Individuals (or a third party acting on their behalf) have the right under Section 7 of the Data Protection Act 1998 to request a copy of all of the personal data held and controlled by an organisation. These are known as data subject access requests (SARs).

An individual does not have to give a reason for wanting to see their personal data although there may be good reasons for requesting it. It is often used as a way to obtain evidence to bring some form of legal action against an employer, an ex-employer or a third party. SARs can also be used as a tool by a knowledgeable employee hoping to uncover something useful for an employment claim, or simply to inform the individual about what personal data is being processed by an organisation.

For an organisation, SARs can end up being very time-consuming and expensive, particularly if they are not handled in the right way and an individual complains to the Information Commissioner’s Office (ICO) or takes court action. So if you receive a SAR what should you do?

- There are no prescribed formalities for making a request other than it must be in writing. Therefore, if a written request for personal data is received from an identifiable individual, it should be assumed that it is a valid request. It is possible to negotiate the scope of the request with the data subject so bear this in mind if the request is very broad. Organisations may also charge a fee of £10.

- Organisations have 40 calendar days within which to provide a response to a request. Acting as quickly as possible when responding to a SAR can help to prevent panic towards the deadline. Notifying relevant internal teams such as IT departments is critical, as it can take even large teams of IT staff weeks to pull together an individual’s personal data. Searches should be thorough and extensive (e.g. back up and archived e-mails) so let your IT teams know the level of searching required. If particular third parties are involved such as line managers, it is important to check their availability so that they can be consulted if need be.

- A number of exemptions can apply which may be used to withhold an individual’s personal data from the response: for example, personal data contained in documents or e-mails which are legally privileged will be exempt from disclosure; or personal data which, if disclosed, would prejudice the prevention or detection of crime are also exempt from disclosure.

- Generally, only the personal data of the subject should be disclosed and any personal data relating to a third party should be redacted or withheld. The law does make an exception where the third party has consented to the disclosure or it is reasonable in all the circumstances to comply with the request without their consent, such as if the third party is an individual’s line manager or supervisor.

- Your response to the data subject should set out clearly a brief summary of the personal data you are providing (unless a more detailed description is requested) and explain if any personal data has been redacted or withheld because an exemption applies or because there is third party data.

**Do’s and Don’ts**

- **DO** require the individual to provide proof of their identity and address.

- **DO** keep a clear record of all the searches carried out, the reasons for redacting/withholding third party data or if you are applying any exemptions. This will become useful if an individual decides to complain to the ICO.

- **DO** be careful in having sensitive or confidential discussions about certain individuals. It is better to have these discussions face to face.

- **DO** make sure you make any redactions carefully when covering up any third party data within documents and e-mails.

- **DO** communicate with your in-house legal teams or external solicitors at the earliest opportunity.

- **DO** train staff in recognising and dealing with SARs and put in place a clear SAR policy for employees to follow.

- **DON’T** ignore a SAR or sit on it until the last minute.
DON'T disclose any third party data unless you have their consent or, on balance, it is reasonable to disclose the data without consent.

DON'T try to extend the 40-day time limit by insisting that they use your standard subject access request forms instead of their own draft.

Zak Karim is a solicitor in the IP team and information law teams at Pinsent Masons. For further information, please contact:

Zak Karim  
Solicitor  
T: +44 (0) 121 626 5701  
E: zahir.karim@pinsentmasons.com

DON'T panic – if you have any queries, please call