SHOOSMITHS

UK GDPR

Dealing with employee DSARs

www.shoosmiths.com

FOR WHAT MATTERS

Data Subject Access Requests (DSARs) serve as the mechanism through which individuals exercise their 'right of access' under the UK General Data Protection Regulation (GDPR) as supplemented by the Data Protection Act 2018 (DPA 2018). Under the GDPR, an employee (known as a data subject) may make a subject access request to you as their employer and the controller of their personal data.

Under this right of access, employees are entitled to the following:

- confirmation of whether or not their personal data is being processed;
- a copy of their personal data; and
- additional information about the manner in which their personal data is processed.

You must respond to a DSAR within 1 month of receiving the request. In some circumstances this deadline can be extended by a further 2 months, but this should not be assumed.

Responding to a DSAR can be a complex and time-consuming exercise. In circumstances where employers have fallen foul of the process, the ICO can issue penalties for non-compliance, which may consist of a warning, reprimand, enforcement notice, or penalty notice. If you are at all unsure, we can assist you through the process.

Strategy

DSARs are often used tactically as a means to gain leverage during litigation or settlement negotiations. They can serve as a 'fishing exercise,' aimed at uncovering information that can bolster a current or potential legal claim or simply disrupt the business. When addressing a DSAR, it's crucial to take into account the broader strategic context, especially concerning ongoing employment matters. Our approach involves actively listening to our clients and providing strategic advice that aligns with the broader issues at hand.

Searching for the data

Once a strategy has been established and the scope narrowed and defined, it becomes essential to thoroughly search your internal systems and databases to collect all relevant personal data about the data subject. You will need to conduct searches across various devices, which may include your computer system, phone network, tablets, external hard drives, USB sticks, and even CCTV footage. Additionally, pay close attention to archived folders, as they often harbour hidden data that might otherwise be overlooked. **The ICO provides guidance on how to approach this, which you can find here**.

Collating the data

Handling a DSAR often involves dealing with extensive volumes of data. The size of these data sets depends on the scope of the request and the employee's length of service. If you haven't managed a request like this before, sifting through potentially thousands of documents and other data can feel overwhelming. However, our team can alleviate the pressure on your business and take charge of the process. We can help you with the approach for the information search and once completed, we'll manage the subsequent steps.

To get started, all you need to do is grant us access to the relevant data. There are several ways to do this depending on the volume of data and your budget.

For smaller data sets, you can simply email them to us in PDF format. Alternatively, if you're dealing with a larger volume, you can upload this to our secure data site called 'Collaborate.'

For larger data sets or those requiring additional sifting and organisation (such as removing duplicates), we work with third-party providers. These providers securely host the data and can also handle additional administrative tasks, ensuring the most efficient and cost-effective process possible.

For very large DSARs we offer SmartSAR, using cutting-edge processing technology and secure client portals to offer an end to end DSAR solution: **SmartSAR**.

Redacting the data

Based on our initial strategy discussion, we establish clear parameters before commencing the redaction process. We will work with you to assess the most appropriate approach to a DSAR; the strategy adopted will vary with each DSAR. This task involves a delicate balancing act and is an area where businesses often benefit from the additional legal support we can provide.

Additionally, we proactively identify any information that may be exempt from disclosure according to the ICO guidelines, providing the business with an extra layer of protection.

Crucially, our redactions are irreversible and cannot be undone. Our systems ensure that redactions are finalised before sharing the data with our clients and data subjects, ensuring that data subjects cannot remove redactions to access information outside the scope of their request.

Responding to the DSAR

Article 15 GDPR provides that responses to DSARs must contain specific information in order to comply with ICO guidelines. To ensure that your business remains fully compliant from the beginning to end of the DSAR process, we provide you with a tailored response letter ready to send to the data subject.

Supporting you with wider employee DP issues

Our team has extensive experience in employment-related data protection issues.

In addition to DSARs, we are able to assist you with some of the wider issues your business may face, including:

- Strategic advice on the overlap between employee data law and employment law issues arising from day-to-day employee relations matters. For example, advice on the use of employee health information, managing the expression of political/philosophical beliefs in the workplace and the degree to which confidentiality can be observed in grievance and disciplinary proceedings;
- Drafting policies such as Employee Data Protection, Employee Privacy Notices and Employee Data Retention policies;
- Personal employee data audits; and
- Rapid response to employee data breaches.

Get in touch

Gwynneth Tan
PARTNER

T +44 (0)3700 868 477
M +44 (0)7718 037 127
E gwynneth.tan@shoosmiths.com

Stuart Lawrenson
PARTNER

T +44 (0)3700 866 733
M +44 (0)7595 096 587
E stuart.lawrenson@shoosmiths.com