

**RECOMMENDATION NO. 1/2006 OF NOVEMBER 29, 2006**

*Our ref.: SA2/SE/2006/059*

**Re: Recommendation related to the compatibility of the whistleblowing systems with the law of December 8, 1992, concerning protection of privacy with regard to personal data processing operations**

---

The Privacy Commission:

Having regard to the Act of December 8, 1992, related to the privacy protection of personal data processing operations (hereafter LVP) in particular its Article 30;

Having regard to the increasing number of issues forwarded to the Commission aimed at determining under what conditions a whistleblowing regulation is compatible with the LVP;

Having regard to the report of Ms. N. Lepoivre and Mr. F. Robben;

Issued the following recommendation on November 29, 2006:

## Definition

Whistleblowing systems are mechanisms that enable individuals to report conduct of a member of their organization, which in their opinion is contrary to a law or a regulation or to the basic rules established by their organization.

## Context

By issuing this recommendation, the Commission has considered it necessary to enunciate its position on whistleblowing systems in general, considering that these systems are increasingly common in all countries of the European Union, including Belgium<sup>1</sup>. Various issues and an official complaint have also been filed with the Commission with regard to the legitimacy of such systems in light of the LVP.

Moreover, attorneys, whose clients want to honor their obligations under the US Sarbanes Oxley Act (hereafter called "SOX") on one hand, which specifically involves foreign companies listed on the New York stock exchange and for foreign affiliates of US companies, and which also want to comply with the recommendations concerning data protection contained in Directive 95/46/EC of the European Parliament and the Council of October 24, 1995, related to the protection of persons with regard to the processing of personal data and the free circulation of these data and in the LVP, have also interrogated the Commission.

The fundamental principles chosen by the Commission to determine whether such whistleblowing systems comply with the LVP can therefore be used as a guideline for organizations planning to implement these whistleblowing systems or else to adapt those already in existence.

## Exercise of equilibrium

The implementation of a whistleblowing system implies a delicate balance in which the legitimate interests of all those involved (the organization, its staff, the whistleblower, the person incriminated and any third parties) must be reconciled.

Indeed, a whistleblowing system pursues several purposes, for the organization and for the staff.

The interest of the organization is evidenced by its need to have its internal rules and regulations respected and by its concern to safeguard its image by means of an effective internal control.

For the personnel, it is important to prevent the environment within the organization from deteriorating, to avoid tensions that could result from a "whistleblowing culture" and the proper treatment of the whistleblower and the person incriminated can significantly contribute to this.

---

<sup>1</sup> Also apparently in the public sector. See for example Article 12bis of the "mediation" decree of July 7, 1998, amended by Decree of May 7, 2004: *"Any member of the staff assigned to an administrative authority as indicated by Article 3, can report wrongdoings, abuse or crimes as covered under Article 3, § 2 and conditions described therein in writing or verbally to the Flemish mediation department."*

An adequate mentoring program is therefore necessary to prevent unjustified charges and also to process justified reports.

In order to be thorough, the Commission has indicated that on February 1, 2006, the independent European consulting body on the protection of data and privacy (hereafter called Group 29) issued an opinion related to the application of EU data protection rules to internal mechanisms for reporting wrongdoing in the fields of accounting, internal accounting controls, auditing, the fight against corruption and bank- and finance-related crimes.

### **Applicability of the LVP**

The establishment of a whistleblowing system brings about a situation in which the LVP can be applied if personal data are automatically processed or even if they are contained or may be included in a file (Article 3 of the LVP). The Commission therefore believes that in almost all of these cases, the use of a whistleblowing system will automatically imply a processing of personal data under the LVP. The processing of personal data within the framework of such a whistleblowing system must accordingly comply with the recommendations of the LVP.

### **Applicable provisions of the LVP**

The Commission believes that personal data must be processed in accordance with the following provisions of the LVP:

- admissibility, fair play, legality and purpose (Articles 4 and 5 of the LVP);
- proportionality (Article 4 § 1, section 3 of the LVP);
- accuracy and precision (Article 4, § 1, section 4 of the LVP);
- transparency (Article 9 of the LVP);
- security (Article 16 of the LVP);
- for all persons whose personal data are kept within the framework of the whistleblowing system (particularly the whistleblower and the incriminated person): rights of access, rectification and erasure of personal data concerning them (Articles 10 and 12 of the LVP);
- obligation of declaration (Articles 17 and 19 of the LVP).

