

RESOLUTION NO. 765/2009

Principles applicable to Personal Data Processing Operations for the Internal Reporting of Financial Wrongdoing (Ethics Guidelines)

The high number of notifications involving Personal Data Processing Operations for handling internal reports of financial wrongdoing (ethics guidelines) and the timeliness required to evaluate them justify the decision of the Portuguese Data Protection Authority (CNPD) to adopt this general-type resolution for application to this type of processing operation.

The aim of this resolution is to establish the principles set down by the Portuguese Data Protection Authority (CNPD) for assessing reports submitted to it. A direct reference will be made in the authorizations being granted to the legal grounds set down herein. This resolution also intends:

- to provide - to those entities responsible for processing the reports - the data protection principles applicable in these situations and to establish the rules for compliance with the Data Protection Act;
- to inform data owners of their rights and the limits established for these data processing operations.

Thus, having regard to:

- Article 35 of the Constitution of the Portuguese Republic;
- Convention 108 of the Council of Europe, of January 28, 1981;
- Directive 95/46/CE of the European Parliament and Council, of October 24;
- Law no. 67/98 of October 26, that approved the Data Protection Act (Law 67/98);
- Law no. 59/2007, of September 4, that approved the twentieth amendment to the Penal Code;
- Law no. 48/2007, of August 29, that approved the fifteenth amendment to the Penal Procedural Code;
- Article 245 A of the Securities Code re-published by Decree/Law no. 357-A/2007, of October 31, and amended by Decree/Law no. 211-A/2008, of November 3, by Law no. 28/2009, of June 19, and by Decree/Law no. 185/2009, of August 12;

- Article 4 of Law no. 19/2008, of April 21;
- Recommendation 2005/162/CE of the European Commission, of February 15, related to the role of non-executive directors;
- Opinion no. 1/2006, of February 1, of the Group of European Data Protection Commissioners (Article 29 Working Group)¹;
- The Governance Code of Securities Companies, of September 2007².

The Portuguese Data Protection Authority (CNPD) has decided to establish the general principles and conditions applicable to Personal Data Processing Operations for the **Internal Reporting of Financial Wrongdoing (Ethics Guidelines)**.

Background

As a result of the cases involving *Enron* (December 2001), *WorldCom* (July 2002) and *Tyco* (2002), in 2002 the United States of America approved the Sarbanes-Oxley Act, that requires companies listed on the stock exchange to promote a system for reporting situations of corruption or mismanagement in general, designated as whistleblowing³, as a way to foster accountability and transparency in companies and to contribute to the financial security in the international financial markets.

On February 15, 2005, the European Commission - as a result of the actions of other community entities - approved recommendation 2005/162/CE of the European Commission, whereby it invites member states to provide incentives to companies listed on the stock exchange (defined as companies whose securities are accepted for negotiation in a market regulated by the Community) to disclose and to comply with "Ethics Codes".

According to the aforementioned recommendation, the boards of directors or supervisory boards of corporations must establish boards of auditors which - among other things - will be responsible for monitoring the procedure whereby the company complies with the current provisions pertaining to the ability of employees to report financial wrongdoing.

¹ Available (9/9/2009) at http://ec.europa.eu/justice_home/fsj/privacy/ocs/wpdocs/2006/wp117_p5.pdf

² Available (9/9/2009) at <http://www.cmvm.pt/NR/exeres/9505C5ED-7D91-4B3A-B97E-47A04EF72B43.frameless.htm>

³ In simple terms, whistleblowing can be defined as a system whereby companies create the conditions under which people can report fraudulent or improper conduct that could seriously affect its activity.

The Working Group - created in accordance with Article 29 of Directive 95/46/CE - issued an opinion on the topic, although limited to the formal application of the rules with regard to data protection of the European Union to internal systems for reporting violations in the fields of accounting, internal accounting review, auditing, the fight against corruption and banking- and finance-related crimes – cf. Opinion 1/2006, of February 1, 2006.

The objective of the aforementioned opinion was to establish a joint position of the data protection authorities at the European level, in response to the anonymous reporting systems of cases or situations of corruption or internal mismanagement in companies listed on the stock exchange as required by the US Sarbanes-Oxley Act, enacted in 2002, following the Enron case, as a way to promote accountability and transparency in companies and to contribute to the financial security in international financial markets.

In the conclusion of its opinion, the Article 29 Working Group, recognizing that whistleblowing systems can help implement (good) governance principles in companies and detect misconduct that has an impact on their financial situation, insisted on the need to strictly apply data protection principles in this area, in particular with regard to the rights of the individuals - whose behavior is being reported - to be informed of the situation, to access, correct and delete the data, and their right to file an objection.

