**Ready to respond**
Dealing with subject access requests

**What is a subject access request?**
From time to time you may receive requests from members of staff, job applicants and former staff members for access to or copies of “Personal Data” you hold about them (see below). Under the Data Protection Act 1998 (“DPA”), these are known as Subject Access Requests (“SAR”).

There are strict legal requirements with which you will need to comply regarding such requests under the DPA. Furthermore, your obligations extend beyond Personal Data held by you, as an employer, to those held on your behalf by a third party.

Those making a SAR are also entitled to request and be provided with details of:
- the purpose(s) for which their Personal Data are processed
- the recipients to whom that Personal Data may be disclosed
- the sources of that Personal Data
CAUTION!
This note and the “frequently asked questions” which follow, provides an overview only of SARs and the applicable legal requirements. Dealing with SARs can be tricky and complex, from identifying a legitimate request, to responding appropriately and within strict timescales. SARs are also being used increasingly as “fishing expeditions” or early disclosure opportunities by potential claimants and their advisors. Responding inappropriately (or failing to respond) can expose the business not only to regulatory enforcement action, fines, and claims from the affected individuals for breach of a statutory duty, but also to adverse publicity or compromise of your position in legal proceedings.

It is strongly recommended that you identify specific individuals within your business to deal with SARs, so that requests can be channelled appropriately and those individuals understand the significance of the task.

A SAR handling policy and procedure should be adopted and training given to those involved. In case of doubt, professional advice should be sought. (Contact details of our own Privacy and Information Law team are provided below).

What is personal data?
So what information might you be required to disclose in response to a SAR as an employer?

‘Personal Data’ is defined in the DPA. It is information which relates to and identifies a living individual, either on its own or when combined with other information held by you as the “data controller”.

Personal Data may be held in a variety of media:

- Automated payroll systems
- Internet logs
- Records of automated door entry systems
- Word processing systems
- Messaging systems
- CCTV records
- E-mails
- Paper records
- Telephone records
- Automated systems
- Databases
- Internet logs
- Records of automated door entry systems
- Variety of media

Computerised data may be held on a central server, a memory stick or the hard drive of a particular computer. If data has been deleted but is technically recoverable, it may be within the scope of the required searches for the purposes of a SAR.

Paper records will also be within scope if they are in a manual filing system which is structured so as to allow retrieval of the Personal Data by reference to an individual (e.g. an organised system of paper HR records) - although, for public authorities subject to the Freedom of Information Act 2000, even unstructured records may need to be considered for the purposes of a SAR.
Timescales and fee
You are entitled to apply a fee to undertake a search in respect of a SAR. With some exceptions (for example in the respect of health records) the maximum amount that can be charged is normally £10.

Acknowledgement of receipt of a SAR should be provided as soon as possible AND the request considered promptly.

A valid SAR must be responded to within **40 calendar days** of receipt of the SAR (or of payment by the applicant of the fee, where it is requested).

**Before responding**

<table>
<thead>
<tr>
<th>In all cases, BEFORE responding to a SAR ensure:</th>
<th>To achieve to 40 calendar day deadline you must AS SOON AS POSSIBLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>– it is made in writing</td>
<td>– identify who, within your organisation, will locate the information and prepare a response</td>
</tr>
<tr>
<td>– you are sure of the identity of the person making the request and their current contact details</td>
<td>– locate the Personal Data held in relation to the applicant</td>
</tr>
<tr>
<td>– you are sufficiently clear as to what information is sought</td>
<td>– assess whether the Personal Data must be supplied in full to the applicant. For examples of exemptions see FAQs below</td>
</tr>
<tr>
<td>– a fee has been paid (if you intend to request fee payment)</td>
<td></td>
</tr>
</tbody>
</table>

For some frequently asked questions, see overleaf.

