Handling data access requests — the blueprint

Davinia Brennan, Associate in the Litigation and Dispute Resolution department at A&L Goodbody, sets out an approach to handling access requests, informed and referenced by case studies from the DPC's Annual Reports

Recent data privacy scandals at home and abroad, such as the Garda taping scandal and the Edward Snowden saga, have put data protection in the spotlight. Along with an increasing awareness by individuals of their data protection rights, there has been a corresponding growth in data access requests made by individuals under the Data Protection Acts 1988 and 2003 ('the DPAs').

The Annual Report of the Data Protection Commissioner ('the DPC') for 2013, published in May 2014, notes that over 50% of complaints received by his Office during 2013 concerned difficulties faced by individuals in obtaining access to their personal data. Organisations often encounter difficulties in responding to access requests due to the amount of personal data involved or the nature of the request. Requests are frequently from aggrieved customers or employees, made in the context of litigation or some other contentious situation, and typically conflict arises between the data subject's legal right to obtain a copy of their personal data, and a data controller's preference to withhold certain types of information to protect their own interests.

This article looks at the scope of the right of access to personal data, the key statutory exemptions, and some case studies from the DPC's Annual Reports, which demonstrate his approach to enforcement of the statutory right of access.

The right of access to personal data

Section 4 of the DPAs provides data subjects with a right to obtain a copy of any information relating to them which is kept on computer or in a structured manual filing system, by any organisation. An individual's right to a copy of their personal data is subject to certain statutory exemptions, as discussed below.

A four step procedure to dealing with requests

Organisations should streamline their procedures for dealing with access requests, in order to save time and effort, and to ensure compliance with the DPAs. Four key steps might be adopted, including:

- checking that the request is valid;
- locating and collating all personal data relating to the requester;
- reviewing the personal data in light of the statutory exemptions; and
- responding to the request within the statutory time limit.

1. Checking that the request is valid

Upon receipt of an access request, an organisation is entitled to demand evidence of identity from the requester (to ensure he is the data subject), and to charge a maximum fee of €6.35.

There are no formal requirements in the DPAs regarding access requests, other than that the request should be 'in writing'. This can be via letter or email. Individuals may be invited to use a particular access request form, but organisations cannot insist on individuals doing so. An organisation should seek clarification in regard to the scope of the request where it is not obvious, in order to avoid unnecessary searches. The date of receipt of the request should also be logged, as the DPAs require a response to the request within 40 days.

It is highly advisable for organisations to appoint a coordinator or Data Protection Officer who will be responsible for responding to access requests, and collating the relevant data.

2. Locating and retrieving all personal data relating to the requester

A requester is entitled to ask for a copy of all information held about them. The definition of 'personal data' in the DPAs is very broad. It includes: 'data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of

the data controller'.

Data access requests constitute a significant burden on organisations both administratively and financially. A recent Opinion by the Advocate General ('AG') of the Court of Justice of the European Union ('CJEU'), in Joined Cases C-141/12 and C-372/12, may serve to lighten this burden, if it is followed by the judges of the CJEU. The AG found that the Data Protection Directive (95/46/EC) does not establish a right of access to any specific document or file in which personal data are listed or used, nor does it specify the material form in which personal data must be made accessible. Member States enjoy a margin of discretion to determine the form in which to make personal data accessible. Therefore, the AG found that the Dutch authorities had met their legal obligations under data protection law by extracting from the relevant documents the personal data relating to the applicant.

"Organisations should be aware that the disproportionate effort exemption can generally only be relied upon where finding and producing the relevant personal data would be disproportionate to the benefit to be derived by the data subject in receiving a copy of the data."

Organisations should ensure that they keep a note of all steps taken to find and retrieve all the personal data, in case of any subsequent investigation by the DPC.

3. Consider whether any of the statutory exemptions apply

The right of access is subject to certain exemptions set out in Sections 4 and 5 of the DPAs. If personal information cannot be brought within the scope of one of these exemptions, it must be disclosed. The narrow scope of the exemptions, and the fact that they do not offer blanket protection to entire documents falling within their scope, but rather to particular parts, sections or sentences of the documents, has been highlighted by the DPC in numerous case-studies contained in his Annual Reports.

