DPC's guidance on SARs—key takeaways for employers

Linda Hynes, Partner in the Employment, Immigration and Reward team of Lewis Silkin Ireland, looks at the recent guidance issued by the DPC on managing subject access requests and considers the key takeaways for employers when dealing with such requests

Towards the end of 2022, the Data Protection Commission ('DPC') issued detailed guidance ('the Guidance') to controllers on handling Data Subject Access Requests ('DSARs') which employers should carefully review and consider. The Guidance closely aligns with guidelines issued by the European Data Protection Board on the same topic. Both sets of guidelines reflect the high standard to which employers will be held in their handling of employee DSARs. As data subjects, employees have the right to request access to and copies of personal data which are being processed in any way by their employer (the controller), subject to certain limited restrictions. This data must be provided in an accessible form, free of charge and within certain time limits.
The Guidance looks at some of the practical issues that commonly arise for controllers in managing and responding to DSARs.

Initial points

The Guidance raises some key points for employers to be aware of before and when receiving DSARs.

First, employers should ensure that employees know how they can submit a DSAR. This might be best dealt with in the employee privacy notice which should be readily available to employees. Second, employers should ensure that they record DSARs and keep records of how they responded to those requests. This is particularly important in order to be able to deal with any complaints being investigated by the DPC. Third, while employers should establish a dedicated internal process for employees to submit DSARs, they should not ignore DSARs received through other channels, for example an employee might mention wanting access to all their personal data as part of grievance email to HR. Even where an employee submits their DSAR other than through the established channel, the timeline for responding to the DSAR still starts when the request was received by the controller. Therefore, it is crucial that employees are adequately trained to recognise DSARs when they are lodged and to re-direct them promptly to the relevant team/department.

How DSARs are lodged is at the discretion of the requesting employee. It is not uncommon for employers to receive DSARs from an employee's solicitor or from a union representative on their behalf. If there is any doubt over a third party having authority to lodge the DSAR on the employee's behalf, then the employer can request evidence of that authority. However, in most scenarios this should not be necessary, particularly if it comes from an employee's solicitor and the employer has already been in correspondence with that solicitor about the employee. In any case, when solicitors make such requests on behalf of employees, they will typically include a letter of authority from their client. This is sufficient for the employer to act on the request.

Clarifying requests

Clarifying requests is an issue of particular interest for employers, given the potentially significant volume of personal data that could be processed by employers in respect of their employees.

The basic principle confirmed in the Guidance is that data subjects are entitled to access 'any and all of their personal data'. However, the Guidance provides that, where the controller processes a large quantity of information pertaining to the data subject, they can ask the employee to specify the information they want to be provided or the specific processing activities they want to access. Whilst this sounds like helpful guidance for employers, it should be noted that the employee is not actually obliged to provide a response to their employer, and the employer must continue to deal with the DSAR even where any such request for clarification remains unanswered. This is an important point for employers to be aware of, as it could impact the timelines for responding to the employee. We also recommend that employers carefully document the reasons for any request for clarification.

Timelines for responding

The Guidance states that DSARs must be responded to 'without undue delay'. It goes on to highlight that 'the

response to an access request may be considered untimely even before the maximum term provided for by law has expired, depending on the circumstances of the case'. This is another important point for employers to note. To give an example of where this might arise, if at the time of a request, the permanent deletion of the personal data sought was imminent, then this could prompt an obligation of speedier action by the employer to respond to the request.

The Guidance clarifies that the one calendar month period under Article 12 of the GDPR is a maximum one, not a minimum, and so we expect to see the DPC being more critical of employers if they are delaying in responding when they could have responded earlier (for example, if the request is only seeking a small amount of personal data that could have been provided quickly). The Guidance is also very clear that exceeding the maximum time limit for a response will automatically constitute a breach. It is clear from the recently published DPC case studies (see page 1) that this is the position the DPC takes when employee DSARs are not responded two within the required time limits. This highlights the importance for employers to ensure their employees recognise a DSAR when it is made and immediately escalate it to the appropriate team within the organisation so it can be addressed without undue delay.

> ***"Poor control over personal data and inadequate procedures around dealing with DSARs will not assist an employer in being able to rely on legitimising an extension] ….A blanket two month extension policy without any justifiable explanation will be difficult to stand over."***

The Guidance is useful on how to calculate the calendar month period for response from the date the DSAR is received. Employers should consider that:

- the period shall end with the expiry of the last hour of whichever day of the following month falls on the same date as the day which initiates the period;
- the period includes public holidays, Sundays and Saturdays;
- the day which initiates the period is the day during which a valid access request is received. For example, if a controller receives an access request on 22nd December, on 22nd January the following year the minute starting at 23:59 will be the last minute in order to respond to the requester, regardless of the intervening Christmas holidays;
- where the period ends on a public holiday, Sunday or Saturday, the period shall end with the expiry of the last hour of the following working day; and
- where the day on which the period should expire does not occur in the month, the period shall end with the expiry of the last hour of the last day of that month. For example, if a controller receives an access request on 31st August, September ends on its 30th day and the maximum one-month period to comply with the access request would expire accordingly.

Although the statutory period within which employers must respond to DSARs is one calendar month, it is interesting to note that the Guidance 'strongly recommends' that controllers put policies and procedures in place aimed at responding to DSARs within 15 days. This could be challenging for employers to comply with, particularly where there may also be a legal dispute with the employee and the employee has been working with the employer for a long time and may have raised multiple grievances.

