of data concerning the data subject or to object to such processing;
    6. the right to lodge a complaint to us and, in the event you are not happy with the outcome of your complaint, the right to lodge a complaint with the Information Commission; and
    7. where the data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  1. Right of Rectification
     1. On receipt of a request under this right, the Data Protection Lead will follow the general response process outlined in section 2. At step 4 however, the Data Protection Lead will instead:
        1. take into account any evidence provided by the data subject and take steps to assess the accuracy of the data and rectify, complete or add a supplementary statement if necessary; and
        2. where the Data Protection Lead is satisfied the disputed data is in fact accurate, explain this to the data subject and record any dispute the Subject Access Request Register.
     2. At step 5, the Data Protection Lead should instead:
        1. as far as reasonably possible communicate any rectification carried out to each recipient to whom the data have been disclosed; and
        2. inform the data subject of any other third parties the data has been disclosed to if asked.
  2. Right of Erasure
     1. Where a right of erasure request is received, the Data Protection Lead will arrange the immediate deletion of the data where:
        1. the data is no longer necessary for the purposes for which it was originally collected;
        2. the data subject has withdrawn consent for the processing and no other lawful basis remains;
        3. the data subject objects to processing based on public task or legitimate interest and no other overriding interests remains, or objects to processing based on direct marketing;
        4. the processing was unlawful;
        5. erasure is required to fulfil a legal obligation; or
        6. the data have been collected in relation to the offer of information society services referred to in Article 8(1).
     2. The Data Protection Lead will indicate a refusal where:
        1. we process the data in the interests of freedom of expression/information;
        2. the processing is required under domestic law for the performance of a public task;
        3. the processing is for archiving purposes in the public interest per Article 89(1) UK GDPR; or
        4. the processing is necessary to establish, defend or exercise legal claims.
     3. Where a deletion requestion is accepted, the Data Protection Lead will arrange deletion from all systems, including live, backup and archival systems.
     4. The Data Protection Lead will then provide confirmation to the data subject. Where this is not possible this should be documented in the Subject Access Request Register.
  3. Right of Restriction of Processing
     1. The Data Protection Lead will only agree to a restriction of data request where:
        1. the accuracy of the data on the data subject is contested by the data subject, for a period enabling the organisation to verify the accuracy of data;
        2. the processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead;
        3. the organisation no longer needs the data for the purposes of the Processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
        4. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the organisation override those of the data subject.
     2. The Data Protection Lead may refuse the restriction applies, including:
        1. where the data subject consents to the processing;
        2. the processing is for the establishment exercise or defence of legal claims;
        3. the processing is for the protection of the rights of another; or
        4. the processing is for an important reason in the public interest.
     3. On restricting the data, the Data Protection Lead must communicate the restriction requirement to any third parties in receipt of the data, unless this proves impossible or an exemption applies. Where this cannot be communicated this must be documented in the Subject Access Request Register.
     4. The Data Protection Lead must further inform the data subject of any third parties in receipt of the data, and if/when the restriction is to be lifted.
  4. Right to Portability
     1. Where we process data based on the consent or contract with the data subject and the processing is by automated means, the Data Protection Lead will arrange for the data subject to provided their data in a structured, commonly used and machine-readable format.
     2. Where feasible, the Data Protection Lead will also transmit the data to another organisation of the data subject’s choosing.
  5. Right to Object
     1. Where an objection is made and the processing is based on legitimate interests or public task, we will immediately cease the processing of the disputed data while the objection is being dealt with.
     2. Where an objection is to processing for the purposes of direct marketing we must cease all processing without exception.
     3. Where the Data Protection Lead identifies that there are compelling overriding legitimate grounds for the processing, or the processing is necessary for the establishment, exercise or defence of legal claims, the request will be informed that an exemption applies.
  6. Right not to be subjected to automated processing
     1. The UK GDPR places a general prohibition on wholly automated processing of personal data, including profiling, which produces legal or similarly significant effects on the data subject.
     2. The prohibition does not apply to automated processing which:
        1. is necessary for entering into, or performance of, a contract between the data subject and an organisation;
        2. is required or authorised by domestic law which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
        3. is based on the data subject’s explicit consent.
     3. If and where we utilise automated processing under the above exemptions, we will:
        1. offer data subjects the right to human intervention by a member of the firm;
        2. enable the data subject to express their point of view on decisions based on automated processing or profiling; and
        3. enable the data subject to contest any decision based on automated processes.

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Comments** | **Reviewed by** | **Date of next review** |
| 22/07/2024 | Implemented policy | Data Protection Lead | 22/07/2025 |
| 23/07/2025 | Reviewed, updated and added version control | Data Protection Lead | 23/07/2026 |