The anonymous system has been rejected in favor of a system of confidentiality, in order to prevent risks of libelous reporting and discrimination.

The group has acknowledged the possibility of restricting these rights when required by the interests pursued by the system, the protection of the rights of the other individuals involved, in particular of the whistleblower, and the purposes of the investigation. As the text of the opinion indicates, topics were addressed such as the compatibility of the whistleblowing system with criminal and/or labor systems insofar as they are specific to the jurisdiction of each member state, in addition to being clearly beyond the scope of the mandate conferred to the Working Group.

In September 2007, the Portuguese Securities Market Commission (CMVM) - affirming the aforementioned recommendation 2005/162/CE of the European Commission – issued the

Corporate Governance Code, which under its point II.1.6, states the rules regarding the adoption of a policy for reporting misconduct and specifically indicating the procedure for reporting misconduct internally, which people are authorized to receive the reports and the treatment (including confidentiality) given to such reports. The CMVM further recommended that the general lines of the whistleblowing policy be disclosed in the company's annual governance report, as previously stated in recommendation 10-A of the Securities Market Commission (CMVM).

The Securities Code, in the last amendment introduced by Decree/Law no. 185/2009, of August 12, established new elements for the adoption, implementation and publication of the corporate governance code, reflecting the pre-project findings prepared by the Securities Market Commission (CMVM)⁴.

The mandatory whistleblowing system in the Portuguese legal system, meets the provision in Article 242⁵ of the Penal Procedural Code, in the wording given by Law no. 48/2007 of August 29.

Due to the integration of the subjective element in a context of mandatory reporting, this depends on the position of the employee within the company.

The concept of employee, for criminal law, covers a range of situations that go beyond the concept of government worker in the strict sense.

⁴ Available (9/9/2009) at <http://www.cmvm.pt/NR/doniyres/9405C5Ed-7D91-483A-B97E47A04EF72B43/8427/TRANSPOSICAOPARCIALDIRECTIVA.pdf>

⁵ The wording provided for the Penal Procedural Code (our underlines):

Article 242

Mandatory reporting

1 – Reporting is mandatory, even when the people perpetrating the crime are unknown:

a) For police organizations, with regard to all the crimes of they become aware of;

b) For employees, in the acceptance of Article 386 of the Penal Code, with regard to crimes they become aware of during the exercise of their duties or as a result thereof.

2 - When various persons are required to report the same crime, the presentation by one of them releases the others.

3 – When referring to a crime whose procedure depends on a particular complaint or accusation, the report only takes place at the onset of an inquiry if the complaint is represented in the legally provided term.

Article 386⁶ of the Penal Code, according to the wording provided by Law no. 59/2007, of September 4, describes the concept of employee.

Law no. 19/2008, of April 21, when introducing measures aimed at fighting corruption, introduces guarantees protecting whistleblowers who are employed by the government or state-run companies and who report violations they become aware of during the exercise of their duties or for as a result thereof⁷, establishing a favorable legal supposition to the whistleblower, and the right not to be identified (unless for investigators) and the right to a transfer at their request.

Companies are adopting procedures aimed at stimulating the internal reporting of misconduct, to prevent or curb alleged misconduct within it, avoiding the aggravation of damage that this misconduct could cause by continuing.

Ethics codes have become commonplace in larger companies, which are establishing whistleblowing systems in order to prevent fraudulent actions.

⁶ The wording provided by the Penal code:

Article 386

Concept of employee

1 – For purposes of criminal law, the term “employee” covers:

- a) the civil employee;
- b) the administrative agent; and
- c) anyone, even temporary or provisional, who for compensation or free-of-charge, voluntarily or by order, has been called upon to perform or to participate in the performance of an activity included in the administrative or jurisdictional public function, or in the same circumstances, to perform duties in public utility organizations or participate in them.

2 – Employees include managers, heads of inspection organizations and workers of nationalized public entities, state-owned entities or those entities in which the state has a majority interest and companies that are concessionaires of public services.

3 – The following are also employees for purposes of Articles 372 to 374:

- a) magistrates, employees, agents and equivalents of the European Union, regardless of nationality or residency;
- b) employees who are citizens of other member states of the European union, when all or part of the violation has been committed in Portuguese territory;
- c) All those who perform duties identical to those described in part 1 within any international or public law organization of which Portugal is a member, when all or part of the violation has been committed in Portuguese territory;
- d) all those who perform duties within procedures of extrajudicial settlement of conflicts.

4 – Employee, for purposes of the criminal law, covers anyone who carries out public functions and who is regulated by a special law.

