TORQUELAW

DATA SUBJECT ACCESS REQUESTS

Under the GDPR and Data Protection Act 2018, individuals (employees) have the right to find out what personal data is held by data controllers (employers) about them. This right is known as subject access. Subject access is most often used by individuals wanting to see a copy of information an organisation holds about them. The right also extends to the right to be told whether personal data is being processed and the reasons for that processing. The right is to see one's own personal data; it is not a right to receive copy documents.

1. What is personal data?

- Information that relates to an identified or identifiable individual. Anonymised information is, by definition, outside the scope of any DSAR.
- To be personal data, the information must **relate to** that individual i.e. it must concern the individual in some way rather than simply identify them (e.g. being sent an email by copy is insufficient to amount to personal data).
- If data is to be used to make or influence a decision about an individual, then it is personal data even if they themselves are not identified in or identifiable from the data.

2. Can we charge a fee?

- In most cases you cannot charge a fee. Where the request is manifestly unfounded, excessive or a repeat request you can charge a reasonable fee for the administrative costs of compliance (or refuse to comply with it altogether).
- When determining a reasonable fee, you can take into account the administrative costs of: assessing whether or not you are 'processing' the information; locating and extracting the information; providing a copy of the information; and communicating the response to the individual.
- A reasonable fee may include the costs of staff time (charged at a reasonable hourly rate), copying, postage and other expenses involved in transferring the data to the individual, including the costs of envelopes, USB devices etc.
- To ensure that any fees are charged in a reasonable, proportionate and consistent manner it is advisable to establish a set of criteria for charging fees, whilst remembering that you must be able to justify the costs in the event that an individual complains to the ICO.

3. What is the timeframe for a response?

- A response to a valid request must be sent without undue delay and at the latest within one month of receipt.
- You can extend the timeframe for a response by a further 2 months (so up to 3 months in total) if the request is complex or you have received a number of requests from the individual data subject. Notification of an extension should be sent within the first month of receiving the request and include an explanation of the reason for the extension.

4. Stopping the clock in order to request clarification

- You may ask an individual to specify the information or processing activities their request relates to before responding to the request if it is genuinely required in order to respond to a DSAR and you process a large amount of information about the individual. The one month time limit for responding to the request is then paused until you receive clarification and this is referred to as 'stopping the clock'.
- If clarification is needed, you should:
    - request clarification without undue delay after receiving the request;
    - ask the individual to provide additional details about the information they want to receive (e.g. the context in which their information has been processed and the likely dates of the processing);
    - explain to the individual that the clock stops on the date of the clarification request and resumes on the date the individual responds;
    - specify whether the individual needs to respond by a certain date; and
    - where possible, respond to the individual in the same format they made the DSAR.
- As mentioned, you may be able to extend the time limit by two months if the request is complex or the individual has made a number of requests. However, a request is not complex just because you need to seek clarification.

5. What if the data includes information about other people?

- You do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if that person has consented to the disclosure or it is reasonable to proceed without that individual's consent.
- In determining if it is reasonable to disclose the 3rd party information you must take account of the type of information to be disclosed, the duty of confidentiality you owe to that person and/or any express refusal of consent.
- One option is to redact 3rd party information to ensure confidentiality is preserved. Another alternative would be to disclose the information in tabular form.

6. What are our obligations so far as undertaking a search for personal data?

- The requirement is for each 'data controller' to take reasonable steps to comply with the request, which includes undertaking a reasonable search of their systems (i.e. those within your control) for any personal data which comes within the scope of the request. Only if compliance would put you / your organisation to disproportionate cost or effort, can you refuse to provide the information.
- Unstructured paper records are not within scope; manual records must be stored as part of a relevant filing system and be capable of being searched against to be within scope.
- The search for personal data on the data controller's systems should include information stored in electronic form, much of which should be capable of being found and retrieved easily using search terms. Electronic form is not confined to work emails but would include word documents, spreadsheets, text and instant messages created and/or communicated via work mobile computers/phones. Where there is an expectation and/or practice that work-related emails containing personal data will be sent via personal email accounts, these addresses should be searched against too.
- A reasonable search of your electronic email systems would extend to deleted folders on a 'live' system, but not emails which have been removed or have been archived and are therefore not as easy to retrieve.

7. Can we refuse to comply with a DSAR?

- You can refuse to comply with a DSAR if it is manifestly unfounded or excessive, including if the request is repetitive in nature. You should be prepared to justify your decision to the individual and the ICO.
- A request may be manifestly unfounded if the individual clearly has no intention to exercise their right of access, or if the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption.
- To determine whether a request is manifestly excessive you need to consider whether it is clearly or obviously unreasonable. You should base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.
- You must consider each request individually when determining whether a request is manifestly unfounded or excessive and you should not presume that it is just because an individual has previously submitted a manifestly unfounded or excessive request.

8. What exemptions apply?

- In addition to the restriction on the disclosure of 3rd party data (see above), the DPA 2018 includes the following exemptions restricting the disclosure of information.
    - **Management forecasting or management planning**: it is possible to withhold management information which is likely, if disclosed, to prejudice the business or other activity of the organisation. The specific example given in the ICO's Code of Practice is the non-disclosure of information relating to a planned re-organisation in advance of it being communicated.
    - **Negotiations with the requester**: personal data which consists of a record of your intentions in negotiations with the individual is exempt from disclosure if it would be likely to prejudice those negotiations.
    - **Legal advice and proceedings**: personal data which is subject to legal professional privilege (which breaks down into legal advice privilege and litigation privilege). In broad terms, legal advice privilege applies to confidential communications between client and legal adviser; litigation privilege applies to confidential communications between client, professional legal adviser or a third party, where litigation is contemplated or in progress.
- It is not legitimate to refuse to comply with a DSAR simply because the requester is contemplating or has commenced legal proceedings. That there may be a 'collateral' purpose to the request (i.e. other than seeking to check or correct personal data) is not relevant so far as the ICO is concerned.

9. What are the consequences of non-compliance?

- The ICO has enforcement powers to compel an organisation to take steps to comply with data protection principles and law, and in extreme cases can fine organisations for serious breaches which are likely to cause substantial damage or distress. The ICO has no power to award compensation to individuals.
- The ICO will not necessarily serve an enforcement notice simply because an organisation has failed to comply with an access request. It is only where the ICO considers the contravention to have caused, or be likely to cause, damage or distress that an enforcement notice would be served. Failure to comply with an enforcement notice is a criminal offence.

November 2020