Commission nationale de l'informatique et des libertés

Paris, 10 November 2005

Guideline document adopted by the "Commission nationale de l'informatique et des libertés" (CNIL) on 10 November 2005 for the implementation of whistleblowing systems in compliance with the French Data Protection Act of 6 January 1978, as amended in August 2004, relating to information technology, data filing systems and liberties.

This document officially and publicly defines the position of the CNIL. It was not adopted in the form of a deliberation issuing a recommendation, so as to ensure maximum flexibility in the case by case examination of individual authorisations of whistleblowing systems. In a second stage, the CNIL will adopt a decision for a unique authorisation of such systems which comply with the orientations which it has defined in this document, so as to simplify the notification duties of companies.

The "Commission nationale de l'informatique et des libertés" (CNIL) has noted the recent development in France of procedures enabling employees to report their colleagues' allegedly law- or corporate policy-breaching behaviors in the office ("whistleblowing systems").

Such whistleblowing systems are neither allowed nor banned under the provisions of the French Labor Code. When they rely on the processing of personal data, i.e. on the collection, the registration, the storage and the disclosure of data related to an identified or identifiable person, they are subjected to the provisions of the French Data Protection Act of 6 January 1978, as amended in 2004, whether the processing is automated or paper-based. When they are carried out in an automated form, they are subject to a requirement of prior authorization by the CNIL, in application of article 25(4) of that Act, due to their qualification as processing operations that may exclude individuals from the benefit of a right or of their employment contract in the absence of any specific legal provision.

In May 2005, the CNIL refused to authorize two specific "whistleblowing systems". However, it has no objection in principle to such schemes, provided the rights of individuals directly or indirectly incriminated through them are guaranteed with regard to personal data protection rules. In fact, such individuals, in addition to the rights which they are granted under labor law if disciplinary actions are initiated against them, are entitled to specific rights under the French Data Protection Act or under Directive 95/46/EC of 24 October 1995 when data relating to them are processed: right to such data being collected fairly; right to be informed that such data is being processed; right to object to such processing for legitimate reasons, right to have any inaccurate, incomplete, ambiguous or outdated information rectified or removed.

In order to contribute to the implementation of whistleblowing systems which comply with the principles defined by the said Act and Directive, the CNIL recommends companies implement the rules below. These rules only bear on the application on these specific texts. They do not refer to matters outside the jurisdiction of the CNIL, in particular those relating to employment legislation.

1) Scope of a whistleblowing system: complementary nature, limited scope, non-mandatory use

The normal operation of an organisation implies that reports on anomalous behaviours, on whatever type of issues they are made, are sent to managers through the hierarchy, or by open reporting systems such as the intervention of personnel representatives or, in relation to account auditing, through auditors' reports. Under French law, the protection and independence of the first and the latter are specifically ensured, for that matter.

The implementation of whistleblowing systems may be justified by the assumption that these communication channels may not function in certain circumstances. Nevertheless, such systems may not be considered by companies as the normal means of reporting anomalous behaviors in the company, on an equal footing with reporting methods managed by personnel whose functions or responsibilities involve precisely the identification and handling of such anomalous behaviours. In this respect, whistleblowing systems must be designed as solely complementary to other reporting systems in companies.

Due to its inherently complementary nature, the scope of such a whistleblowing scheme should be limited. Schemes with a general and indiscriminate scope (such as those intended to ensure compliance with legal requirements, corporate policies or internal rules on business conduct, for instance) raise an automatic difficulty with regard to the French Data Protection Act due to the risk of abusive or disproportionate incrimination of the professional, or even personal integrity of the employees concerned.

In this respect, one may derive from article 7 of the French Data Protection Act of 6 January 1978, as amended, that a whistleblowing system may only be considered as legitimate if it is necessary to comply with a legal obligation (statutory or regulatory) imposing the setting up of said systems (article 7(1)), or if it is necessary for the purposes of realizing the legitimate interest pursued by the data controller responsible for the processing, when this legitimate interest is qualified and its realization does not imply to "override the interests or the fundamental rights and freedoms of the data subjects" (article 7(5)).

This requirement of legitimacy is qualified under Article 7(1) of the French Data Protection Act of 6 January 1978 when a whistleblowing system has the sole purpose of meeting a statutory or regulatory obligation under French law aiming at the establishment of internal control procedures in precisely defined areas. Such an obligation clearly results, for example, of provisions relating to the internal control of credit and investment establishments (Regulation of 31 March 2005 amending Regulation by the Banking and Financial Regulatory Committee, "Comité de réglementation bancaire et financière", Nr. 97-02 of 2 February 1997).