### **Admissibility, fair play, legality and purpose**

#### Admissibility

With regard to admissibility, the Commission has found two possible legal bases in Article 5 of the LVP enabling an organization to justify its whistleblowing system, to wit:

1. The existence of a legal or regulatory obligation requiring it to process personal data via by means of a whistleblowing system (Article 5, c) of the LVP);
2. In the absence of such a legal obligation, a legitimate interest therein provided the fundamental freedoms and rights of the incriminated person are not taken advantage of (Article 5, f) of the LVP.

Insofar that the data supplied and processed are personal data pursuant to Article 8 of the LVP, in this case the personal data concerning suspicions related to violations, Article 5 of the LVP does not suffice to enable the organization to process the data in question. In principle, there is even a prohibition of processing (Article 8, § 1 of the LVP) which however can be lifted, if the organization can invoke a legal or regulatory basis for the exceptional processing of these data as specified

in Article 8, § 2 of the LVP. This will be the case if the processing is necessary for the achievement of the purposes established by or under a law, decree or order (Article 8, § 2, b) of the LVP) or if the processing operation is necessary for the management of the organization's own disputes (Article 8, § 2, c) of the LVP) and by meeting additional conditions as provided in Article 25 of the Royal Order of February 13, 2001, *involving enforcement of the LVP*<sup>2</sup>.

If there is to be a legal obligation in accordance with Article 5, c) of the LVP, whereby an organization is responsible for processing personal data via a whistleblowing system, a legal provision of Belgian law must be involved. A foreign legal provision obligation cannot be taken into account in this case. In this regard, the Commission shares the standpoint of Group 29<sup>3</sup> and French<sup>4</sup> and Dutch<sup>5</sup> Privacy Commissions.

As an example, section 301 (4) of the SOX - that states that co-workers of a company must be able to express their concern to an auditing committee concerning accounting or audit-related problems all while being guaranteed confidentiality and anonymity - indeed constitutes a foreign legal obligation.

To appreciate the legitimate interest of the organization pursuant to Article 4, f) of the LVP, it is appropriate to take into consideration the seriousness of the facts charged and the aspects of proportionality and subsidiarity.

In the case of an obligation imposed by a foreign law, this law may not constitute an interest for an organization only to the extent the whistleblowing system is created to ensure compliance of mandatory provisions of these regulations. For example, the SOX only requires, it appears, notices alerts in the fields of accounting or auditing.

Without getting involved in the controversy that exists concerning the extraterritorial applicability of the aforementioned US laws, the Commission understands that for Belgian companies listed on the New York stock exchange, the obligations imposed by the SOX Act must be respected in order to avoid various problems and sanctions.

---

<sup>2</sup> - *categories of persons, with access to personal data, must be designated by the person in charge of the processing or, if applicable, by the subcontractor, with a precise description of their position with respect to the processing of the data in question;*

- *The list of categories of people thus designated must be kept at the disposal of the Commission by the person in charge of the processing, or if applicable by the subcontractor;*
- *He must ensure that the persons designated are bound - by a legal or statutory obligation, or by an equivalent contract provision - to the respect of the confidential nature of the data in question;*
- *When the information - pursuant to Article 9 of LVP - is forwarded to the person in question or when the statement indicated in Article 17, § 1, of the LVP is made, the person in charge of the processing must disclose the legal or regulatory basis authorizing the processing of personal data indicated in Articles 6 8 of the LVP.*

<sup>3</sup> Group 29 has declared in this regard that: *"An obligation imposed by a foreign law or regulation requiring the establishment of whistleblowing systems cannot be qualified as a legal obligation legitimizing the processing of data in the EU. Any other interpretation would allow foreign laws to bypass the rules set by the EU with directive 95/46/EC".*

<sup>4</sup> Orientation document adopted by the French National Commission for Information Technology and Civil Liberties (CNIL) on November 10, 2005 for the implementation of whistleblowing devices in accordance with the law of January 6, 1978, amended in August 2004, related to information technology, files and liberties.

<sup>5</sup> Opinion of January 16, 2006, related to the request for authorization pursuant to Article 77, paragraph 2 of the Dutch law WBP of the College Bescherming Persoonsgegevens.

The consequences for an organization that does not meet this foreign legal obligation must also be considered to determine any possible application of Article 5, f) of the LVP.

#### Fair play, legality and purpose

The scope and purpose of the whistleblowing system, therefore the type of reports that can be made by the whistleblower via the internal whistleblowing system and the scope of this system must be described with precision.

The organization must also take care to precisely describe the procedure for filing and processing reports (who, what, where, when, how, etc.).

