



**International Chamber of Commerce**

*The world business organization*

**Department of Policy and Business Practices**

**Commission on E-Business, IT and Telecoms**

---

**Task Force on Privacy and the Protection of  
Personal Data**

**Informal input to the CNIL on anonymous hotlines**

**Introduction**

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. ICC promotes an open international trade and investment system and the market economy. Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment, e-business, IT and telecoms policy, as well as on vital technical and sectoral subjects.

Within ICC, the Task Force on Privacy and Protection of Personal Data analyzes the impact of regulatory frameworks in the area of privacy and data protection and formulates business positions on these issues.

ICC appreciates the opportunity to respond to the 'Commission Nationale de l'Informatique et des Libertés' (CNIL) draft guidelines for the implementation of whistleblowing schemes under the French Data Protection Act of January 6th, 1978, as amended on August 6th, 2004.

However, due to the short deadline in providing the CNIL with ICC feedback, this informal contribution will be finalized later with an official position on anonymous hotlines through consultation with all ICC members.

---

**International Chamber of Commerce**

38, Cours Albert 1er, 75008 – Paris, France  
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59  
Web site [www.iccwbo.org](http://www.iccwbo.org) E-mail [icc@iccwbo.org](mailto:icc@iccwbo.org)

28 October 2005 MvdL/dfc



As a general comment, it would be helpful if the jurisdictional scope of the guidelines are clarified. This is especially important in order to avoid conflicts between various national approaches to this issue.

## **1. Scope of the alert device**

The first and second paragraphs seem to imply that an employee may use the alert system only as a secondary option, possibly after having exhausted all other available mechanisms (such as reporting to their hierarchy). Companies believe that various reporting routes should be made available to employees at the same level, so that they can choose the option with which they are more comfortable with depending on the circumstances. Indeed, employees may be afraid of retaliation by contacting their hierarchy. Even when retaliation is not an issue, the direct line managers may not be the most available people to assist the employee with his/her concern, nor the most suited, as they may not have the full knowledge of the legal issues at stake and may not handle these issues with the appropriate care (risk of inappropriate disclosures). The people in charge of running alert systems are more limited in numbers than the managers and can be required to follow processes to ensure appropriate handling of the issue. So, we believe that there are important benefits to have all reporting mechanisms made available to employees in parallel without privileging one or the other.

The scope of the Guidelines (re: alert systems) should be clarified. It would be useful for companies to understand whether the conditions they impose apply only to alert systems using dedicated phone/fax lines or email addresses or whether they apply (in full or in part) to usual compliance mechanisms set up by large companies where employees are given the possibility to report non compliances (or may be required to do so), to other organizations in the group than their reporting line managers (e.g. compliance managers, legal departments, ombudspeople, human resources ...). Companies would like to understand whether the guidelines restrict them in any way to set up their own “natural chains of command”.

Businesses don't understand why the scope of alert systems should be restricted to mere financial and accounting issues. Indeed, companies need to have compliance mechanisms to ensure that rules are complied with, whether they relate to financial laws or other laws such as environmental laws, child labour, harassment related rules, data protection laws, health and safety regulations, export controls, etc. Employees work in a complex legal environment. For this reason, companies strive to make this environment accessible to employees by synthesizing it into company internal rules (ethics codes). They therefore need to implement alert systems which encompass violations to internal rules which are in compliance with the applicable legal environment in which employees work.

With all due respect, it is a contradiction to state that Sarbanes Oxley cannot in itself justify an alert system (Section 1, 4<sup>th</sup> par.) while at the same time allowing such types of system for issues which fall within the scope of SOX. In addition, it is important to stress



that SOX goes beyond financial and accounting issues and requires companies to address any type of risk which can have a financial impact (Section 806).

We believe that the data protection principles are the same whatever the topic of the alert issue, and that therefore alert system should be authorized for a broader scope provided that they comply with data protection principles. Moreover, it would be difficult to limit alert systems to financial and accounting violations, as these notions are broad and can encompass all sorts of situations, including not only falsification of accounts but also bribery, fraud on travel and living expenses etc.

Besides, the prior to last paragraph indicates that companies should refrain from pursuing alerts reported through the alert system which are outside of the scope of the alert device. This would put companies at risk, since they could be blamed later on for that, for instance for not having assisted an employee in a difficult situation. Also, it would not be reasonable to require from companies not to pursue on a claim which is unrelated to financial and accounting issues but which could cause serious harm to the company, to an employee or a third party (e.g. a security problem).

ICC wants to stress that in a company it is every employees' responsibility, at their level, to ensure proper compliance with laws, provided they have been clearly explained by the employer. Companies are nowadays under important risks (bankruptcy, reputation risk etc.) due to misbehaviours of some employees, and the consequences may affect not only the company itself but also its suppliers and the whole society. Such risks cannot always be avoided by mere punctual audits and controls. It therefore seems more proportionate to involve employees in the every day compliance of the company (provided this is done in a reasonable and proportionate way) than to create more burdensome controls on their daily activities.

## **2. Limited categories of individuals to be involved in a whistle blowing scheme**

It does not seem appropriate to create such limitations. Employees who have no direct responsibility in accounting and financing may indeed be involved in financial and accounting non compliances. For instance, a fraud made on payslips by an employee who accesses the payroll system and falsifies the information may be committed by employees who do not belong to the Finance and Accounting departments of the company.

Also, any type of employee may be in a situation where he could need to use the alert system. For example a factory worker who witnesses that his boss or colleague diverts on a regular basis some of the equipment manufactured by the company to sell it on the black market should be given a chance to report this situation.