On the other hand, it does not seem possible to consider that the existence of a foreign legal provision in application of which a whistleblowing scheme is to be set up may be considered as a factor making the processing operations legitimate by virtue of Article 7(1). This applies namely to the provisions of section 301(4) of the Sarbanes-Oxley Act, which state that a company's employees must have the possibility to directly inform the audit committee of this company of their concerns relating to questionable accounting or auditing matters, while being assured that they may report such allegedly anomalous behaviours while benefiting of conditions of confidentiality and anonymity.

In this last case, however, and by reference to article 7(5) of the French Data Protection Act, it is impossible to ignore the legitimate interest held by French companies listed in the United States, or French subsidiaries of companies listed in the United States, which must certify their accounts with the US stock market authorities, in setting up whistleblowing procedures in relation to alleged anomalous behaviours in accounting and auditing matters. Obviously, ensuring that reports on suspected account rigging which may have an impact on the financial statements of the company properly reach the Board of directors is a critical concern for any public issuer.

Far from being limited to the United States, initiatives were also taken in Europe (see in particular the recent recommendation of the European Commission of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board), which are aimed at achieving the same objective as the Sarbanes-Oxley Act, i.e. reinforcing the security of financial markets.

These different texts clearly qualify, pursuant to article 7(5) of the Data Protection Act of 6 January 1978, the legitimate interest held by companies in setting up whistleblowing systems in the areas which they cover and, in this context, such systems must be considered as accepted.

For the same reasons, whistleblowing systems whose purpose is to combat bribery, for instance bribery of foreign public officials in international business transactions (OECD convention dated December 17, 1997, ratified by Act Nr.99-424 dated May 27, 1999) may be considered as legitimate.

Whistleblowing systems limited to the above-defined scope will benefit from a single authorisation from the CNIL, subject to compliance with the other rules which it further recommends below. On the other hand, for systems not based on statutory or regulatory obligations of internal control in the financial, accounting, banking and anti bribery areas, the CNIL will carry out a case by case assessment, of the legitimacy of the purposes and the proportionality of the whistleblowing system envisaged, in the context of its authorisation powers.

So as to avoid improper use of whistleblowing systems to report facts unrelated to such pre-determined areas, data controllers must clearly indicate that these systems are strictly reserved for such areas, and must refrain from investigating reports related to other areas, unless the vital interest of the company or the physical or moral integrity of its employees are at take.

More generally, the use by personnel of a legitimately set up whistleblowing system must not be compulsory. In this respect, the French Minister for Labor and Social Affairs underlined, in a letter sent to the CNIL, that *"the use of whistleblowing systems must not be compulsory, but be merely encouraged. (...) Making reporting mandatory would result in passing on to employees the employers' duties to ensure compliance with the company's internal rules of procedure. It can be argued also that a compulsory reporting requirement would breach article L120-2 of the Labor Code as a requirement out of proportion with its objective ».*

2) Definition of the categories of persons affected by the whistleblowing system

In accordance with the principle of proportionality, the categories of personnel who may be incriminated through a whistleblowing system must be precisely defined in reference to the reasons supporting the setting up of this system.

This definition is left to the responsibility of the company management, who must set the limits to the procedure, in compliance with the procedural requirements provided for in employment law.

3) Restrictive handling of anonymous reports

The possibility to file anonymous reports can only increase the risk of slanderous reports. Conversely, requesting an individual's identification prior to letting him/her make a report can only help increase the responsibility of the users of the process and thus reduce such a risk. In practice, identified reports offer several advantages, as they make possible :

- To avoid or at least limit false and/or slanderous accusations;
- To organise the protection of the whistleblower against retaliation ;
- To ensure a better handling of the report, with the option of requesting additional details on the alleged facts from the author of the report.

Protecting the whistleblower is a requirement inherent to whistleblowing systems. It does not belong to the CNIL to determine how such protection may be appropriately ensured, except for one area that results clearly from the Data Protection Act. The whistleblower's identity must be processed under conditions of confidentiality so that this individual does not suffer any detriment due to his actions. In particular, this identity may not be disclosed to the incriminated individual while exercising his/her right of access pursuant to Article 39 of this Act.

However, the existence of anonymous reports, even and especially in the absence of organised confidential whistleblowing systems, is a reality. It is difficult for company management to ignore this type of report, even when not in favour of them on principle.

The handling of such anonymous reports involves that specific precautions are taken, in particular a preliminary examination by their first recipient of the opportunity of communicating them through the system.

