How to...

Respond to a Data Subject Access Request

A quick and easy reference guide on the basics
Top tips on responding to a Data Subject Access Request (DSAR)

1. Consider whether the request provides sufficient information to identify the individual and the relevant data. If appropriate, request the identification information and/or payment of the fee
2. Decide the search parameters and conduct the search
3. Assess whether the data comes within the scope of the DSAR
4. Consider whether any exemptions apply and whether to obtain any third party consents
5. Respond within the time limit (currently 40 days)

About our HR How to Guides
These bite-sized reference guides provide an outline of the processes commonly managed by HR in the workplace. They do not provide full detail of these processes and are not a substitute for legal advice, particularly as every situation will depend on the particular circumstances.
How to respond to a Data Subject Access Request

What is a data subject access request?

If a business carried on in the UK collects, holds and uses (processes) personal data for its own purposes, it will be a ‘data controller’ under the Data Protection Act 1998 and must respond to data subject access requests (DSAR) from individuals requesting copies of their personal data. Data protection law is changing from 25 May 2018, and new rules set out in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 will govern DSARs from then on.

Steps to take on receipt of a DSAR

The time limit for responding to a DSAR is currently 40 days from receipt of the request, so the process of searching for the individual’s personal data should be started promptly on receipt of a DSAR. Under the GDPR, the time limit will be shortened to 1 month (unless the request is complex).

If the request does not provide enough information to identify the individual and the relevant data, ask for the relevant information. Employers are currently allowed to charge a fee of up to £10 for responding to a DSAR. Where further information and/or payment of the fee is requested, the deadline is extended to 40 days from them being received.

It is good practice to write to the individual to:

• confirm receipt of the DSAR, and
• indicate when you are likely to respond, taking into account the 40 day time limit.

In some cases it may be appropriate to explain or try to agree the scope of the search and the terms to be used.

Why is it important to get the process right?

If an individual is dissatisfied with how their DSAR has been dealt with, they can make a complaint to the Information Commissioner’s Office (ICO) which may issue an enforcement notice. Persistent or serious breaches could lead to further action by the ICO, including a fine.

An individual may also pursue a complaint in the courts by:

• seeking an order for compliance with their request, and
• bringing a claim to compensate them for damage or distress suffered.
Conducting the search

Appoint someone to manage the DSAR, who should provide the following information to the heads of all departments which may hold personal information on the individual:

• an explanation of what "personal data" is
• instructions not to delete any personal data relating to the individual, unless it would be deleted in the ordinary course of events
• an explanation of the extent of the searches they should carry out (unless these are being carried out centrally)
• the timescale for completing the searches

Liaise with IT and identify potential sources of personal data relating to the individual (e.g. emails of other employees, workspaces/hard drives/memory sticks and deleted items) and decide how they will be searched.

Search terms may need to be decided upon in order to locate personal data held electronically, such as in emails. It is important to ensure that the search parameters can be justified, so careful thought should be given to any search terms that are used.

Manual files (e.g. the individual’s personnel file) may also need to be searched if they meet certain requirements in terms of the way they are structured or organised.

Other potential sources of data include mobile devices, records of automated entry systems such as swipe cards, telephone records, CCTV, payroll systems, photos and internet logs.

What is personal data?

Once data relating to the individual has been located, it must be reviewed carefully to establish whether it is personal data that falls within the scope of the DSAR.

“Personal data” is information relating to the individual, from which they can be identified, directly or indirectly, including by reference to an identification number or another code. All searches should therefore include searches for the individual’s initials and any pseudonyms or code names.

Personal data includes:

• any expression or opinion about the individual and any indication of the intentions of the employer (or any other person), in relation to the individual
• information that has the individual as its focus and affects the individual in some way
• any personal details about the individual

Merely having the individual’s name in a document, for example emails in which the individual is the sender or recipient, but with nothing linking them to the subject matter of the email, does not amount to personal data and therefore does not come within the scope of a DSAR.

What is personal data?
Providing the data and response

Consider whether any data is exempt from disclosure, which may mean that the employer is justified in withholding it. There are a number of exemptions which may apply, including for:

- personal data that is subject to legal professional privilege
- health records where disclosure would be likely to cause harm to the physical or mental health of the individual or anyone else
- confidential references given by the employer
- personal data held for personal, family or household affairs including recreational purposes
- personal data processed in connection with management forecasting or planning to the extent that complying with the DSAR would prejudice the conduct of the business (e.g. organisational change, redundancy planning)
- personal data consisting of records of the intentions in relation to negotiations between the business and the individual to the extent that complying with the DSAR would prejudice the negotiations (e.g. pay or bonus negotiations)

Decide if consent should be sought from any third parties who may be identifiable from the data. If it is not appropriate to seek consent or consent cannot be obtained, consider whether it would be reasonable to disclose the third-party information without consent or whether any steps can be taken to remove the third-party data.

Before responding to the DSAR, where appropriate remove or black out data:
- that is confidential to the employer and does not contain personal data or is otherwise exempt, and
- from which a third party can be identified where they have not given their consent or their consent was impracticable to obtain and it is not reasonable in the circumstances to disclose the data without their consent.

Respond to the DSAR within the deadline by providing a written response to the request. Consider including an explanation of the types of data provided, and whether and for what reasons any data has been withheld. You should keep a copy of what is sent to the individual.

Please contact one of the partners in our team, or your usual advisor at Clyde & Co.

Robert Hill
Partner
T: +44 20 7876 6214
E: robert.hill@clydeco.com
50
Offices

3,600
Total staff

390
Partners

1,500
Lawyers

www.clydeco.com