QUICK REFERENCE GUIDE

GDPR: Data subject access requests

Under Article 15 of the GDPR, individuals have the right to make a data subject access request ("DSAR"). While an individual has had the right to access data held about them for many years, the development of digital technology has led to a massive expansion in the nature and quantity of data processed making responding to such requests more complex,time-consuming and costly. This guide provides an outline of what to consider when dealing with DSARs from employees in particular – but remember that all living individuals have this right.

What should i do if I receive a DSAR?

Employers have a duty to facilitate the exercise of a DSAR, to handle the request fairly and transparently and to provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It is important to note that requests can be made orally or in writing (including by email or any other electronic means such as social media) and without a particular prescribed form. It might be a good idea to set out a preferred method of contact to reduce the risk of overlooking requests although you cannot make the use of such a method mandatory.

SHOOSMITHS

03700 86 30 00
www.shoosmiths.co.uk

Initial considerations

- Verify the identity of the requester – is it an employee? Is it their own personal data they are requesting? Is it a third party requesting data on someone else's behalf, and do they have the specific authority to do so?
- Consider how broad the request is – an employee does not have to be specific and can just request "all personal data about them". You can ask them to narrow this down (particularly where you process a large amount of information – for example by timescale or subject or source) but they don't have to agree.
- Do you need more detail to be able to locate the data?
- Who will deal with the request and how do you intend to go about locating the data?
- Will you be able to respond to the request within the timeframe?

Timescales

Requests must be handled with undue delay and, in any case, within **one month** of the receipt of the request. ICO guidance states that this period starts the day you receive the request until the corresponding calendar date in the next month, unless that day is a bank holiday or weekend, in which case it ends on the next working day. If there is no corresponding date (i.e. the next month is shorter) then the deadline is the last day of the following month.

You may request up to a two- month extension if the request is particularly complex but you must respond to the employee within **one month** of the request to acknowledge receipt of the request, explain that you are extending the response period and provide your reasons for not being able to provide the data within the initial month.

Refusing a request

If you are not the data controller then you do not have to comply with a DSAR. For example occupational health records may be held by the OH provider which is a controller in its own right. However, you do still need to respond to the employee/requester to explain this to them. You must provide them with written reasons as to why you cannot provide the data within one month of the request and inform them of their option to complain to the Information Commissioner's Office ("ICO").

It is possible to refuse a request if you believe the request is "manifestly unfounded or excessive". If you refuse the request then you must write to the employee/requester as soon as possible but in any event within one month providing your reasons and informing them of their option to complain to the ICO.

Be cautious with this approach – the ICO will scrutinise such decisions closely and if they do not agree with your refusal you could be in breach of the GDPR.

Where to start looking and preparing the data to be disclosed

Emails are the usual starting point. Be sure to search a number of inboxes using various searches to make sure you've covered the possible options.

Once you've identified a pool of emails that contain the personal data, search again if you're looking for more specific data. Consider other sources of data such as back-up drives or archives. Note also that personal data held by data processors for you is also in scope.

Consider what information needs redacting or needs to be disclosed. Is it personal data which relates to other individuals but does not relate to the employee? Is it personal data which is information about the employee but also contains personal data about another individual? For example, if it is an email from one individual to another commenting on the poor performance of the employee then that email will be deemed to contain personal data about the employee but also about the person making the comments.

If there is more than one individual's personal data involved then ideally you should seek consent from the other individual to disclose that information. You are not obliged to seek consent of the other individual if it is reasonable to disclose the information without the consent of the other individual. If consent is granted, you must disclose the information.

Redacting data

If you do not have consent of the other individual, and you do not believe it is reasonable to act without consent, then consider if you can redact the information. Remember:

- information which is not personal data does not need to be disclosed, for example, financial performance or business expansion plans. These fall outside of the scope of GDPR and can be redacted
- you can redact any personal data or other information which does not relate to the employee
- you can redact other exempt personal data (see below).

Exemptions to the rule

There is no obligation to disclose personal data under a DSAR where the request relates to:

- personal data which would be legally privileged in legal proceedings or in obtaining legal advice
- a reference given or to be given, or received or to be received, in confidence for employment, training or educational purposes
- personal data processed for purposes of management forecasting or management planning in relation to a business or activity where compliance would prejudice the conduct of that business or activity
- personal data consisting of records of intentions in relation to negotiations between an employer and employee where compliance would prejudice those negotiations.

This is a non-exhaustive list and others include (for example) criminal investigations and judicial proceedings. ICO guidance is available on all exemptions here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/. Any data that falls under one or more of these exemptions can be redacted or removed. You should keep a clear record of why each redaction was made, and be prepared to justify it if challenged.

What must the response contain?

Article 15 of the GDPR provides that responses to DSARs must:

- be in writing or, if appropriate, by electronic means
- provide a copy of the personal data (making sure there is no inadvertent disclosure of other's personal data)
- provide information on the purpose of processing – for consistency consider using the description in your privacy notices
- provide information on the categories of personal data concerned – again look to your privacy notices
- detail any recipient or categories of recipient that receive the personal data – for example, payroll, line managers, the bank and auditors may receive salary information of the employee
- provide information on the source of the data except where the data was provided by the employee
- detail any relevant data retention periods
- provide information on the employee's rights to request rectification or erasure of personal data, right to restrict processing or object to processing of personal data (particular circumstances apply)
- identify if any decisions are based on automatic processing
- provide information of any safeguards if data is being transferred outside the EEA; and
- inform the employee of their right to lodge a complaint with a supervisory authority – the relevant authority in the UK is the ICO.

Employment contacts:

Gwynneth Tan
T: +44370 086 8477
E: gwynneth.tan@shoosmiths.co.uk

Stuart Lawrenson
T: +44370 086 6733
E: stuart.lawrenson@shoosmiths.co.uk

Adele Hayfield
T: +44370 086 4226
E: adele.hayfield@shoosmiths.co.uk

Commercial contacts:

Nick Holland
T: +44370 086 8754
E: nick.holland@shoosmiths.co.uk

Anastasia Fowle
T: +44370 086 7052
E: anastasia.fowle@shoosmiths.co.uk