The system must clearly describe the consequences of justified and unjustified alerts.

The person in charge of the processing, with whom the rights of access, rectification and erasure of the personal data can be exercised by the whistleblower and by the incriminated person, must be explicitly designated.

The whistleblowing system cannot impose reporting obligations on members of the staff. The use of the whistleblowing system must therefore be optional by nature.

The whistleblower must have reasonable grounds to have suspected the problematic situation he is reporting. Accordingly, mere rumors are not considered as sufficient grounds for filing a report.

The information provided must be sufficiently precise. Accepting overly vague reports could lead to a "whistleblowing culture", which naturally must be avoided.

In light of the foregoing, the Commission favors a general prohibition of anonymous reporting. The question of anonymous or open reporting (i.e., whether "complaint manager" knows the identity of the whistleblower), within the framework of whistleblowing system regulations, has been carefully examined by Group 29. The Commission has subscribed to the argument developed by Group 29 that authorizes the processing of anonymous reports on a very restricted basis if they meet certain conditions. On the contrary, the Commission promotes reports in which the whistleblower is identified.

When processing the report, the whistleblowing system must make it impossible to identify the whistleblower or include any information that could lead to his identification without his consent.

Only after the accusations have been processed and the charges are found well-grounded or clearly baseless can the result be communicated to the organization.

The report must be collected and processed by a person in the organization specifically appointed to hear complaints. This person (called "the complaint manager" in this recommendation) is bound to professional confidentiality when processing the report, even with regard to executives (unless immediate precautionary measures are required), other members of the staff, labor union organizations and third parties.

The complaint manager must be able to work with sufficient autonomy with respect to the organization. The whistleblowing system must guarantee that this autonomy cannot be compromised. The complaint manager must act by having a precise responsibility and accordingly may be questioned, for example, in case of a breach in his obligation of confidentiality with regard to the whistleblower, the incriminated person, or third parties during the processing of the report.

The complaint manager must be protected from any pressure exerted by executive management or labor unions, particularly if the person incriminated is an executive or officer with a labor union.

The complaint manager must process the report with the utmost discretion.

The complaint manager shall cease processing the report within the whistleblowing procedure in the event of intentional violation of confidentiality by the whistleblower himself.

## **Proportionality**

### A limitation in the scope of application

In principle, normal control procedures with regard to executive officers, accounting, etc., conducted by persons who represent the management of the organization - whose task is precisely that of detecting and processing wrongdoing in the company – should suffice to dissipate concerns related to conduct that violates the company's standard by the personnel.

The internal whistleblowing system can only be used as a specific and subsidiary channel whereby all or certain members of the staff designated in the whistleblowing system can report serious irregularities within the company.

The Commission has stressed the strictly supplemental nature of the whistleblowing system. It can only involve reports concerning problems that clearly would not be processed by the normal line of command and for which there is no specific procedure or body legally regulated (for this latter aspect, think about the problem of workplace harassment or sexual harassment).

A whistleblowing system can only involve reports pertaining to serious acts (violation of regulations applicable to the organization in question or internal written company rules (particularly in the departments of finance and accounting) or if a crime is involved. It therefore must involve serious wrongdoing – (without necessarily being violations) – but nevertheless sufficiently serious facts or situations that must be reported in the general interest of the company or for the proper governance of the organization and for which the whistleblower considers it not or no longer possible through normal channels (e.g., when the previous report was not processed properly by the management, or when those channels are involved in the problem reported by the whistleblower, etc.).

Only those people who are part of the organization can report or be the focus of reports in fields where the whistleblowing system applies.

## **The complaint manager**

The complaint manager must ensure that personal data:

- are adequate, pertinent and not excessive for the processing of the report alert;
- remain limited to the designation of the facts and do not contain judgments of worth. Subjective evaluations must therefore generally be rejected;
- are explicitly disclosed as such if they concern unproven facts;
- are kept for a period of time that does not exceed what is necessary for processing the report, including any legal or disciplinary procedures with regard to

the person incriminated (in case of a justified report) or with regard to the whistleblower in case of unjustified reports or libelous accusations.

### **Precision and accuracy**

The complaint manager is responsible for monitoring – if applicable with the help of a sufficiently independent internal or external examining board (in order to proceed with certain verifications) that the personal data intended for processing reports are accurate and precise.

### **Transparency**

#### Collective level

The organization that wishes to set up a whistleblowing system must notify its staff thereof by respecting the laws on the collective labor rights (by notifying, if appropriate, the company council, the committee for the protection and prevention of work [sic], the labor union delegation or the negotiation or bargaining committees).