**Responding to a SAR**

**REMEMBER** that just because it may be difficult for you to find the requested Personal Data or the search generates a large volume of documents, this is **not** a valid basis for refusal (although it may affect the extent to which you provide copies).

– the request does not have to specifically mention the DPA or say it is a SAR to be valid, nor to can you compel the use of a specific form to make the request

– the right of applicants is to see their own Personal Data, as opposed to a right to see copies of entire documents that contain their Personal Data. Practically however often the easiest way to provide the relevant information is to provide copies of the original documents.

– you must generally provide a copy of the information to be disclosed in response to a SAR in a permanent form

– it may be appropriate to provide certain information in redacted form. This is often fraught with difficulty and leads to error. It is strongly recommended that redaction of any documentation is undertaken only with specialist advice

– complex terms or information contained in the data which the applicant is unlikely to be familiar should be explained

– you are **not** obliged to inform the applicant that an exemption applies to some of the requested data or that exempt information has been withheld but it is good practice to do so and to explain the reasons. (For examples of exemptions, see FAQs overleaf)

**For further information or advice, please contact**

Paula Barrett
Partner

T: +44 20 7919 463
paulabarrett@eversheds-sutherland.com

Mark Fletcher
Partner

T: +44 115 931 7595
markfletcher@-sutherland.com
Some frequently asked questions

1. Is it a Subject Access Request?
   A SAR must be made in writing. Any written request by an individual asking for their personal information is a SAR, whether or not it refers to ‘Personal Data’ or the DPA.

   Example of a SAR – “Please send me a copy of my staff records”.

2. Are you sure of the applicant’s identity?
   In most cases, the identity of the applicant will be known to you or will be apparent.

   If in any doubt, check! - for example by comparing the address or contact details given by the applicant against your employee records. Supplying a SAR response to the wrong person or to someone holding themselves out to be someone else, will be a significant security breach (and a serious breach of the DPA).

3. Do you understand the request?
   Before responding to a SAR, you may require additional information in order to locate or identify the requested Personal Data.

   The fact that a SAR is broad and onerous to deal with (eg commonly SARs will ask for “all Personal Data held on me”) is not an acceptable reason for delay, unless it is not possible to understand the requests made.

4. Has the fee been paid?
   You are entitled to await payment of any requested fee (maximum of £10) before handing a SAR, providing this accords with your standard practice ie fees cannot simply be charged for broad requests or specific individual applicants.

   If the fee is not paid with the SAR, you should request payment and the 40 day response time limit will run from the date on which the fee is paid.

5. What if the requested information is not available?
   If you do not have access to the requested Personal Data or the data does not exist, you should inform the applicant in writing as soon as possible, preferably with an explanation.

   NB Information held on your behalf by a third party must still be located, reviewed and disclosed (unless exempt from disclosure – see below).

6. Can you alter requested information?
   You may not make changes to Personal Data after receiving a SAR, even if the information it seeks is inaccurate or embarrassing.

   However, routine amendments and deletions to personal information which would have occurred in any event are permissible - with caution! - and the unamended version should still be considered for disclosure.

7. Are there any exemptions to supplying requested Personal Data?
   The Personal Data of the applicant must be provided subject to certain exceptions. There are a number of such exceptions but these are not always easy to identify or to apply in practice.

   Amongst the most commonly applicable exceptions to disclosure are where the requested data:

   Contains Personal Data or information regarding the Personal Data of a third party
   You will need to weigh up carefully obligations of confidentiality to the third party and the extent to which these might be overcome.

   NB This is rarely straightforward and it is strongly recommended that you seek specialist advice.

   Is a confidential reference given by the recipient
   The requirements regarding disclosure of references can often be confusing. Simplistically, references you have received must be disclosed unless this will infringe a duty of confidentiality/ third party personal data whilst those you provide to another party are likely to be exempt.

   Would be likely to prejudice ongoing management planning or business forecasting by the recipient. (The factual context and timing of disclosure are critical to this exemption.)