Some of the most common exemptions include: an opinion given in confidence; disproportionate effort; third party data; repeated access requests; data concerning the investigation of an offence; data protected by legal professional privilege; and health data.

Opinion given in confidence: The DPAs contain an exemption in respect of opinions given in confidence about the data subject. However, the DPC has repeatedly warned that a very high threshold of confidentiality must be met before this exemption may be invoked to refuse a requester access to his or her personal data. It only applies where the opinion would not have been given but for the understanding that it would be treated as confidential.

In case study 11/2013, the DPC indicated that it is not sufficient that the document is marked 'confidential', and that references or reports given by managers or supervisors will not generally be protected by this exemption, as it is an expected part of their role to give opinions on staff which they should be capable of standing over. Therefore, it seems this exemption is limited to circumstances where confidentiality is of utmost concern, such as whistleblowing or complaints made by one staff member against another. In the case mentioned above, the DPC, having examined an email containing the personal data sought, found that the author was in a position of some authority over the data subject and that the document in question should be disclosed to the employee.

In case study 10/2011, the DPC noted a recurring theme of financial institutions withholding personal data in credit assessments, or submissions to credit committees, on the basis that they involved expressions of opinion given in confidence. The DPC highlighted that a financial services employee must be able to stand over any opinion he/she gives on a customer, and warned that any further reliance on this exemption to withhold such data would be met with enforcement proceedings.

Disproportionate effort: Organisations are required to supply a requester with a copy of their personal data in permanent form, unless the supply of such a copy is not possible, or would involve disproportionate effort. Organisations should be aware that the disproportionate effort exemption can generally only be relied upon where finding and producing the relevant personal data would be disproportionate to the benefit to be derived by the data subject in receiving a copy of the data.

Third party data: Where an organisation cannot comply with an access request without releasing information relating to another individual, then that information may be withheld (unless that other individual has consented to the disclosure). However, where it is possible to redact the particulars identifying the other individual, then the organisation should do so, and release the remaining information.

Repeated access requests: Where an organisation has previously complied with an access request, it does not have to comply with an identical or similar request from the same individual unless 'a reasonable interval' has elapsed. In determining whether a reasonable interval has elapsed, the DPAs require regard to be had to the nature of the data, the purpose for which the data are processed, and the frequency with which the data are altered.

Investigation of an offence: If granting access to personal data could potentially prejudice a criminal investigation, then access may be

(Continued on page 6)

(Continued from page 5)

refused. In case study 3/2012, the complainant, a healthcare assistant in a nursing home, complained that the Health Information and Quality Authority had refused his access request to personal information relating to an incident he had been involved in at work. The Authority claimed that it held the data in question for the purpose of investigating offences under the Health Act 2007. The DPC advised the Authority that a prejudice test applies to the applicability of this exemption, and the mere existence of the investigation did not permit the exercising of a blanket exemption by the Authority across all personal data held by it. The DPC further highlighted that the exemption is not a permanent one. When an investigation is completed, and the prejudice no longer exists, a copy of the personal data must be made available to the data subject. Following the DPC's investigation, the Authority agreed to provide the requester with the data concerned, on the basis that no prejudice would arise by release of such data.

Legal Professional Privilege ('LPP'): The DPAs specifically provide that the right of access does not apply to personal data 'in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers'.

Case study 13/2013 demonstrates the use of a data access request as a litigation tool. The DPC investigated a refusal by a claims adjuster firm to supply CCTV footage to a data subject relating to an incident involving him. The DPC noted that the ruling of the High Court in *Dublin Bus v The DPC* [2012] IEHC 339 (which concerned an access request for a copy of CCTV footage of a woman falling on a bus), had clarified that the existence of legal proceedings between a data requester and the data controller does not preclude an access request under the DPAs, nor does it justify the data controller in refusing the request. As a result, the claims adjuster released a series of photographic stills from the CCTV footage, which showed the requester's image only. The DPC held this was satisfactory, as no audio had been recorded on the data controller's CCTV system.