⁷ Cf. Article 4 of Law no. 19/2008, of April 21

The Portuguese Data Protection Authority (CNPD) is required to determine whether the processing of reports complies with data protection principles, specifically with regard to the quality of the data and with regard to the scope and admissibility of the processing.

Prior review

Processing operations of [personal] data in order to manage internal reports of financial wrongdoing (Ethics Guidelines) have an effect on data that, although not classified as sensitive data as provided in Article 7 of Law 67/98, are considered as being specifically protected (cf. section 2 of Article 8 of Law 67/98) and accordingly legally subject to special protection that requires a prior review by the Portuguese Data Protection Authority (CNPD), in accordance with paragraph a) of Article 28 of Law 67/98.

Consequently, a processing operation may not begin before authorization has been secured from the Portuguese Data Protection Authority (CNPD); the authorization is issued according to the terms and conditions established after informing the Commission of the processing.

Principles of data protection

With regard to the quality of the data, it must be in compliance, pertinent and not excessive with regard to the end purpose of the gathering procedure. The processing must be performed legally and in accordance with the principles of good faith and transparency in order to be admissible.

Compliance, pertinence, and the need for the non-excessive data are gauged by evaluating the categories of the data collected as a function of the purpose of the processing.

In particular the principle of proportionality

Determining the interests in question of the entity responsible and the data owners with regard to the principle of proportionality, the Portuguese Data Protection Authority (CNPD) will check whether the reported processing of data has been shown to be the appropriate means for the anticipated purpose, on one hand, assuring the protection of the personal data and the other fundamental rights of the data owners, and on the other, the interest of the entity responsible

which is also based on the law that cannot be condensed more than necessary; a fair balance must also be achieved that does not affect the essential content of the rights in question.

This determination first and foremost requires preserving the right to dignity, privacy and protection of the personal data of all people, as a basic right explicitly set down in the bill of individual rights, liberties and guarantees, with the private interest of the entity responsible for the processing operation admitting that there is generally a mutual interest in promoting accountability and transparency in companies and in contributing to the financial security in international markets.

With regard to the scope and admissibility, it is important on one hand for the Portuguese Data Protection Authority (CNPD) to check whether conditions under which the data has been gathered and processed are legitimate, and on the other, that the assurance of respecting the fundamental rights of the data owners, and the individuals whose behavior is being reported has been safeguarded.

Determining the criterion of proportionality becomes crucial in gauging whether the conditions for processing personal data are legal.

Basis of legitimacy

Processing can generally be authorized by the Portuguese Data Protection Authority (CNPD) when the processing operation has been proven by the entity responsible to be necessary for legitimate purposes, provided this does not take precedence over the rights, liberties and assurances of the data owner – section 2 of Article 8 of Law 67/98.

The processing of reports meets this legal requirement; it remains necessary however, to observe the “standards of data protection and security of information”, provided in Article 15, of Law 67/98, given the nature of the information in question – that is alleging illegal activities.

Entity responsible for processing the data,

According to paragraph d) of Article 3 of Law 67/98, the entity responsible for the processing is “the individual or group, with a public authority, a department of any other organization that

individually or in combination with others, determines the purposes and the means of processing the personal data”.

The obligations resulting from the Data Protection Act, i.e., the notification provided in Article 27, to secure prior authorization, must be assumed by anyone – upon acceptance of the aforementioned paragraph c) of Article 3 – who takes on that capacity, jointly or severally. The entity responsible must be indicated individually, only if accepting the joint responsibility among institutions when it is absolutely impossible to individually determine the responsibility for the processing.

The entity responsible will be the company that adopts internal procedures and assures means that permit the whistleblowing and subsequent investigation of conduct violating the law or the company’s or group’s policies and ultimately decides on the final destination for the report being presented.

The entity responsible for the processing must ensure that rules are adopted for implementing the communication and processing the reports, indicating the individuals or entities within the company or group specifically assigned to gather and process the reports, which shall be a limited number, with appropriate technical training and complies with its duty of confidentiality as assumed under contract.

These entities shall agree on their actions by means of principles of independence and impartiality and by respect for the principles in effect in domestic law, in particular in the Labor Code and the Penal Procedural Code.

Notwithstanding any types of subcontracting, the entity responsible for the processing will be limited to checking compliance with the measures of security, for which is legally responsible and the safekeeping of the adequate measures.

Subcontractors

If outside services are used to gather or process the data, the persons specifically entrusted with this mission within the service provider may only access the data within the parameters of their duties.

