Data protection and employment — Part I

In the first of a new six part series on data protection issues which arise in the context of handling employee information, Oisin Tobin and Phillip Nolan from Mason Hayes & Curran consider staff subject access requests — what must be disclosed and what can be withheld

Under Section 4 of the Data Protection Acts 1988 and 2003 (the 'Acts') an employee is entitled, subject to a number of explicit exemptions, to receive a copy of his or her personal data as held by their employer.

Effectively responding to such 'subject access requests' is a challenge for many organisations. This challenge flows from the somewhat complex drafting of the relevant provisions of the Acts, and is accentuated by the fact that such requests are often made in the context of litigation or some other dispute between employer and employee. In such circumstances, there is a natural tension between the employee's right to obtain a copy of their personal data, and the desire of an employer to withhold certain types of information to protect either their own interests, or those of another employee.

This article explains how employers can navigate this tension, and sets out a framework for thinking about, and responding to, subject access requests in an employment context.

Subsequent articles in this series (to be published in consecutive editions of this journal) will explain how data protection law applies to: monitoring staff activities and communications, including using line managers, private detectives, CCTV cameras and website monitoring technologies (Part II); disclosing staff information to outside third parties — the legal requirements that must be met before staff information can be sent outside the organisation (Part III); retaining staff records, including setting appropriate periods of time for keeping information (Part IV); data protection issues arising from mergers and acquisitions (Part V); and the role of the Data Protection Commissioner and what to do if he instigates an investigation (Part VI).

Structure

It is useful, when approaching subject access requests, to adopt a clear process. Such a process should involve the following steps:

- reviewing the request;
- collating all relevant personal data;
- assessing that personal data in light of statutory exemptions; and
- responding to the request.

At all stages it should be borne in mind that a subject access request must be responded to within 40 days of receipt. The Acts contain no explicit provision allowing for an extension of this time limit due to the scale or difficulty of the request.

Reviewing the subject access request

At the outset, the employer should satisfy itself that a proper subject access request has been received.

The Acts do not set down any formal requirements for a subject access request, other than that the request be 'by notice in writing'. In practice, most requests will be made by way of letter, often prepared by the employee's lawyer or based upon a template suggested by the Data Protection Commissioner ('DPC'). It should be noted that, as a result of the Electronic Commerce Act 2000, 'writing' includes communication via an electronic medium. Consequently, employees will also be able to make a subject access request via email.

Upon receipt of a request, the employer is entitled to demand the provision of such information as may reasonably be required to identify the requestor. In an employment context, an employer may be satisfied that the relevant request relates to an identified employee and may not seek any further information.

Employers, like all data controllers, are entitled to charge a fee of €6.35 to respond to a subject access request. Should an employer decide that it will require a fee prior to responding to any subject access requests, it is advisable that this policy be clearly stated in the employee handbook or the organisation's data processing policy documents.

It should be noted that, in the case of numerous requests from the same employee, an employer may refuse to furnish any further information. Section 4(10) of the Acts provides that, where a data controller has previously complied with a subject access request, it is not obliged to respond to an identical or similar request by the same individual unless, in the opinion of that data controller, 'a reasonable interval has elapsed between' the two requests. When determining whether a reasonable period has elapsed, regard should be had to 'the nature of data, the purpose for which the data are processed and the frequency with which the data are altered'.

What information is within the scope of the subject access request?

Subject access requests are very broad in scope. In terms of content, they take in all 'personal data' relating to an employee. This includes all information relating to an employee which is stored electronically or which is held, in hard copy, in a structured filing system (for example paper files, where the content organised chronologically or alphabetically by employee). This goes beyond an employee's HR file and may, for example, include emails relating to a given employee.

The scope of such requests means that it is not sufficient to merely hand over an employee's file. The employer will need to take further, proportionate steps to pull in all personal data held about the employee. (The reference to 'proportionate' is in terms of the effort required — see section 4(9) of the DPAs).

"An employer cannot simply withhold a document because it makes reference to a third party. If the redaction of the third party's details could effectively conceal that third party's identity, the document should be redacted and handed over. Experience has shown that the DPC has a preference for data controllers providing limited redacted information, as opposed to withholding all documents."

What information can be withheld?

Sections 4 and 5 of the Acts lay down a number of exemptions to the scope of a subject access request. It is the view of the DPC that these exemptions are exhaustive. Consequently, if personal information cannot be brought within the scope of one of these exemptions, it must be disclosed. The key exemptions that may apply in an employment context are categorised into the four headings below.

