BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Security & Surveillance

French Data Protection Authority Sets Conditions For Whistleblowing

Jan Dhont
Crowell & Moring
Brussels.

Reprinted from the December 2005 issue of BNA International's
World Data Protection Report

French Data Protection Authority Sets Conditions For Whistleblowing

By Jan Dhont, an Associate with Crowell & Moring, Brussels. The author may be contacted at jdhont@crowell.com

For some time, there has been a degree of uncertainty surrounding the legal status of ethics hotlines in France. Recent documents adopted by the French Data Protection Authority (CNIL) however, have gone some way to providing clarification in this regard.

On November 10, 2005, the CNIL adopted an "orientation document" ("document d'orientation") that outlines the conditions on which the CNIL will insist that whistleblowing procedures ("dispositifs d'alerte professionnelle") comply with the French Data Protection Act.[1] In its orientation document, the CNIL announced in principle that it will no longer be opposed to such procedures if individuals' data protection and privacy rights are guaranteed as outlined within the orientation document. The CNIL also stated that, in a second phase, it will issue a "single authorisation decision" ("Décision d'autorisation unique") to simplify formalities for companies. It is expected that the decision will be published before the end of 2005.

In May 2005, the CNIL refused to authorise the implementation of McDonalds' and Exide Technologies'[3] ethics hotlines or "whistleblowing" hotlines, designed to ensure compliance with Sarbanes-Oxley requirements, in France.[4] The CNIL determined that anonymous hotlines are disproportionate to the objectives sought and create risks of slanderous denunciation. In refusing to authorise McDonalds' and Exide Technologies' hotlines, the CNIL made it clear that it considered the company's approach to whistleblowing to be incompatible with the French Data Protection Act, finding that the harm to an individual's professional reputation that could result from potentially abusive and anonymous reporting could be of a greater threat to an individual's right to privacy, reputation, and autonomy than the damage that the hotline is seeking to prevent. The CNIL thought that a more transparent and less invasive method of reporting would offer a more legitimate solution to the problem Sarbanes-Oxley sought to remedy, and would ensure better protection for the privacy and personal autonomy of employees.

These decisions have far-reaching consequences for the French subsidiaries concerned, which risk criminal and civil sanctions if they by-pass the CNIL's decision. Furthermore, the CNIL's decisions appear to be upheld by the French courts. On September 15, 2005, the Libourne Court of First Instance prohibited Bsn Glasspack – an affiliate of the Oxens Illinois Group – to roll out its ethics line.[5] In reaching its summary conclusions, the court echoed the CNIL's concern that the threat to due process and civil liberties that may result from anonymous reporting and subsequent investigation is disproportionate to the harm that the procedures seek to prevent. Finally, many companies with E.U. operations feared that other E.U. national authorities would follow the CNIL's decision, and that corporations, in attempting to respond to the CNIL's decision, would risk failing to comply with the requirements of Sarbanes-Oxley or would be forced to abandon a uniform approach to reporting ethics violations.

CNIL Guidance: Requirements for Whistleblowing Procedures

The orientation document formally states that the CNIL is no longer opposed to the implementation of whistleblowing procedures, such as ethics hotlines.[6] Whereas the CNIL, in both the McDonald's and Exide Technologies cases, presumed that ethics lines are intrinsically threatening to individuals'personal autonomy and therefore illegal, the CNIL now takes the view that the French Data Protection Act does permit whistleblowing procedures, but only under strict conditions. In the simplest terms, the CNIL's orientation document indicates that the CNIL will engage in a proportionality assessment to determine whether particular whistleblowing procedures are permissible. In addition to ensuring respect for general principles of law (*e.g.,* due process and rights of defence), and specific labour law requirements (*e.g.,* involvement of the Works Councils), the CNIL states that corporations should (i) have objective and legitimate interests to implement ethics lines, and (ii) ensure that the pursuance of such interests is adequately counter-balanced with effective guarantees to preserve employees' individual autonomy. The orientation documents provides guidance to help corporations strike the right balance.

Condition 1

Whistleblowing procedures should be (i) complementary in nature; (ii) restrictive in scope; and (iii) facultative. These requirements are basic to the orientation paper and reflect the above-mentioned proportionality principle.