The service provider assumes under contract⁸ the responsibility for not using the data for other purposes, for ensuring its confidentiality, for respecting the period of safekeeping and destroying or returning all the manual or computer supports of the personal data in accordance with the period of performance of the contract.

Notwithstanding the described contract obligations, it will always be necessary to reaffirm the obligation of the result required of the entity responsible for the processing regarding the maintenance of the quality and security of the data.

Purpose of the processing

The purpose is a decisive element for gauging the admissibility and requirements of the Personal Data Processing Operations.

As stated by paragraph b) of Article 5 of Law 67/98, the personal data being processed must be gathered for a determined set of clear and legal purposes; any subsequent processing is incompatible with this purpose. The purpose of the processing of data object of this resolution is the management of the internal reports of wrongdoing.

Thus, only reports intended to prevent and/or to repress wrongdoing within the companies, in the fields of accounting, internal accounting review, auditing, the fight against corruption and banking- and finance-related crimes may be processed, in order to guard against the occurrence of more serious damage for the activity of the companies, to promote accountability and transparency thereof and to contribute to the financial security on international financial markets.

Categories of data

In accordance with the paragraph a) of Article 3 of Law 67/98, personal data includes “information of any kind and independently of its support, including sound and image [recording], related to an identified or identifiable individual (“data owner”); a person is considered identifiable who can be directly or indirectly identified specifically by reference to an identification number or one or more specific elements of his/her physical, physiological, psychological, economic, social or cultural identity”.

⁸ In accordance with the obligation of reducing the contract provided in Article 14 of Law 67/98, of October 26

The supply of information by the entity responsible for the processing to the data owner is a basic right under the data protection system, protected under the constitution and is a corollary of the principles of good faith, legitimacy and transparency.

b) Right of access and correction

The right of the data owner to access his/her personal data, and the corresponding right to correct the data are also basic rights (section 1 of Article 35 of the CRP); these rights are crucial for the verification of the principles of compliance, accuracy and updating of a person's data (paragraphs c) and d) of Article 5 of Law 67/98).

Thus, the entity responsible for processing the data must ensure that the data owner has the right to access his/her data and to request its correction or deletion if it proves to be inaccurate, incomplete or erroneous – Article 11 of Law 67/98.

When processing data in order to determine the truthfulness of the alleged criminal conduct, the right of access is exercised through the Portuguese Data Protection Authority (CNPD) – section 2 of Article 11 of Law 67/98.

The individual whose behavior is being reported cannot however obtain information on the identity of the whistleblower from the entity responsible for processing the data. However, legal protection of the individual whose behavior is being reported will never undermine his/her basic rights, i.e., the defense of his/her reputation and privacy and in particular, his/her right to file a complaint for libelous reporting, in accordance with the provisions and penalties of Article 365⁹

⁹ The wording provided (our underlines):

Article 365

Libelous reporting

1 – Whoever, by any means - before an authority or publicly - with the intent to falsify the attribution, reports or launches on certain person the suspicion of practice of crime, with the intent that against him is proceeding, is punished with penalty of prison up to three years or with a fine.

2 – If the conduct consists of the false allegation of a violation of an order or lack of discipline, the agent can be handed down a prison sentence of up to one year or with a fine up to 120 days.

3 – If the means used by the agent involves presenting, altering or perverting evidence, the agent can be punished:

a) in case 1, with a prison sentence of up to five years;

b) in case 2, with a prison sentence of up to three years or with a fine.

4 – If the plaintiff is deprived of a freedom, the agent can be punished with a prison sentence of one to eight years.

5 – At the request of the plaintiff, the court orders that the ruling be made public, in accordance with Article 189.

of the Portuguese Penal Procedural Code, thereby limiting the confidentiality protection system by establishing use parameters.

Rights of the whistleblower

Those who use the mechanism will be informed of the identity of the entity responsible for processing the data, the purpose and fields covered by the report, the optional nature of the device, the non-existence of consequences for failure to use the device, the recipients of the report, any transfer of data to a State outside the EU and the right of the persons identified within the device to access and correct information.

Whistleblowers will also be warned that any **improper or bad faith use** of the reporting device could expose the person responsible to disciplinary sanctions and/or criminal prosecution.

Within these limits, the whistleblower will be given assurances of confidentiality in the processing of the data regarding him/her.

Transfer of data outside the EU

Communications of data outside the EU shall respect the provisions regarding international data transfers.

Compliance with the level of data protection conferred to a state that does not belong to the European Union is evaluated as a function of all the circumstances regarding the transfer, i.e., the nature of the data, the purpose and duration of the processing operations, the countries of origin and destination, the laws and the sector-specific rules in effect in the receiving State and the safety measures respected in that state – section 2 of Article 19 of Law 67/98.

