FOCUS

INTERNATIONAL EMPLOYEE DSARS

Practical tips for UK employers

Since the General Data Protection Regulation (*2016/679/EU*) (GDPR) became enforceable in 2018, there has been a significant increase in the number of data subject access requests (DSARs) lodged by current and former employees for the purposes of obtaining personal data held by their employers.

Employee DSARs have proven to be one of the most onerous areas of the GDPR for organisations to manage. They are more complex when compared to other types of DSAR, as they usually cover more custodians and longer time periods, and generally encompass greater volumes of data. A further layer of complexity is added, as employee DSARs are frequently used as a negotiation tool in employment disputes.

DSARs in employment disputes

Under Article 15 of the retained EU law version of the GDPR (UK GDPR), an employee has the right to ask their employer what personal data it holds about them and obtain a copy of that data, subject to various exemptions. While employees may have a legitimate, non-contentious desire to see their personal data, employee DSARs are almost always tied to a wider employment dispute. This can raise complex issues, particularly where a DSAR is used as a tactic to obtain a favourable settlement (*see feature article "Cyber incidents: managing the employee fallout", www.practicallaw.com/w-035-0663*).

Guidance from the Information Commissioner's Office (ICO) (ICO guidance) states that the general rule is that data controllers must be "motive blind" when responding to DSARs (*https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/*). In other words, the data subject's intention when making a request should be irrelevant in how it is handled.

Recently, however, in *Lees v Lloyds Bank PLC*, the High Court arguably increased the scope for data controllers to refuse to respond to DSARs, particularly where the data subject's request is deemed to be vexatious or tactical (*[2020] EWHC 2249*). The court considered a number of factors, including:

- The number and repetitive nature of the requests.
- The underlying purpose of the DSAR, which in *Lees* included to obtain documents, not personal data, and to assist the individual's position in separate proceedings.
- Whether there is a benefit to the data subject if that personal data is disclosed.

While *Lees* was specific to the facts, it serves as a reminder that the motives of the data subject may be a relevant consideration in responding to DSARs.

Article 12(5) of the UK GDPR and the ICO guidance make clear that employers can refuse to comply with a DSAR if it is manifestly unfounded or manifestly excessive. This is particularly relevant in the context of an employment dispute. If the employee's request is being used to harass an organisation with no real purpose other than to cause disruption or if the employee clearly has no intention to exercise their right of access, then it may be justifiable to refuse to comply.

In any event, DSARs made in the context of employment disputes are usually costly and can act as a motive to encourage settlement of an ongoing employment dispute. Organisations need to ensure that they have efficient processes in place to deal with DSARs, which usually requires collaboration between legal and HR teams in order to minimise disruption to the business while respecting the individuals' rights of access.

Relevant law

As more jurisdictions provide the right to access personal data, it is possible that organisations will need to handle DSARs to which multiple jurisdictions' data protection laws apply. The key question at the outset of multi-jurisdictional DSARs is to determine which legal regime applies to each DSAR. Generally, to mitigate any risk of non-compliance, organisations should proceed on the basis that the legislation that affords the most expansive rights to the data subject will apply.

The multi-jurisdictional element of a DSAR adds another level of complexity as a number of practical issues will need to be considered. For example, an employer needs to consider the timeframe within which it must respond, whether it is possible to extend the timeframe and, if so, what the basis is for an extension. It also needs to consider whether different exemptions apply, and whether the obligation is limited to carrying out a reasonable search.

A key issue for multi-jurisdictional DSARs is that certain data may be disclosable under one regime but not under another. Organisations will need to take local advice. This will continue to be particularly important for UK employers if the UK data protection regime begins to diverge from the EU data protection regime following Brexit.

Before the request

The key steps to prepare for employee DSARs involve getting the basics right:

- The most important step for handling employee DSARs is to know what data is held and where. Data mapping will greatly help to reduce the burden of handling complex, international DSARs. Organisations should ensure that they

have accurate records on the format of employee personal data and where it is stored.

- Information should be readily available on how employees may make a DSAR; for example, on staff intranet pages, in leaflets or in the data protection policy. Not only is this legally required, but it will help to prevent a DSAR from being sent to a "no-reply" or intermittently monitored mailbox and missed.

- Employers should ensure that staff are trained on, and able to recognise, a DSAR, and that the relevant policies and procedures are drawn to staff members' attention.

- Employers should try to minimise the storage of personal data by employees and ensure that information is not kept for longer than necessary for its purpose. The threshold for organisations to search across storage types of information is high, so the less data that is held, the less data that needs to be searched through.

- The organisation needs to ensure that it responds in time by diarising deadlines and maintaining a log of DSARs that have been received.

Receiving the request

Dealing with employee DSARs can be labour-intensive so preparation is key to ensuring that a response can be sent within the one month time limit. If the request is complex, or the employee has submitted a number of requests, the deadline to respond can be extended by a further two months (*Article 12(3), UK GDPR*).