First, ethics lines may not overlap with existing complaint and control mechanisms that are imposed on corporations by French law. For instance, French company law requires that company accounts be reported to an independent body of "commissaires aux comptes" (audit committee) for review. Ethics lines should not replace existing legal communication and control mechanisms, but can be used to notify irregularities arising in the context of such existing control mechanisms.

Second, whistleblowing procedures permitted by the hotline should be limited in scope to reflect the requirements of Sarbanes-Oxley. The CNIL considers that they may cover the following matters: (i) accounting and financial matters; (ii) bank-related matters; and (iii) fight against corruption. Procedures to report a broader range of workplace irregularities, including "respect for legal rules, work regulations and internal rules of professional conduct", are considered problematic given the risks of misuse, *i.e.,* professional denunciation. The CNIL believes that utilising an ethics hotline for such broad purposes is disproportionate in light of employees' professional and personal integrity.

As is the case with all personal data processing operations, data controllers must be able to invoke one of the predefined

  WDPR ISSN 1473-3579

legal bases to justify their data processing operations. According to the CNIL, the processing of alerts or complaint reports in the context of an ethics hotline may be based on (i) a legal requirement to have an ethics line in place;[7] or (ii) a legitimate and established interest of the data controller under the condition that the data subject's interests or fundamental rights and freedoms are not ignored.[8]

Perhaps most importantly, the CNIL takes the position that a whistleblowing procedure may be legitimate only in light of French legal requirements regarding internal controls (*e.g.,* requirements imposed on the banking sector).[9] According to the CNIL, an obligation of foreign law to have an ethics line in place cannot serve as a legal basis to process personal data under French law. Consequently, section 301(4) of the Sarbanes-Oxley Act, which requires publicly-traded U.S. companies to implement whistleblowing mechanisms for accounting or auditing matters, does not constitute a legally justifiable basis on which to process alerts and complaint reports.[10]

However, the CNIL goes on to state that it considers the Sarbanes-Oxley obligations imposed on publicly-traded U.S. companies to be a legitimate corporate interest, justifying the implementation of an ethics hotline for accounting controls and auditing matters alone. Of course, as regards such matters, corporations will need to ensure that all data protection rights are effectively guaranteed in order to ensure that employees" privacy rights are not overridden. In practice, many U.S. companies have broadened the scope of their whistleblowing procedures and allow alerts on matters other than mere accounting and auditing, such as compliance with other legal requirements or a more broadly-defined code of conduct. Although receiving complaints beyond accounting and auditing irregularities may fall outside of the formal Sarbanes-Oxley requirements, an argument can be made that alerts concerning violations of internal codes of conduct also constitute a legitimate corporate interest, particularly if the conduct at issue is legally sanctionable. The CNIL did not however, endorse such a broad use of ethics hotlines and, therefore, there is a risk that ethics lines that are broader in scope will not be eligible for regularisation under the CNIL's single authorisation decision.

Finally, the CNIL has clarified that the use of whistleblowing procedures to fight corruption and fraud are also considered legitimate.[11]

In the context of the announced authorisation procedure, the CNIL will closely review whistleblowing procedures that are broader in scope than the abovementioned matters. In conducting its assessment of whistleblowing procedures, the CNIL will also consider whether employees are obliged to use a whistleblowing procedure, and continues to view any such obligation as contrary to French law. Thus, the use of a hotline should remain a faculty amongst other control mechanisms. As discussed below, employees will need to be informed about the employer's expectations of the use of the hotline.

Condition 2

Strictly define the categories of individuals that may be subject to reporting in light of the legal requirements or legitimate interests that allow a whistleblowing procedure.

This requirement is derived from the proportionality principle according to which personal data may be processed only if such data is objectively required to reach the purposes of the processing. According to the CNIL, workers at the low end of the organisational hierarchy are generally not involved in accounting and auditing matters and should, therefore, not be the subject of an alert. While there is some sense to this distinction in theory, implementing a hotline that distinguishes between potential wrongdoers – *i.e.,* identifying "reportable" and "non-reportable" employees – is practically difficult and, in any event, is likely not sufficient to satisfy SOX requirements. In addition, this exercise may also be politically difficult and will, obviously, require involvement of the works council.