In any event, the organisation must not encourage the persons who are to use the system to do so anonymously, and the publicity which is made on the existence of such a system must be designed by taking this requirement into account. On the contrary, the procedure must be designed in such a way that the employees using the system are requested to identify themselves each time they make an alert and report information relating to facts rather than to individuals.

4) Communication of clear and extensive information on the whistleblowing system

Clear and complete information on the system must be given to potential users by any appropriate means.

Beyond the collective and individual information to be provided pursuant to the French Labor Code, and in application of article 32 of the Data Protection Act of 6 January 1978, as amended, this information must in particular identify the entity responsible for the system, the objectives sought and the domains covered by the alerts, the optional nature of the system, the absence of consequences for employees for not using the system, the recipients of the alerts as well as the existence of a right of access and rectification for persons identified in the context of this system.

Lastly, it should be clearly stated that any abuse of the system may result in disciplinary action and judicial proceedings being filed against the author of the abuse, while on the other hand, use in good faith of the system, even if the facts are subsequently not borne out, may not make the whistleblower liable to sanctions.

5) Collecting reports through dedicated means

The reports may be collected by any data processing means, whether electronic or not.

Such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for added data confidentiality.

6) Only relevant, adequate and non excessive data in reports

The medium on which data collected through a whistleblowing system is recorded should only mention data that is formulated in an objective manner, that is directly related to the scope of the scheme and is strictly required for verifying the alleged facts.

The wording used to describe the nature of the reported facts should express that the facts are alleged.

7) Internal management of reports limited to specialists, in a confidential framework

The collection and the handling of reports must be entrusted to a specific organisation set up within the company to specifically deal with these matters. A limited number of persons must be responsible for dealing with these reports. They must be specially trained and bound by a contractually defined obligation of confidentiality.

The confidentiality of personal data must be guaranteed when it is collected, disclosed or stored.

The data received through the whistleblowing system may be communicated within the group if such communication appears necessary to the requirements of the investigation and results of the organisation of the group. Such communication will be considered as necessary to the requirements of the investigation for example if the report incriminates a partner of another legal entity within the group, a high level member or management official of the company concerned. In this case, data must only be communicated in confidential and secure conditions to the competent organisation of the recipient legal entity which provides equivalent guarantees as to the management of whistleblowing reports.

If such communication appears necessary and the recipient of the data belongs to a legal entity established in a country outside the European Union which does not provide adequate protection, the specific provisions of the EC Directive 95/46/EC of 24 October 1995 and of the French Data Protection Act of 6 January 1978, as amended, relating to international data transfers apply (i.e. specific legal framework and information of the persons concerned that data will be transferred to said country).

Finally, in the event that the management of the whistleblowing system is entrusted to an external service provider, this provider must contractually agree to ensure confidentiality and comply with the time limits set by the data controller for the storage of the data. As a data controller, the company will in any event remain liable for the data processing carried out by the processor on its behalf.

8) The possibility of system assessment reports

For the purpose of evaluation of the whistleblowing system, the responsible company may send to the different organisations dedicated to this task within the group all statistical information useful to their task (such as data relating to the type of reports received and the corrective measures taken).

This information must in no case enable the direct or indirect identification of persons involved in alerts.

9) Limited data storage periods

Data relating to a report found to be unsubstantiated by the entity in charge of processing such reports must be deleted immediately.

Data relating to alerts giving rise to an investigation must not be stored beyond two months from the close of verification operations, unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report or the author of an abusive alert.

10) Accurate notification of the incriminated person

Pursuant to Articles 6 and 32 of the French Data Protection Act of 6 January 1978, as amended, notification to the person identified in an alert must in principle be carried out by the person responsible for the system, no later than at the time when the relevant data is recorded, whether in a digital form or not, so as to enable him or her to exercise his statutory right to object promptly to his or her data being processed, for a legitimate reason.

At any rate, the reported individual should not be informed before indispensable protective measures have been taken, in particular to avoid the destruction of evidence necessary to the handling of the report.

The information is given in a way which ensures that the reported person is properly notified.

In particular, the reported employee must be informed of the entity responsible for the system, the facts he is accused of, any departments which might receive the report as well as how to exercise his/her rights of access and correction.

11) Complying with rights of access and rectification

Pursuant to articles 39 and 40 of the French Data Protection Act of 6 January 1978, as amended, any person identified through the whistleblowing system may access data concerning him/her and request, as applicable, its correction or removal.

They may in no case gain access, on the basis of their right of access, to information relating to third parties, such as the identity of the whistleblower.