**How to manage a Subject Access request.**

**Right of Access**

Under the Data Protection Act 2018, individuals have rights of access in relation to the personal data that you hold on them. A request for such information is called a ‘subject access request’. The right permits individuals to see the information that you process about them, not to actually receive a copy of the information. However, it is likely that the easiest way to allow the individual to see the information is by sending a copy of it to the individual.

A subject access request must be in relation to an individual’s personal data, including special categories of personal data. Where a request is made for information which is not the individual’s personal data, the request will not be a subject access request and the following rules will not apply. You should make contact with the employee to explain that you are under no obligation to respond to the request as a subject access request. It may, however, be more appropriate to deal with it as a freedom of information request.

**Personal Data.**

“Personal data” is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including a name.

“Special categories of personal data” includes information relating to:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sex life or
* sexual orientation.

**What you should do upon receiving a Subject Access request.**

When you receive a request, you should first ensure that the data requested is personal data relating to the employee. If it is not, for example, if it relates to profit data, then a subject access request is not the appropriate method for a request. You should consider whether the request should be dealt with as a Freedom of Information request.

If the request is general or vague, for example, you are able to ask the employee to be more specific regarding the data they wish to have access to. You may also do this where you process a large amount of personal data in relation to the employee. Your request for further information should not carry the intention of narrowing down the request, although this may in fact be the end result. You may ask them to provide information about the context in which the information about them may have been processed and about the likely dates when processing occurred if this will help you deal with the request.

Where a request is received that does not specify which personal data the employee wishes to be disclosed e.g. “all personal data relating to me”, or where a large amount of data is processed on the employee, you may ask the employee to be more specific on the data to which the request relates. If the employee offers no more specific a request, you are able to either:

* charge a reasonable fee to comply with the request or
* refuse to deal with the request on the grounds that the request is “manifestly unfounded or excessive”.

**Payment/Fee**

Under the GDPR, you may no longer request a fee from the individual in order to supply information as a standard procedure. The information must be provided free of charge. There are two circumstances in which a fee may be charged:

* if the request is “manifestly unfounded or excessive, particularly if it is repetitive” or
* where further requests of the same information are made.

**Time Periods**

Information must be provided without delay, and at the latest within one month of receipt of the request.

However where requests are complex or numerous, you may extend the normal one month maximum time limit by a further two months, meaning that the overall deadline is three months from the date of receipt. Where you decide to use the extension, you must inform the employee within one month of receipt of the request and give reasons for the extension.

**Locating information**

Whilst you have a duty to facilitate the request, you are not required to do anything which is unreasonable or disproportionate to the importance of providing access to the information. You are expected, however, to make extensive efforts to find and retrieve the information requested.

Electronic systems usually allow for relatively efficient locating of data by using search terms and refining by adding parameters on date. Remember you may need to look through information that you have archived. In cases where you have deleted data, you are not expected to attempt to retrieve it. However, emails should not be considered as ‘deleted’ just because they have been moved to the ‘Deleted Items’ folder. It is not likely to be disproportionate to have to look through emails that have removed from your ‘live’ systems.

If information identifies others:

In many cases, information that must be provided in response to a subject access request will identify people other than the requester. In these cases, you do not need to disclose the information except where:

* the other individual has consented to the disclosure or
* it is reasonable in all the circumstances to comply with the request without that individual’s consent.

You should follow the following three step approach to dealing with information about third parties:

* does the request require the disclosure of information that identifies a third party? Can you redact a document to remove identification of the other party? As the right of access covers access to information only and not to documents, this would be one resolution
* has the third party consented? It is good practice to ask the third party for the consent to the disclosure of their information as part of a response to a subject access request. You are not obliged to get consent and in some cases it will not be appropriate to try to get consent
* would it be reasonable in all the circumstances to disclose without consent? If consent from the third party is refused, for example, you would need to consider whether, in all the circumstances.

**How to supply the information.**

You must send a copy of the personal data in writing to the employee. You may also send it by electronic means and if the request was made by electronic means, your response should be in “a commonly used” electronic form. You must also send the following information:

* the purposes of the processing
* the categories of personal data concerned
* the recipients or categories of recipients to whom data has been or will be disclosed
* the period during which personal data will be retained
* information on the source of the data
* information regarding complaints and disputes: the right to complain to a supervisory authority, the right to request rectification or erasure of personal data, to object to processing of data or to restrict that processing and
* where personal data is transferred outside the EEA, information on any safeguards
* In practice, most of the above information will be included in your privacy notice.

Information can be provided in hard copy or electronically. The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to the information they have requested. The Information Commissioner acknowledges that this will not be appropriate for all organisations but may work well in particular sectors.

Diagram

Description automatically generated

Diagram

Description automatically generated

Diagram

Description automatically generated