Condition 3

Avoid encouragement of anonymous denunciation.

In one of its most significant pronouncements, the CNIL states that providing a means whereby whistleblowers can be identified will minimise the likelihood that the system is misused to unjustifiably denounce employees. According to the CNIL, whistleblowers would feel responsible when using the system and think twice about the impact of the whistleblowing activity before making a hotline report. This lack of anonymity would, according to the CNIL: (i) avoid misuses such as slander and illegitimate denunciation of co-employees; (ii) allow the corporation to take measures to protect the whistleblower; and (iii) ensure higher efficiency by opening a means of communication to request additional information for purposes of an investigation.[12] The identity of the whistleblower should, of course, remain confidential and may, for instance, not be disclosed to personnel in the context of an access request.

Perhaps in recognition of the centrality of anonymity to the SOX reporting scheme, the CNIL does not outlaw anonymous reporting. Instead, the CNIL suggests that specific procedures should be implemented with respect to the communication and handling of complaints/alerts made by whistleblowers who can be identified, including: (i) a prior examination of the complaint to decide whether its communication within the organisation is opportune; and (ii) avoid inciting employees to anonymously conduct alerts. Corporations should have procedures in place to restrict the communication of alerts, internally and at the group level, both to ensure confidentiality and to enhance the efficiency of the investigations. Furthermore, the CNIL suggests that the system be set up in such a fashion that employees identify themselves when lodging a complaint, and that information is submitted referring rather to facts than to persons. While avoiding specific references to persons is obviously illusory, companies could and should pre-define a lexicon of objective facts – with enough detail – that are reportable.

Condition 4

Provide clear and complete guidance on the use of the system.

Potential users of the hotline should receive complete and clear information about the purposes of the hotline and reporting procedures, and should also obtain a notice in case they are the subject of an alert or a report. The obligation to inform data subjects is set forth by article 32 of the French Data Protection Act and requires that data controllers provide adequate notice on the following elements: (i) the identification of the data controller;[13] (ii) the

data processing purposes and the matters that may be reported; (iii) the facultative character of the system; (iv) the absence of sanctions in case the a matter is not reported by employees; (v) the recipients of the alerts; and (vi) the fact that data subjects have a right of access and rectification. The CNIL further requires that employees be informed about disciplinary or judiciary sanctions in case of misuse of the system and that a good faith use will not result in such sanctioning even if the facts reported prove to be inaccurate or do not lead to any prosecution or sanctioning. Companies will, by consequence, need to implement internal measures to carefully and promptly check the veracity and the quality of the facts reported, and purge any information that is inaccurate. Evidently, the application of the data quality principle should be interpreted in a reasonable fashion since the accuracy or veracity of the information may become clear only after a period of time.

Condition 5

Alerts and complaint reports should remain strictly confidential and may not be used for other purposes than for conducting the investigation.

Given the high sensitivity of the information processed in the context of a hotline, companies will need to take appropriate measures to ensure watertight confidentiality and information security during the communication and conservation of the alerts and reports. Although alerts do not necessarily contain sensitive data in the sense of the French Act or the Directive, the information processed may have great impact on employees' professional and personal integrity and may, therefore, be considered intrinsically sensitive by the data protection authorities. Pursuant to the CNIL, complaint reports should be conserved separately from other data. Any complaints should be formulated in an objective fashion, and all information registered within the system should be strictly necessary to verify the made allegations. Many companies have implemented hotlines that are fully compliant with these requirements.

Condition 6

Alerts should be pertinent, adequate and not excessive.

The alerts and reports that are conserved within the system should (i) be formulated in an objective fashion; (ii) directly relate to the legitimate purposes of the hotline – discussed under condition no.1; and (iii) be strictly necessary for the verification of the allegations made. While the requirement to process only factual and objective information subscribes to the logic of French and European data protection law, it may be difficult, if not impossible, to fully comply with these requirements at all stages of the process set up by a hotline. It is simply not the case that anonymously submitted hotline complaints will be clinically dry and objective, since the report will almost always involve the subjective perception of individual reporting the conduct. Alerts will generally result in the processing of suspicions and allegations for investigation, which may even qualify as sensitive "judiciary data" in some Member States.[14] The risks of processing of rumours and inaccurate suspicions can, in some ways, be reduced by ensuring swift investigation and by ensuring accurate and objective reporting in the intermediary and final stages of the investigation.[15]

Condition 7

Provide for a specific organisation within the company, consisting of trained people, that receives and handles the alerts/complaints.