#### Individual level

All co-workers of the organization who are conceivably involved in the whistleblowing system must be notified:

- of the scope and the purposes of the whistleblowing system;
- of the procedure for filing and processing reports;
- of the consequences of justified and unjustified reports;
- of the way in which the rights for accessing, correcting and erasing information can be exercised and the procedure through which these rights can be exercised;
- of third parties to which personal data concerning the whistleblower and the incriminated person may be transmitted within the framework of the processing of the report, e.g., the internal auditing department if the complaint manager must check certain things.

It is important for the whistleblower to be notified of the obligation of confidentiality when filing the report and during the processing thereof.

The incriminated person must be informed as quickly as possible by the complaint manager of the existence of a report and the facts he is charged with in order to enable him to exercise his rights provided under chapter III of the LVP.

The information of the incriminated person can be reported in exceptional circumstances (e.g., if there is the possibility of evidence being destroyed).

### **Security**

The whistleblowing system must provide guarantees so that personal data processed within the reporting procedure are not processed for other purposes. It must therefore involve an operation that is differentiated from other processing operations.

It must provide guarantees of integrity, authenticity, availability and confidentiality of the personal data.

It must ensure that personal data cannot be illegally destroyed during the processing of the report.

It must make it possible to conduct the audit so that the way in which the personal data are processed can be easily tracked (control aimed at determining who did what, with what personal data and at what time).

The guarantee of anonymity of the whistleblower and any parties involved is also important at the security level.

Personal data cannot be exported to countries outside the European Union except under the provisions of the LVP concerning data transfers (Article 21-22 of the LVP).

Data transfers to a parent company in a country outside the European Union can only be justified if it involves particularly serious issues for which it has become obvious that the processing of the report cannot or can no longer be properly done exclusively at the European organization level or that the processing may have repercussions beyond the company located in Belgium or in the European Union.

### **Rights of the incriminated person, the whistleblower, third parties**

All those involved in the whistleblowing system have rights under chapter III of the LVP regarding their personal data.

They are therefore entitled to correct any of their personal data that may be incorrect and the right to erase a) data that might be incomplete or not pertinent; b) data the processing of which is prohibited or d) data that are kept after the report has been processed.

They are not entitled to access personal data of others unless consent has been explicitly provided.

The incriminated person can therefore not access the identity of the whistleblower or that of third parties (or information that could lead to their identification) unless consent of the party in question has been provided or in the case of an unjustified report or libelous accusation of the whistleblower or false testimony from a third party.

The whistleblower is also therefore not entitled to access the personal data of the incriminated person or third parties. This access prohibition can however be lifted if after an inquiry, it appears that the incriminated person mistakenly suspected the whistleblower (by affirming for example that the whistleblower was himself implied in the wrongdoing that he reported) or if third parties acted in bad faith) e.g., interrogated persons making false testimony) .

The whistleblower is entitled to know the result from his report and any follow-ups.

### **Statement**

Prior to implementation, a statement of a whistleblowing system that provides for the automatic pre-processing of personal data is mandatory according to the Commission (application of Article 17 of the LVP).

If within the framework of the whistleblowing system, personal data are used again in a manual file or are intended to be used therein, no statement is generally required, unless the Commission requires it (Article 19 of the LVP. In this case, this requirement seems to be met, considering the special nature of the personal data (data included under Article 8 of the LVP, data related to alleged violations, etc.) that will be processed.

This is also true if it involves gathering personal data aimed at determining a judgment regarding the persons in question.

### **Evaluation reports of the whistleblowing system**

The Commission does not object to evaluation reports of the whistleblowing system being prepared. These reports cannot however be forwarded in such a way that provides identification of the persons involved.

The Commission would like to point out in this regard that the erasure of identification data with regard to the persons concerned cannot however prevent them from being identified, if necessary. In other words, the risk cannot be avoided that their identity may be revealed indirectly. As the nature of the complaint, the organizational and/or structural problems observed and the recommendations made are described in detail in the report, there is an increased risk of violating the requisite anonymity, which must be prevented.

### **BASED ON THESE GROUNDS,**

The Commission considers that the whistleblowing systems are only compatible with the LVP if they minimally respect the fundamental principles disclosed above. These principles can therefore be used as a guideline for organizations planning to implement such systems or if necessary to adapt such systems already in existence.

The administrator

The vice president

Jo Baret

Willem Debeuckelaere

