

Date: 1st May 2018

Subject Access Request Response Procedure

Subject Access Request Response Procedure

1. About this Procedure

- 1.1. Data subjects have certain rights in respect of their personal data. When we process a data subjects' personal data, we shall respect those rights. These procedures provide a framework for responding to requests to exercise those rights. It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.
- 1.2. For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.
- 1.3. These procedures only apply to data subjects whose personal data we process.
- 1.4. A Data Subject is 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.
- 1.5. Data Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
- 1.6. The DPO is responsible for this procedure and any questions relating to SAR's should be directed to them.
- 1.7. This procedure applies to all staff and contractors but does not form part of your contract with the company or your contract of employment. The company may amend this procedure from time to time without consultation.
- 1.8. Failure to follow this procedure may lead to disciplinary action including summary dismissal.

2. RESPONDING TO REQUESTS TO ACCESS PERSONAL DATA

- 2.1. Data subjects have the right to request access to their personal data that is being processed by us. Such requests are called subject access requests (**SARs**). When a

person makes a SAR we shall take the following steps:

- 2.1.1. log the date when the request was received (to ensure that the relevant timeframe of **one month** for responding to the request is met);
 - 2.1.2. inform the General Manager of the request and complete the initial response letter in Appendix 1;
 - 2.1.3. confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity. We should not release information without confirming the person making the request, is the data subject;
 - 2.1.4. search databases, systems, applications and other places where the personal data that are the subject of the request may be held; and
 - 2.1.5. confirm to the data subject whether or not their personal data is being processed by us.
- 2.2. If personal data of the data subject is being processed, we shall confirm our response in the letter in Appendix 2 and provide the person with the following information in a concise, clear, understandable and easily accessible form, using plain language, in writing or by other (including electronic) means:
- 2.2.1. the purposes of the processing;
 - 2.2.2. the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);
 - 2.2.3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers) if applicable;
 - 2.2.4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - 2.2.5. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;
 - 2.2.6. the right to lodge a complaint with the Information Commissioner's Office (ICO);
 - 2.2.7. where the personal data are not collected from the data subject, any available information as to their source;

- 2.2.8. no automated decision making is undertaken by the company.
- 2.2.9. no personal data are transferred outside the EU]
- 2.3. We shall also, unless there is an exemption (see *Paragraph 9* below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request.
- 2.4. If the request is complex, or there are a number of requests, we may extend the period for responding by a further **two** months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.
- 2.5. **Before** providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact (delete) the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.
- 2.6. If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.
- 2.7. If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

3. RESPONDING TO REQUESTS TO RECTIFY PERSONAL DATA

- 3.1. Data subjects have the right to have their inaccurate personal data corrected. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), rectify the personal data without undue delay.
- 3.2. We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject

requests it.

4. RESPONDING TO REQUESTS FOR THE ERASURE OF PERSONAL DATA

- 4.1. Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), erase the personal data without undue delay if:
 - 4.1.1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - 4.1.2. the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;
 - 4.1.3. the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;
 - 4.1.4. the data subject objects to the processing of their personal data for direct marketing purposes;
 - 4.1.5. the personal data have been unlawfully processed;
 - 4.1.6. the personal data have to be erased for compliance with a legal obligation to which we are subject; or
 - 4.1.7. the personal data have been collected in relation to the offer of e-commerce or other online services.
- 4.2. When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see *Paragraph 4.5* and *Paragraph 9* below), take the following steps:
 - 4.2.1. log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
 - 4.2.2. inform the General Manager and complete the initial response letter in Appendix 1;

- 4.2.3. confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this. This is particularly important in requests for erasure;
- 4.2.4. search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request.
- 4.2.5. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;
- 4.2.6. where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and
- 4.2.7. communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.
- 4.3. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.
- 4.4. If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.
- 4.5. In addition to the exemptions in *Paragraph 9* below, we can also refuse to erase the personal data to the extent processing is necessary:
 - 4.5.1. for exercising the right of freedom of expression and information;
 - 4.5.2. for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;
 - 4.5.3. for reasons of public interest in the area of public health;
 - 4.5.4. for archiving purposes in the public interest, scientific or historical research

purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
or

4.5.5. for the establishment, exercise or defence of legal claims.

5. RESPONDENT TO REQUESTS TO RESTRICT THE PROCESSING OF PERSONAL DATA

5.1. Data subjects have the right, unless there is an exemption (see *Paragraph 9* below), to restrict the processing of their personal data if:

5.1.1. the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

5.1.2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

5.1.3. we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and

5.1.4. the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

5.2. Where processing has been restricted, we shall only process the personal data (excluding storing them):

5.2.1. with the data subject's consent;

5.2.2. for the establishment, exercise or defence of legal claims;

5.2.3. for the protection of the rights of another person; or

5.2.4. for reasons of important public interest.

5.3. Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

5.4. We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been or will be, disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those

recipients if the data subject requests it.

6. **RESPONDING TO REQUESTS FOR THE PORTABILITY OF PERSONAL DATA**

6.1. Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), provide the personal data without undue delay if:

6.1.1. the legal basis for the processing of the personal data is consent or pursuant to a contract; and

6.1.2. our processing of those data is automated.

6.2. When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps:

6.2.1. log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

6.2.2. Inform the General Manager and complete the initial response letter in Appendix 1;

6.2.3. confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity; and

6.2.4. search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request.

6.2.5. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

6.3. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of

providing or transmitting the personal data, or refuse to act on the request.

- 6.4. If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

7. RESPONDING TO OBJECTIONS TO THE PROCESSING OF PERSONAL DATA

- 7.1. Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:

7.1.1. can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

7.1.2. are processing the personal data for the establishment, exercise or defence of legal claims.

- 7.2. Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

- 7.3. Where such an objection is made, we shall, unless there is an exemption (see *Paragraph 9* below), no longer process a data subject's personal data.

- 7.4. Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

8. RESPONDING TO REQUESTS NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

- 8.1. Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or also significantly affects them.

- 8.2. Where such a request is made, we shall confirm that we do not make any decisions based on automated decision making.

8.2.1. is necessary for entering into, or the performance of, a contract between us and the

data subject;

8.2.2. is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

8.2.3. is based on the data subject's explicit consent.

8.3. If the decision falls within *Paragraph 8.1.1* or *Paragraph 8.1.2*, we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

9. **EXEMPTIONS**

9.1. Before responding to any request we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

9.1.1. national security;

9.1.2. defence;

9.1.3. public security;

9.1.4. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

9.1.5. other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

9.1.6. the protection of judicial independence and judicial proceedings;

9.1.7. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

9.1.8. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in *Paragraph 9.1.1-9.1.5* and *Paragraph 9.1.7* above;

9.1.9. the protection of the data subject or the rights and freedoms of others; or

9.1.10. the enforcement of civil law claims.

9.2. If at any time you are unsure how to deal with a SAR, you must take no further action until you have spoken to the DPO/M or have reported your concerns to your line manager who will seek guidance from the DPO/M.