The CNIL requires that companies set up a structure of professionally trained people who are dedicated to handle the alerts and conduct the investigation and reporting. Those individuals would need to be limited in number, specially trained and held by contractually binding confidentiality requirements. Although the CNIL refers to a group of specialised people within the company ("au sein de l'entreprise"), it will be important to comply with general principles of due process to ensure the independence of this body. At the same time, it may not be opportune or simply inefficient (trade and other secrets) to outsource an entire investigation to a trusted third party. While companies can rely on third parties, such as a call centre, to collect the alerts, part of the investigation will require expertise from inside the organisation, and the procedures will need to ensure that sufficient checks and balances are adequately implemented. In any event, the distribution of complaints within the company (or at the group level) should be absolutely minimised to avoid stigmatisation of data subjects.

The general obligations concerning the outsourcing of data processing will apply in case corporations retain a third party such as a call centre. This implies that contractually binding data processing instructions, confidentiality, and information security measures must be imposed on such third party service providers.

Also, corporations must abide by the provisions on transborder data flows set forth in the French Data Protection Act and the Directive in order to transfer alerts to non-EEA countries that are not considered to provide an adequate level of data protection. In this context, the question arises as to whether alerts concerning a violation of national law may be handled by the parent company based in a third country. This question cannot be answered in the abstract case, and the distribution of investigative powers as well as liabilities between the entities within a group of affiliated companies, will be influential here. There is little argument against using a call centre that is based in a third country, since the processing of alerts by such a call centre remains, as a data processor, subject to French data protection law (or for other Member States, to the law where the data controller is established). Of course, it will be critical that corporations impose clear data processing instructions in such an outsourcing scenario and execute adequate controller-to-processor data transfer agreements.

Condition 8

Possibility to evaluate the system.

Corporations may evaluate the use of the whistleblowing procedures based on aggregated data (for instance, for purposes of assessing a typology of alerts received, and to take corrective measures, if necessary). Such information should in no event allow the direct or indirect identification of data subjects (whistleblowers, data subjects or other parties reported). The CNIL does not impose an obligation to audit the use and working of hotlines, and only foresees a corporate ability to conduct such an assessment. To ensure smooth functioning and to eliminate malfunctions, companies should

  WDPR ISSN 1473-3579

regularly evaluate the functionality of hotlines to assess whether the hotlines are serving the intended purposes, with the principles of proportionality in mind.

Condition 9

Provide for conservation limits, and immediately delete information on allegations that have shown to be gratuitous.

According to the CNIL, alerts that prove to be gratuitous or that are unfounded should be immediately deleted in application of the proportionality principle. Furthermore, the CNIL advises that reports of complaints that require further investigation should be deleted within two months of such investigations being finalised, unless the corporation has decided to start disciplinary or court proceedings against the reported individual(s) and the information is required for conducting such proceedings. To avoid unnecessary complaints and to enhance data subjects' control over the processing of their personal data, companies should consider providing notice of the fact that their personal data has been purged in case of an unfounded complaint or upon termination of an investigation.

Condition 10

Inform data subjects from the moment that evidence has been preserved.

The orientation document states that data subjects against whom complaints have been reported should be informed from the moment that the alert or complaint is reported so that they can exercise their rights of access, objection and rectification. Strict compliance with this rule would, of course, hinder most investigations from the very beginning. The CNIL has anticipated this problem and allows that measures are taken to avoid deletion or loss of evidence. Although the CNIL does not state it explicitly, common sense does not require that individuals be informed as long as the evidence is secured. It is of course important that such measures are taken quickly and that data subjects are informed about the investigation after the information is adequately secured. Corporations have legitimate interests to collect all information required to effectively investigate a complaint and it can therefore be defended that individuals should not be informed before all required information is collected.

