SUBJECT ACCESS REQUEST GUIDANCE

1. DATA SUBJECTS' RIGHTS OF ACCESS UNDER THE GENERAL DATA PROTECTION 2016

1.1 Under the General Data Protection Regulation 2016 ('GDPR') a person will have the right to ask an organisation to confirm whether or not it is processing any of their personal data.

1.2 Where that is the case they will have a right of access to that data, and to other supplementary information concerning their rights.

1.3 The supplementary information an organisation must provide includes the following:

1.3.1 the purposes of processing;

1.3.2 the categories of data processed;

1.3.3 the recipients or categories of recipients;

1.3.4 the retention period or criteria used to determine this period;

1.3.5 the individual's rights under the GDPR (e.g. right to rectification or erasure, to restrict processing or object to processing and lodge a complaint with the supervising authority)

1.3.6 information regarding the source of the data (if not collected by the organisation); and

1.3.7 any automated decision taking undertaken.

1.4 Individuals are allowed this access so that they are aware of and can verify the lawfulness of the processing of their personal data.

1.5 Unless one of the exceptions applies (see sections 4 and 5) you must provide a copy of the personal data that you hold upon request.

2. FEES

2.1 You must provide a copy of the personal data free of charge. Under the Data Protection Act 1998 ('DPA 1998') organisations were able to charge a £10 fee. This is no longer the case.

2.2 You are, however, able to charge a reasonable fee when a request is 'manifestly unfounded or excessive', particularly if it is repetitive.

2.3 You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

2.4 The fee must be based on the administrative cost of providing the information.

3. TIME LIMITS TO RESPOND

3.1 The information requested must be provided without delay and in any case within one month of receipt of the request. Please note that this is less time than allowed for under the DPA 1998 which was forty days.

3.2 You will be able to extend the one-month time limit by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of receiving the request that you require an extension and explain why it is necessary.

3.3 Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to. The one-month deadline to respond to the request does not begin to run until you have received the further information required to enable you to deal with the request.

3.4 You must use reasonable means to verify the identity of the person making the request. If you require further information to verify their identity, then the one-month deadline does not begin to run until you have received the required information.

4. WHEN YOU CAN REFUSE TO RESPOND TO A REQUEST

4.1 Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you are able to charge a reasonable fee for providing the information **OR** refuse to respond. You will need to be able to provide evidence of how you reached this conclusion. The Information Commissioner's Office (ICO) should provide further guidance on this shortly. Please check the ICO website for updates.

4.2 You can also refuse to respond to a request where one of the exemptions apply (see section 5 below for further details).

4.3 Where you refuse to respond to a request, you must do so without undue delay and at the latest within one month. Additionally, you must explain the reasons for the refusal and inform the individual of their right to complain to the supervisory authority (usually the ICO) and to a judicial remedy.

4.4 You should keep a record of your decision to refuse to respond to a request including your justifications for taking such action.

5. EXEMPTIONS

5.1 The GDPR are European Regulations, but they allow individual member states to pass their own laws to restrict the scope of a person's right to access their data. The UK government recently published a draft Data Protection Bill, which when it is finalised will supplement the GDPR. The draft bill replicates many of the exemptions which already apply under the Data Protection Act 1998.

5.2 Some of the exemptions will only be applicable to certain industries or public bodies, but there are broader exemptions which may be applicable to many different types of organisation.

5.3 Under the draft bill an individual's rights to access their data under the GDPR do not apply to:

5.3.1 personal data which if disclosed could compromise national security;

5.3.2 information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;

5.3.3 situations where complying with a request would lead to self-incrimination of an offence;

5.3.4 data that is processed under an act of parliament or by the government in order to secure the health and safety of persons at work;

5.3.5 confidential references given by the data controller in confidence for the purposes of an individual's education, training or employment, or the provision of a service by them;

5.3.6 management information, i.e. personal data that is processed by the data controller for the purposes of management forecasting or management planning;

5.3.7 records of any negotiations with the requester, to the extent that releasing the information would prejudice those negotiations; and

5.3.8 information that is available to the public.

5.4 There are also exemptions for specific categories of data, including:

5.4.1 exemptions for reasons of freedom of expression and information – these are connected with journalism, literature and art;

5.4.2 data processed only for the purposes of research, history and statistics. We can provide additional guidance if you think this may apply; and

5.4.3 information connected with a person's health, education and social work records.

5.5 One of the main exemptions that organisations will be able to rely on is a restriction based on protecting the rights of others. You are not obliged to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information. This exemption does **not** apply, however, where the other individual has consented or it is reasonable to disclose the information without the consent of the other individual.

5.6 In deciding whether it is reasonable to disclose the information without the consent of the other person you need to take into account:

5.6.1 the type of information that would be disclosed;

5.6.2 any duty of confidentiality owed to the other person;

5.6.3 any steps you have taken to get the consent of the other person;

5.6.4 whether the other individual is capable of giving consent; and

5.6.5 any express refusal of the other person.

Note: We can provide additional guidance if you believe that any of these exemptions may apply in relation to a subject access request you have received, and we will provide further guidance once the draft Data Protection Bill is finalised.

6. MISCELLANEOUS

6.1 Where a request has been made by email you should respond by email unless the data subject has requested you respond in a different format. You could send the data subject a scanned pdf copy of your letter response (using our template letter as a basis) or use the text of our template letter as an email response.

6.2 Where possible, you should be able to provide remote access to a secure self-service system providing the individual with direct access to their personal data. It is understood, however, that this will not be appropriate for all organisations.

6.3 The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

6.4 You can supply the supplementary information referred to in section 1 above by re-stating the information contained in your privacy notice and/or privacy policies provided to the particular category of data subject or attach copies of the notices/policy to your response.

7. DATA PORTABILITY

7.1 In addition to subject access rights, data subjects also have a right to 'data portability' under the GDPR.

7.2 This allows data subjects to require organisations to provide them with their personal data they have provided to the organisation in a commonly used and machine readable format and, if required, transmit it to a third party.

7.3 The aim of the right is to support user choice, user control and consumer empowerment.

7.4 Unlike the subject access right, data portability does not apply to all personal data held by the organisation concerning the data subject. Data portability rights are only available where:

7.4.1 the data is automated data (paper files are not included);

7.4.2 the person's data has to be actively provided by the data subject; and

7.4.3 the personal data is processed by the organisation with the data subject's consent or pursuant to a contract with him/her.

Time Limits to respond to a data portability request

7.5 Organisations must respond to requests for data portability without undue delay and within one month. Where you are unsure of the identity of the individual making the request you can request further information to verify their identity before you respond to the request.

7.6 The one month deadline can be extended by two months where the request is complex or a number of requests have been received.

7.7 Organisations must inform the data subject within one month of receipt of the request and explain why the extension is necessary.

7.8 Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervising authority (usually the ICO) and a judicial remedy without undue delay and within one month of receiving the request. The information must be provided free of charge unless you can demonstrate that the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

8. TEMPLATE RESPONSE LETTERS

Attached to this guidance note are two template letters. One can be used where you refuse to respond to a subject access request, require further information to be able to respond to the request or require an extension to the period of time in which to respond. The other template letter can be used when responding to a subject access request by providing the information sought by the individual.