In addition, employees, without distinction, may witness other types of non compliances than financial and accounting ones (health and safety, child labour, harassment ...) and should be provided means to report their concerns.



### **3. Restrictive processing of anonymous reports**

We understand this paragraph as not prohibiting companies to follow up on anonymous denunciations provided that they do not encourage such type of denunciations. We think that the last sentence should be clarified though: “Cela implique de ne pas faciliter la dénonciation anonyme, et notamment de ne pas ouvrir une ligne téléphonique qui ne prévoirait pas l’identification de l’émetteur de l’alerte au début de l’entretien ». We understand that if someone brings up an alert by phone, his/her name should be asked but that if he/she refuses to provide it, the person answering the phone can continue the interview if it thinks it is appropriate. If our understanding is correct, the sentence could be reworded as follows : “Cela implique de ne pas faciliter la dénonciation anonyme, et notamment de demander l’identification de l’émetteur de l’alerte au début de l’entretien. Toutefois, si celui-ci refuse de s’identifier, l’entreprise peut décider de poursuivre l’entretien ».

### **4. Communication of clear and extensive information on the whistleblowing scheme**

The last sentence requires companies to clearly state that any abuse of the systems will result in disciplinary action and criminal proceedings being filed against the author of the abuse.

This position seems severe towards employees, especially because ultimately it is the responsibility of the company to judge on the merits of a report and to decide whether to follow up on it. Besides, the notion of “abuse” is difficult to define and companies, to take disciplinary sanctions would have to provide such a definition in their “règlement intérieur”. Nevertheless, as the French criminal code sanctions malicious reporting, companies could warn employees that malicious reporting may expose them to criminal proceedings. This would act as a deterrent to people who abuse the system.

### **5. Relevant, adequate and non excessive data in reports**

The word “objective” should be deleted. Indeed, there will necessarily be some personal judgement made in a report. In some cases, reports are indeed not edited. They are kept as they come in. However the comments made by the organization in charge of handling the alert could be drafted in such a way to show that the report is an allegation under verification, as suggested by the second sentence of section 6.

### **6. Processing of internal reports reserved for specialists in a confidential framework**

The requirement to have the reports handled by a specific organization doesn’t raise an issue. We just would prefer the use of the term “organisation” as opposed to the term “entité”, and of the word “spécifique” as opposed to “dédiée” which could be interpreted as referring to a legal entity or to a single department within a single legal entity. Indeed,



in some companies there may be dedicated functions in charge of processing only alerts but in other companies alerts may be processed by a specific group of individuals (General Counsels, Compliance managers etc.) who belong to different internal departments and whose functions are not dedicated to handling alerts exclusively.

The second paragraph requires confidentiality, which is of course an essential protection. However, this should be a “limited confidentiality” which should not prevent companies from informing upper management of the company or police/judicial authorities in due time.

We understand and agree that data sharing should be strictly limited to what is necessary for businesses to handle the report. We are worried however that the second and third paragraphs could be interpreted in a way contrary to normal ways of operation of large groups by limiting data sharing among legal entities of the group to limitative exceptional cases (suspicion upon upper management). In some multinational groups, the organizations in charge of processing alerts may not be made of individuals who work only for the French legal entity. It is for instance not unusual for companies who have European headquarters outside of France to have their compliance organization located in this other European country. Also, some companies create networks of people in charge of receiving questions or reports in various countries and it would not be in an employee’s interest to impose on them to contact only the French representative of this network. They should be able to contact anyone in the restricted network (for language reasons, or because they want their issue to be handled by people who do not have potentially personal relationship with the suspected person). So in these contexts, there may be data sharing between members of the specific organization who are employed by different legal entities of the group. However, since they will belong to the specific organization, adequate safeguards will be ensured.

Also, for example, under SOX reports should be centralized within an organization of the company which is listed at a US stock exchange. This company may be the parent company of a French subsidiary. Therefore, in this framework, data sharing with the parent company is necessary.

Regarding the last paragraph which relates to the use of a third party supplier, we understand that the supplier must comply with data protection requirements and be required to do so by contract. However, regarding the requirement “to inform the individuals identified by the whistleblowing system”, we think that it should be added “unless the company has elected to comply with this obligation itself”. Indeed, in some instances it may be more appropriate that the information to the suspected employees be conveyed by his employer or his group rather than a supplier.

## **7. Circulating anonymous business reports**

Since the statistics will be anonymous, we do not understand why their distribution should be restricted to organizations in charge of alerts. Indeed if people cannot be identified, there is no risk of harm to them and there could be interest for the company



to communicate to its employees about compliance statistics. Anonymous examples could be used to show employees examples of inappropriate behaviours and would be important to avoid new occurrences. Data which does not relate to personally identifiable individuals falls outside of the scope of data protection.

**8. Limited Data retention periods**

The data retention periods specified in this section are not sufficiently flexible and can put companies in violation of data retention requirements. The Guidelines should recognize that compliance with mandatory legal requirements is a legitimate reason for keeping reports longer.

In addition, it is important for a company, even in case of ungrounded claims, to keep information in order to be able to evidence later on which steps have been taken to handle the matter and to close the matter. Indeed, the suspected employee or the whistleblower may for instance decide to bring a lawsuit against the company. The company should be able to show which steps have been taken. Of course this data should not be available in “live” systems but should be archived securely and its retrieval should be made possible only by specifically identified people under very limited grounds. Besides, companies should be able to keep anonymous data.

**9. Accurate information provided to incriminated persons**

It should be made clear that companies could in exceptional circumstances, for investigation purposes, delay the information due to the incriminated person provided that they have an overriding legitimate interest.

\* \* \* \* \*