Condition 11

Provide for the effective implementation of the rights of access and rectification.

Data subjects have the right to access personal information reported and processed in the context of the whistleblowing procedure.[16] Pursuant to Article 39 of the French Data Protection Act, the right of access is formulated in broad terms, and is not limited to obtaining a confirmation or copy of contact information that is maintained on file. Based on the wording of the Act, data subjects could obtain a copy of the alerts and reports on file.[17] The rationale for this rule is that all information on file qualifies as "personal data", since it can be linked to an identified or identifiable natural person. However, the general right of access must be applied in a reasonable fashion. First, companies can take the position that they are not required to provide access until the investigation has been finalised. In the context of access requests to human resources evaluation reports, the CNIL has already considered that evaluation data concerning employees may not be communicated as long as these are of a preparatory nature that cannot be opposed by the employer.[18] There is little reason why the same rule should not apply here, knowing that in most cases no notice will be provided until all evidence is secured, *i.e.,* upon termination of the investigation. Second, the right of access is to be balanced with the privacy rights of other employees or third persons mentioned in the reports.[19] Pursuant to Article 13 (g) of the Directive, Member States could, at least in theory and depending on the wording of national data protection law, limit the right of access if such access would restrict their "rights and freedoms".[20] A substantial and legitimate interest of the data controller can, in some Member States, outweigh the right of access. The Implementation Study commissioned by the European Commission states the following:

> "[…] the UK law has a provision whereby access can be denied to 'confidential references' given about job applicants and to personal data used in 'management forecast' or 'planning' and negotiations with the data subject to the extent that providing access to such information would be likely to prejudice the interests of the data controller. In Ireland, the law contains particular exceptions to subject access, for instance, concerning in-house estimates of possible liability for claims made against the controller to the extent that providing access so such information would be likely to prejudice the interests of the data controller".[21]

The French Act does not provide for much flexibility, but data controllers should consider formulating a restriction to the right of access in their application for an authorisation.[22] While it may be possible to restrict access in exceptional circumstances, such restrictions will of course also need to be reconciled with general principles of due process and proportionality.

The right of rectification allows data subjects to correct inaccurate personal data. Allowing the same data subjects to amend alerts and investigative reports is nonsensical, since this would imply data subjects could amend evidence. A solution could be to provide for a procedure whereby data subjects can comment on the alerts and reports. In any event, companies will, within the parameters of national law, need to provide for procedures to balance the right of access and rectification with the personal autonomy of other named individuals and the legitimate interests of the corporation.

Procedural Aspects

A whistleblowing system, whether it complies with the abovementioned conditions set forth in the orientation document or not, remains subject to prior authorisation by the CNIL. However, the CNIL announced that it will issue a formal decision setting forth the conditions of a "single authorisation procedure". Pursuant to such a single authorisation procedure, companies will only need to formally declare compliance of the whistleblowing procedures with the specific conditions set forth in the future decision.[23] Companies will need to go through an individual authorisation procedure if they do not fulfil the

decision's requirements or do not satisfy the CNIL's interpretation thereof.

The CNIL's decision to issue a single authorisation procedure is welcomed news, as it will ease the administrative burden and bring greater legal certainty to companies that intend to implement or have already implemented whistleblowing procedures. Prior to such declaration, companies are required to carefully audit the procedures they have in place, take corrective actions, and ensure that the requirements stipulated by the future decision – and that will generally be a reflection of the orientation document's conditions – are respected. The CNIL's decision is expected to be published during December 2005.