Case study 13/2011 further demonstrates that the DPC considers that the LPP exemption cannot be applied to refuse an access request for a copy of a surveillance report or accompanying photographs or video footage taken by a private investigator, hired by a data controller or by a solicitor on their behalf. The DPC stated that the LPP exemption 'does not equate to privilege at common law'. He indicated that the LPP exemption in the DPAs does not extend to communications between a client and a third party or his legal adviser and a third party made in anticipation of litigation. It remains to be seen whether the courts will uphold such a narrow interpretation.

Health data: The right of access to health and medical records is also subject to a limited exemption. Statutory Instrument No. 82 of 1989 provides that health data relating to an individual should not be made available to that individual, in response to an access request, if it would be likely to cause serious harm to the physical or mental health of the data subject. A data controller who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor or some other suitably qualified health professional.

4. Responding within the 40 day time-limit

Having retrieved the relevant information and redacted or removed documents in reliance on the exemptions, organisations should then respond to the request. The requester should be supplied with a copy of their personal data in permanent form, unless the supply of such a copy is impossible, or would involve disproportionate effort, or the data subject agrees otherwise. In addition, the DPAs require the requester to be informed of the categories of personal data being processed, the purposes of such processing, the identity of any recipients to whom the data may be disclosed, and details of the source of those data, where available (unless such information would be contrary to the public interest). Furthermore, any refusal of an access request must be 'in writing', and include a statement of the reasons for the refusal, and inform the requester that he or she may complain to the DPC about the refusal.

The statutory 40-day time limit to respond to a request does not begin to run until the application fee is paid or any further information relating to the identity of the requester or the location of the data is supplied. However, a data controller who intends to charge the discretionary fee for an access request must do so at the earliest opportunity within the 40-day time limit.

In case study 2/2012, the DPC found that a telecommunications company had contravened section 4(1) of the DPAs by not providing the relevant personal data within the 40 day time limit. The company had requested the fee more than two months after receipt of the access request, and did not commence processing the request until the fee was received.

Enforcement of right of access by the DPC

If a data subject is dissatisfied with a response to a valid access request, or where there has been a failure to respond, then the data subject may make a complaint to the DPC. The DPC will investigate the matter (unless he is of the opinion that it is frivolous or vexatious) and ensure a data subject's rights are fully upheld. If the DPC is unable to reach arrange for an amicable resolution within a reasonable time, he will make a formal decision. Where the data controller is in contravention of the DPAs, the DPC may serve an Enforcement Notice requiring him to take such steps as are specified in the notice, within such time as may be specified. Failure to comply with an Enforcement Notice is an offence punishable by a fine of up to €3,000 on summary conviction, or €100,000 on indictment. Any decision or Enforcement Notice may be appealed to the Circuit Court by the data subject or data controller, respectively.

Case study 6/2008 shows that the DPC will use his legal powers when necessary in order to uphold the rights of a data subject. In this case, the

DPC served an Enforcement Notice due to a Health Club not complying with an access request relating to the data subject's membership, in contravention of section 4(1) of the DPAs. The Health Club also failed to explain the reasons for refusal, contrary to section 4(7) of the DPAs. In addition, it failed to co-operate with the DPC's statutory investigation, ignoring correspondence and phone calls from his Office. As a result, the DPC sent two of his authorised officers to the premises of the Club to carry out an inspection, whereupon further personal data relating to the data subject was discovered. Soon afterwards, an amicable resolution was achieved.

Conclusion

The key to dealing efficiently with data access requests is having in place a clear internal procedure. Organisations should also be upfront in explaining to individuals how they can request their personal data. In addition, as highlighted by the DPC in his Annual Report for 2013, it is important to ensure effective customer service systems are in place, as this will assist in pre-empting data access requests.

The adoption of transparent policies and procedures concerning data-handling practices should increase trust and confidence in an organisation, and reduce the likelihood of any complaints and costly disputes arising.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com