Data relating to other employees/ individuals

Section 4(4) of the Acts makes clear that an employer, when responding to a subject access request, does not have to disclose personal data relating to anyone other than the employee making the request. Indeed, one could argue that the employer has a separate obligation to such third parties to avoid unnecessarily disclosing their personal data. However, an employer cannot simply withhold a document because it makes reference to a third party. If the redaction of the third party's details could effectively conceal that third party's identity, then the document should be redacted and handed over. Experience has shown that the DPC has a preference for data controllers providing limited redacted information, as opposed to withholding all documents.

Opinion given in confidence

Section 4(4A) of the Acts provides that the expression of an opinion about the data subject given by another person does not need to be disclosed if that opinion was given in confidence, or on the understanding that it would be treated as confidential. The scope of this exemption is often a source of contention. It should be noted that the DPC has tended to take a very narrow interpretation of its scope, and has suggested that the exemption will only apply in cases where the opinion would not have been given but for the understanding that it was to be treated as confidential. The DPC has further stated that the mere fact that a document is marked confidential is insufficient to invoke this exemption, and that this exemption does not generally cover references or reports given by managers or supervisors about their subordinates. Consequently, it appears that the exemption has largely been limited to circumstances where confidentiality is of utmost concern, such as whistleblowing or complaints made by one staff member against a colleague.

Employers seeking to use this exemption more broadly are likely to encounter resistance.

Legally privileged information

Pursuant to Section 5(g) of the Acts, personal data that are legally privileged do not need to be disclosed. From an employer's standpoint, this is a very useful and important exemption, particularly as its scope is well litigated and certain, in contrast to some of the more nebulous exemptions discussed above. At a high level, all documents prepared in contemplation of litigation

(Continued on page 8)

(Continued from page 7)

or providing legal advice are legally privileged. This would encompass, for example, solicitors' letters advising on disciplinary proceedings and medical reports which were specifically prepared to defend litigation, such as in an employer's liability case (for an example, see *Mayo VEC v. Data Protection Commissioner*, unreported, Circuit Court, 12th February 2010). However, it should be remembered that the mere fact that material, such as CCTV footage, is evidence in litigation does not render it legally privileged (see *Dublin Bus v. Data Protection Commissioner*, unreported, 5th July 2011).

Proportionality

Section 4(9) of the Acts allows a data controller to avoid supplying personal data if to do so would involve disproportionate effort. Given the burden that subject access requests impose on employers, there may be a temptation to rely on this exemption as a ground to avoid handing over personal data. However, employers should note that the DPC has tended to take a narrow construction of this exemption, and this ground is generally only accepted where physically finding and producing the relevant personal data is an onerous task. For example, an employer that has produced employee's HR and management files may be able to invoke proportionality as a justification for not conducting an exhaustive, and very expensive, search of all electronic communications on their network that may refer to the employee in some tangential way.

"Pursuant to Section 5(g) of the Acts, personal data that is legally privileged does not need to be disclosed. From an employer's standpoint, this is a very useful and important exemption, particularly as its scope is well litigated and certain, in contrast to some of the more nebulous exemptions discussed above. At a high level, all documents prepared in contemplation of litigation or providing legal advice are legally privileged."

Responding to the request

Having collated the relevant information and redacted or removed documents in reliance on the above exemptions, the employer will be in a position to formally respond to the subject access request. At this point, it is quite useful for an employer to prepare three files: two files containing all information which will be provided to the employee (one to be sent to the employee and the other for the employer's own records) along with a third file setting out all personal data relating to that employee, including personal data which has been withheld. This last file provides an important paper trail in the event of an investigation.

The response to the employee should be covered by a letter which informs the employee of their right to complain to the DPC (as required by Section 4 (7) of the Acts) and which also informs the employee of the categories of personal data being processed by the employers, the purposes for such processing and the identities or categories of any recipients to whom the data may be disclosed. Provided it is sufficiently robust, enclosing a copy of the employer's HR privacy policy may suffice for these purposes.

Conclusion

As can be seen from the above, subject access requests pose significant challenges for employers. The key to meeting this challenge is preparation. If an employer is likely (perhaps due to its size) to receive regular subject access requests from current or former employees, it should seek to implement a clear internal procedure to effectively deal with such requests.

Philip Nolan and Oisin Tobin
Mason Hayes & Curran
pnolan@mhc.ie
otobin@mhc.ie