Handling access requests — lessons from the Access Rights Index

Thierry Bernard, Partner at law firm Quadrige in Paris, explains what organisations subject to French data protection law can learn from the results of a recent survey, the Access Rights Index

A recent survey carried out in France by the French Association of Data Protection Officers (in partnership with the 'High Institute of Electronics of Paris') on the rate and quality of organisations' responses to subject access requests (the 'Access Right Index', 28th January'), revealed that less than 20% of responses met the legal requirements. Further, less than two thirds of the respondent organisations answered within the stipulated two month period.

This Access Rights Index highlights the necessity for public and private organisations in France, and foreign companies with operations in France, to improve or, in some cases, to set up a management policy in relation to the access rights afforded to data subjects under French data protection law (implementing Directive 95/46/EC).

This article examines the questions raised by the key findings of the Access Rights Index for organisations seeking to comply with the Act.

Data subjects' rights in France are protected via Act n°78-17 of January 6th, 1978 on Data Processing, Data Files and Individual Liberties ('the Act'), supplemented by decree n° 2005-1309 of 20th October 2005 ('the Decree').

It is in organisations' interests to seek to comply with the Act because:

i) the public are increasingly aware of their rights (even if this is not reflected in its exercise of those rights); and

ii) since 2004, the CNIL (the French Data Protection Authority) is invested with greater powers of enforcement (Law n° 2004-801 of 6th August, 2004). The CNIL can impose fines of up to 150,000 euros, or to 300,000 euros in case of a second offence. Further, a private bill which was notified to the Senate on 6th May 2009 proposes a doubling of these fines.

Rights of individuals in respect of processing of personal data

The first right afforded to individuals is to be informed about the existence of their right to access their own personal data. The data controller must, on or before the point that the data are collected, inform individuals of their right of access, and, in certain circumstances, their rights of rectification and deletion (Articles 32 and 40 of the Act).

The Act specifies that, to enable data subjects to exercise their rights of access, the identity of the data controller must be indicated through the material used for the collection of data or, failing this, through a document brought to the attention of the data subjects in readable characters, prior to the data collection (Article 90 of the Decree).

The data controller should also provide, the contact information for the department where data subjects should direct their requests of access, opposition and correction (under the same conditions as above).

Responding to access requests

Individuals can exercise their rights to access their data either in writing or in person. Also, where the data controller allows access to the data in his premises, it may be done only subject to the protection of the personal data of third parties. Applications on which a decision cannot be taken immediately warrant a dated and signed notice of receipt to be delivered to the applicant. In any case, the data controller should respond to an application presented by a data subject within two months of receipt. However, if the application is vague or does not contain all the items allowing the data controller to carry out the operations required, he can ask the applicant to clarify. The request for further information has the effect of suspending the two month period.

Data subjects should be able to exercise their access right free of charge, though there is provision for a data controller to charge for the costs of reproducing the information in certain, specified, circumstances.

It is clear from the legal obligations, as well as from the Access Rights Index, that a certain number of precautions must be taken in order to properly answer access requests:

Training of individuals tasked with responding to data subjects — The Access Rights Index recorded the errors in responses ranging from errors in the name of the addressee, failures to

accurately identify a request (sample answer: "Have you a problem with your subscription?"), and even in the understanding of the law ("We are owners of the data and we do not communicate them").

One of the first lessons to be learned from the AFCDP's survey is that, before answering the access requests, it is essential to have appointed particular individuals as responsible for the service, and to have informed and trained them in the law.

Verifying the identity of the applicant — The data controller must take measures to ensure that he ascertains the identity of the individual applying for the implementation of his rights. Such rights are strictly reserved for the data subject.

Where they are presented in writing to the data controller, the data controller must check that the applications for the implementation of the rights is signed and accompanied by the photocopy of an identity card showing the signature of the holder.

Where there is any doubt about the address indicated or the identity of the applicant, the answer may be dispatched by registered mail without notice of receipt, and the address or the identity of the applicant should be checked at the time of the delivery of the mail.

Where an application is presented in person, the interested party must prove his identity to the data controller by any means. He may be advised by a counsel of his choice. The application may also be presented by a person especially empowered for that purpose by the applicant, who must show his power of attorney, his identity, and the identity of the principal.

Obligation to constantly monitor the data held — Individuals' access requests may highlight inaccuracies in the data held. Article 6 of the Act requires personal data to be kept accurate, relevant and up to date. This can be done either from the organisation's own information or at the request of the persons concerned. Also, the duration of the data's retention is limited by the requirement for it to be proportionate to the purpose of the data process and, in any case, in accordance with the duration specified in the initial notification or request of authorisation of the data processing with the CNIL.

Compliance with the above provisions requires being able to centralise the information and to establish automatic processes for updating.

Organisations should avoid dealing with companies that sell directories of data on customers on CD-ROM: the CNIL has imposed fines of up to 30.000 euros for uses of such directories. In some cases, the organisation in question had purchased lists of customers which turned out to be obsolete, on the grounds that "by nature, the CD-ROM support cannot be updated although several tens of thousands modifications intervene every day on the data base directory" (the 'Isotherm' case, 27th November 2008).

Ensuring that data subjects' intentions are communicated between data controllers — The individual that receives objection or correction requests should immediately communicate the data subject's request to any other data controller to whom the said individual has previously sent the data (Articles 97 and 99 of the Decree). This is a 'best efforts' obligation, with the requirement being to achieve this as far as possible without disproportionate effort.

Respect response times and ensure the clarity of responses — In cases where the data controller was liable for failures in relation to requests to unsubscribe from its mailing lists, the CNIL has specified that it considered that the data controllers should handle the requests of opposition "in an effective, systematic and immediate way" ('CDiscount' Case, 6th November 2008). In one particular case where an organisation was fined 30,000 euros, the CNIL noted that there was no automated system for the management of the requests to unsubscribe, that the process did not allow for requests received by mail, and that the system for unsubscribing was unnecessarily complex (for example, it required the consumer to enter a password).

The responses of data controllers must be complete (the CNIL, in the 'Neuf-CI' Case, 12th June 2008, fined an internet provider 7,000 euros when it answered only partly to repeated access right requests of a customer) and clear: the codes, initials and abbreviations appearing in the documents delivered by the data controller must be clarified (Article 95 of the Decree).

The decision of the data controller to refuse to comply with a data subject's request must indicate the mechanisms for appeal, and deadlines (Article 94 of the Decree).

Proof that the requests of opposition or rectification have been carried out — Upon the data subject's request, the data controller has to justify, free of charge, when it carried out the request for deletion, rectification, etc.

Not to answer — French law authorises the data controller not to answer requests for access, rectification or deletion when the requests are obviously abusive, whether it is by their number, or their repetitive or systematic character (Article 94 of the Decree).

Appointment of a CIL — The law establishes the role of 'Correspondant Informatique et Libertés' or 'CIL' (the data protection officer), which can either be an employee of the data controller or an outside person. Though the appointment of CIL is not mandatory, according to Access Rights Index, there was a higher rate of compliance in responding to access requests amongst organisations that had appointed CIL's, with 80% of answers meeting the obligations in terms of timeliness and quality.

The advantages of appointing a CIL are that it helps organise the centralisation of the function of data protection compliance relating to the data files within the organisation, as well as helping to achieve the aim of broadcasting legal and security rules.

The private bill mentioned above plans to make the appointment of a CIL compulsory for private or public organisations which process personal data and have more than fifty individuals with direct access to the data or responsible for its implementation.

Thierry Bernard
Quadrige, société d'avocats
tbernard@quadrige-avocats.com