Whether a request is deemed "complex" depends on the specific circumstances of each case, including the volume of data requested, the size and resources of an organisation, and whether specialist legal advice is needed before responding to the DSAR. However, the ICO guidance states that the fact that it would take the controller a vast amount of time and effort to provide the information to the data subject does not, on its own, render a request excessive.

Disclosing third-party data

In some situations, it may be reasonable to disclose a third party's data and this will depend on the circumstances. An employer will need to balance the data subject's right of access against the other individual's right to privacy.

A practical example to consider is where employee A makes a formal complaint about employee B, which is a factor that leads to disciplinary action against employee B. Employee B then makes a data subject access request to the employer. In this scenario, there will be communications and materials that contain personal data on both employees and would therefore be disclosable to employee B. The context of these documents would likely make the identity of employee A obvious, on the basis that it refers to incidents that occurred between employees A and B. In this case, the employer would need to assess whether employee A's right to privacy outweighs employee B's right of access. A number of factors will need to be considered, including the sensitivity of the information being disclosed and any duty of confidentiality that may apply to employee A.

The most intensive stages for organisations responding to a DSAR include identifying where the data is stored, exporting and reviewing the data, redacting any third-party information and producing a package of relevant documents that can be shared with the employee.

Additional demands on time include assessing the applicable regulations for obligations and exemptions, and providing updates on the process to data subjects, legal counsel and internal stakeholders. It is crucial that enough time is given to each stage so that unforeseen issues can be resolved and the regulatory deadline can be met.

Identity verification

On receipt of a DSAR, it is important to confirm the identity of the data subject making the request. This may be achieved by requesting additional information, such as passport or driver's licence. However, the request for identification must be reasonable and proportionate. Organisations should not request more information if the requester's identity is obvious.

Where an employee is emailing from their work email address or there has been a conversation with the employee about the request, a request for identification is unlikely to be necessary. In some circumstances, an employee making a DSAR may be represented through their solicitors so employers will need to request evidence of authority to act on the employee's behalf.

Scope and search terms

In a dispute, employees often ask for all of the data that their employer holds on them. They are entitled to do so but, in reality, they are often only interested in data about particular incidents or from certain individuals. In the first instance, an employer should run a full search on the employee in accordance with their proposed scope to determine the potential size of the task. The volume of data retrieved will, in turn, help to ascertain whether it would be excessive or unreasonable to proceed on the basis of that scope.

In some circumstances, employers may request that a data subject reduce the scope of their DSAR. Under the UK GDPR, controllers are only required to carry out a reasonable and proportionate search in response to a DSAR. It can therefore be useful to clarify with the employee whether there is a particular search scope or search terms that may be applied.

Where an employer contacts the employee to clarify the scope of their DSAR, the time under the regulatory deadline is paused until the employee provides a response.

Once the scope of the search has been clarified, the employer should consider the search terms that should be used to retrieve an accurate data set. It may be appropriate to

agree these search terms with the employee in order to mitigate the risk of any challenge further down the line.

How and where to search

After identifying search terms and undertaking an initial search, an organisation must ensure that all relevant documents have been considered, including any archived emails. Other forms of communication used for work purposes must also be reviewed, including instant messenger apps such as WhatsApp and Microsoft Teams.

Where employees use personal devices for work purposes, these must also be searched if there is a good reason to believe that the employee is holding relevant personal data on that device. It is important that employers have a bring your own device policy in place to ensure that employees are aware of their own obligations in response to a DSAR (*see Briefing "Bring your own device: responding to the trend", www.practicallaw.com/7-530-5276*).

Consider exemptions

Certain types of personal data will fall outside the scope of any DSAR, including third-party personal data, personal data that is subject to legal professional privilege, personal data subject to a legal duty of confidentiality, negotiations concerning the data subject and confidential references.

By making a DSAR, the data subject is requesting their own personal data. Any personal data relating to third parties should not be disclosed unless consent has been obtained from the relevant third party or it is reasonable to comply with the DSAR without the third party's consent (*see box "Disclosing third-party data"*).

Conducting the review

Having considered the scope and exceptions, taking certain practical steps can make conducting the review more efficient. Employers should:

- Use an online review platform that collates all the potentially responsive data in one place for online review and analysis. Online review platforms ensure a far more efficient review and redaction process which, in turn, frees up internal resource to focus on managing the strategic side of the DSAR.
- Put in place a set of standard template DSAR responses to ensure that responses to any DSAR can be managed quickly and efficiently.
- Ensure that employee privacy policies are up to date, compliant and available to employees. As part of a response to a DSAR, an employer will need to provide certain information about its processing activities, which should be included in the employee privacy policy.
- Maintain a record of the copies of information supplied in response to a DSAR, together with copies of any material withheld and why.
- Produce a standard checklist that staff can use to ensure that they take a consistent approach to the review and redaction process.

Katie Hewson is a partner, Kate Ackland is an associate, Joseph Samuelson is a trainee solicitor, and Jake Saville is a solicitor apprentice, at Stephenson Harwood LLP.