Conclusion

The CNIL's orientation document and promised future single authorisation decision indicate that U.S. multinationals with operations in France may soon be free from the untenable legal position in which they found their SOX hotlines over the past few months. The CNIL's orientation document provides guidance and a solid preview of the authorisation decision that will ultimately be issued with respect to how companies may set up a whistleblowing procedure that complies with both the requirements of the U.S. SOX Act and French (and European) data protection law. However, companies should not expect the CNIL to bless a broad approach to whistleblower hotlines, and should expect the CNIL to be rigorous in its evaluation of declarations submitted under the future single authorisation decision; whistleblowing procedures that deviate from the conditions posed by the CNIL will not be authorised. Thus, multinational corporations that had previously embarked upon a strategy of maintaining a uniform approach to ethics hotlines will likely be sorely disappointed with the future authorisation, and will be forced to consider non-uniform approaches or a scaled-back ethics hotline program. And the CNIL's authorisation may just be the tip of the iceberg. Multinational corporations that have establishments in other EEA countries will need to comply not merely with the French data protection standard, but also with the standards imposed by national data protection law of other relevant Member States. While the standards set forth in the CNIL's orientation document are quite high and could probably be transplanted and applied within other jurisdictions, it will be necessary to verify peculiarities under national law and it may be difficult to harmonise divergent requirements. It can only be hoped that the Working Party will effectively provide for additional guidance to assist corporations to bridge variations in national law while implementing a whistleblowing procedure.

1 Documentation d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.

2 See Délibération n° 2005-110 du 26 mai 2005 relative à une demande d'orientation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle.

3 See Délibération n° 2005-111 du 26 mai 2005 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de ligne éthique.

4 Pursuant to Article 25(4) of the French Data Protection Act, companies need to obtain the CNIL's prior authorisation to implement information systems that may, by means of their nature, their extent or purposes, exclude individuals from a right, a service or a contract, in the absence of specific laws or regulations.

5 Tribunal de grande instance de Libourne Ordonnance de référé 15 septembre 2005, CE Bsn Glasspack, syndicat CGT / Bsn Glasspack, *www.legalis.net/jurisprudence-decision.php3?id_article=1497*.

6 The orientation documents states « Pour autant [la CNIL] n'a pas d'opposition de principe à de tels dispositifs dès lors que les droits des personnes mises en causes directement ou indirectement dans une alerte sont garantis au regard des règles relatives à la protection des données personnelles. »

7 Article 7-1° of the French Data Protection Act.

8 Article 7-5° of the French Data Protection Act.

9 The CNIL provides as an example of such a legal ground the French Decree on the Committee for banking and financial regulations :« Arrêté du 31 mars 2005 modifiant le règlement du Comité de la réglementation bancaire et financière n° 97-02 du 21 février 1997 ».

10 Section 301(4) of Sarbanes-Oxley requires that "each audit committee shall establish procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and the confidential anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters".

11 The CNIL refers to the requirements imposed by the OECD Convention of 17 December 1997, ratified by the French Act n° 99-424 of 27 May 1999 (Loi no. 99-424 du 27 mai 1999 autorisant la ratification de la convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationals, faite à Paris le 17 décembre 1997).

12 CNIL Orientation Document, p. 4.

13 The controller generally will be the French entity, but it is possible that the U.S. parent company will qualify as co-controller since the system is typically organised and imposed by the latter.

14 See for instance, p. 15 of the Analysis and Impact Study on the Implementation of Directive 95/46 in Member States: "The Belgian law extends the restrictions on the processing of to data on any legal disputes and to mere suspicions".

15 See in this context the Guidelines for Terminated Merchants, issued by the Article 29 Data Protection Working Party on January 11, 2005. Principle no. 8 that "the database shall only contain objective factual information related to irregularities commonly addressed by Participants as a risk factor, and shall not contain rumors and mere suspicions".

16 Articles 39 and 40 of the French Data Protection Act.

17 See Article 39-I : « Une copie des données à caractère personnel est délivrée à l'intéressée à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction ». For further information on the practicalities of the right of access under the French Act, consult the Deliberation no. 80-010 of 1 April 1980: « Délibération n° 80-010 du 1er avril 1980 portant adoption d'une recommendation relative à la mise en oeuvre du droit individual d'accès aux fichiers automatisés ».

18 Analysis and Impact Study on the Implementation of Directive 95/46 in Member States, p. 21.

19 See Article 39-II of the French Data Protection Act.

20 Article 13 states inter alia: "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard: […] (g) the protection of the data subject or of the rights and freedoms of *others*". (emphasis added). The notion "others" may also allude to the data controller.

21 Implementation Report, p. 24.

22 See Article 39-II of the French Data Protection Act.

23 See Article 25-II of the French Data Protection Act.