Extending the timeline

The Guidance addresses the issue of extending the timeline to respond to a DSAR by a further two months, but confirms that this can only be availed of when it is necessary to do so and in the event of complex or multiple requests. Employers should be careful about exercising blanket extensions to all employee DSARs and make sure they keep a record of the reasons why they determined the extension was required. This could be queried by the DPC in the event of a complaint. The Guidance sets out that extensions may be legitimate where:

- the amount of data is not readily available on the controller's systems;
- the controller would need to employ extra resources to comply;
- the response will need considerable redaction of third parties' data; and
- the response requires exemptions to be applied before it can be provided.

However, the Guidance is clear that the situations outlined above will depend on the specific circumstances and the resources of the controller. Poor control over personal data and inadequate procedures around dealing with DSARs will not assist an employer in being able to rely on any of the above points when extending the timeline to respond. In any event, the Guidance recommends that the controller extends the time as little as possible in order to comply. A blanket two month extension policy without any justifiable explanation will be difficult to stand over.

The DPC also points out that where controllers can partially satisfy the DSAR within the initial one month timeline, they should do so, and only apply the extension to the more complex aspects of the DSAR. We often recommend that employers provide everything that is easily accessible and doesn't require redaction or exemption review (for example, the employee's contract of employment and personnel file) to the employee as soon as possible on receiving a

(Continued on page 6)

(Continued from page 5)

DSAR.

The response

The Guidance summarises best practice in terms of responding to a DSAR. The points are similar to previous guidance issued by the DPC, but include some practical examples, particularly around providing context to the employee on the results. The Guidance states that controllers must allow the data subject to have 'meaningful interaction' with the personal data requested and must provide access to the personal data in such a way that allows the requestor to 'grasp the actual relationship' between them and the personal data provided. The Guidance gives the example of where the personal data at issue include handwritten notes about the data subject. In this case, the controller cannot simply provide the data subject with access to the notes as typed up by a secretary on a digital format, as the handwriting itself constitutes personal data. The Guidance also makes it clear that data subjects should not be unnecessarily overwhelmed by the DSAR response (which can sometimes be tempting with a challenging data subject!).

The Guidance does recognise the time and expense that can be incurred in dealing with DSARs and helpfully reiterates that controllers are not obliged to conduct searches which go beyond what is reasonable in terms of time and money, taking the specific circumstances into account. For example, where deleted emails are easily retrievable by searching the deleted folder in an email inbox, then this should be included in the search. However, if the emails are permanently deleted in accordance with the employer's retention policy, the employer is not expected to implement technology to retrieve this deleted information unless it is readily or already available to the employer.

Redaction

How far redactions should go when responding to employee DSARs is always a hotly debated topic and different organisations take different approaches to this. The DPC has a separate guidance, 'Redacting Documents and Records', which is an additional resource for employers when considering their DSAR processes. In the most recent version of this, the DPC points out that redaction of names may not be enough to render third parties unidentifiable and that other details, for example their position in the organisation may need to be redacted to ensure a third party can't be identified.

However, employers should remember that the employee is entitled to be informed about the context in which their personal data are used and should be able to have 'meaningful interaction' with their personal data so an appropriate balance needs to be achieved when considering redactions.

Charging for providing the response

The Guidance reiterates the position under the GDPR that controllers may, in limited circumstances, be able to charge a reasonable fee based on their administrative costs. This would arise where two or more access requests are manifestly unfounded or excessive, or where additional copies of the personal data have been requested. In our experience, this rarely arises in the employment context. The DPC also points out that there is a high threshold to prove that a request is unfounded or excessive.

Restrictions on the right of access

The Guidance sets out a helpful summary of some of the limits on the right of access under Irish legislation. The most relevant and potentially useful exemptions for employers when considering an employee DSAR are:

- Section 60 of the GDPR: processing for important objectives of general public interest (e.g. to exercise or defend a legal claim or in relation to opinions given in confidence); and
- Section 162 of the GDPR: processing related to legal advice, privileged communications, or court orders.

Where an employer relies on a relevant exemption to withhold certain information, they will have to identify the relevant exemption, explain to the employee why it applies and consider conducting a necessity and proportionality test. They are also obliged to inform the employee of their right to lodge a complaint to the DPC or seek a judicial remedy. It is also important to remember that utilising the 'expression of opinion given in confidence' exemption in the employment context is extremely difficult and generally employees will be entitled to see emails where managers discuss them, regardless of how potentially embarrassing or problematic disclosing these emails may be for the employer.

Conclusion

DSAR-related complaints and litigation is only likely to increase, and so employers should continue to keep their DSAR processes under review to ensure employee DSARs are properly addressed and to minimise the risk of challenge. The Guidance reminds us that there is no one size fits all approach to handling DSARs and each request must be considered based on its own facts and the context. While the Guidance is helpful for employers, it also highlights that handling employee DSARs continues to be a burdensome and challenging area.

Our advice to employers is to ensure anyone dealing with employee DSARs is aware of the Guidance and that, where possible, reference is made to it in any decisions made in respect of individual DSARs, particularly where organisations are limiting their response to an employee or seeking to extend the timeline for response.

Linda Hynes
Partner
linda.hynes@lewissilkin.com