Time period for keeping the data

In accordance with paragraph e) of section 1 of Article 5 of Law 67/98, a person's data "can only be kept for the length of time necessary to achieve the purposes of the collection or subsequent processing thereof.

Accordingly, and mindful of the purpose, the Portuguese Data Protection Authority (GNPD) considers that:

- Personal data indicated in the report will be immediately destroyed if it is shown to be inaccurate or useless;
- When a disciplinary action or legal prosecution is shown to be unwarranted, the data that was checked will be destroyed 6 months after the close of the investigations;
- If there is a disciplinary action or court proceeding, the data will be kept until the end of the proceeding. In this case, it will be kept under a restricted access system and for a time period that does not exceed the legal proceeding.

Security measures

Security measures must be applied to data contained in automated files as well as to data collected manually. Moreover, attention should be paid to the actual procedure where information is collected, processed and distributed.

Computerized systems must be structured to allow access to the processing of data by means of personal user IDs and passwords, that are changed periodically, or by other means of authentication. This access is recorded and its compliance monitored. Security measures must then be adopted that prevent unauthorized access to information.

Still with regard to security measures, restricted access must be guaranteed from the physical and logical standpoint, to servers of the system.

Moreover, backups must be made of information which shall only be kept in the area accessible to the system administrator.

With regard to data maintained on hardcopy, organizational measures must be adopted that ensure an identical level of security, preventing improper access and handling.

The entity responsible for processing the data must take the necessary precautions to preserve the security of the data, when gathering, communicating or preserving it. Independently of the security measures adopted by the entity responsible for processing the data, it is also responsible for ensuring the result of the actual security of information.

Specific limits

The possibility of expanding the whistleblowing system to internal policies of the company (or other public or private entities), rather than to areas identified in this resolution, would likely expand the range of data substantially, and might be considered as significantly intruding on a person's private life, which for the aforementioned reasons mentioned, is not admissible.

Thus, we point out the following limits:

a) Objective parameters

Due to the seriousness that this could represent for the data owners and for the principles of good faith, legitimacy and trust governing relations in the work place, it has been decided to restrict the whistleblowing system to the fields of accounting, internal accounting review, auditing, the fight against corruption and banking- and finance-related crimes¹⁰.

b) Subjective parameters

Only people who have been entrusted with management duties related to the fields of accounting, internal accounting review, auditing, the fight against corruption and banking- and finance-related crimes may be the object of the whistleblowing.

Considering the purpose for processing/communicating misconduct that seriously affects the credibility and the financial well-being of the institution, resulting from management activities – this mechanism should not be used to support a general-type whistleblowing system, particularly at the bottom level of an organizational structure, since the general nature of employees' work is not directly or indirectly involved in decision making at the management level.

The similarity of the understanding in Opinion 1/2006 of the Article 29 Working Group, in the General guidelines of 11/10/2005 and in the decision of 12/8/2005, decisions of the CNIL (French) and the Resolution of 3/26/2008 of the DataInspektionen (Swedish) joint data protection authorities.

This is accordingly a mechanism based on evaluating the company's risk, particularly at the managerial level and according to a top-down analysis, with the exercise of the right to whistleblowing performed according to bottom-up.

c) Procedural parameters

It has been further decided to consider the use of the system in question as restricted to a complementary mechanism of the company's regular business, limiting it to cases where the use of the other mechanisms of internal communication or those resulting from the national legal order is not objectively justifiable, thereby being considered as a subsidiary device in the terms and with the limitations described.

The necessary correlation that is required in this field falls on the judgment of compliance and pertinence of the data gathered and processed versus the final purpose in the collection/management of internal reports and misconduct intended to prevent and/or to repress misconduct within the companies, in the fields of accounting, internal accounting review and auditing, the fight against corruption and banking- and finance-related crimes, to avoid more serious damage for the activity of the companies, to promote the accountability and transparency and to contribute to the financial security in international financial markets – making it possible to gauge the proportionality of the recommended solution.

d) Autonomy of willingness

A controversial issue with particular repercussion at the ethics level of the device is considered with the mandatory or optional nature of the report.

From the application of the criminal and penal procedural system subsidiarily to other branches of the law, that contemplate a law similar to that argued in the criminal procedure¹¹, either due to the suspected violation, crime or serious misconduct whose interference with the social sphere justify legal sanctions, justify the defense of an approach for a volunteer system of whistleblowing, limited only with the application of the general criminal system, with the

¹¹ This occurs, with regard to law governing violations of orders and the disciplinary law within the field of labor relations.

whistleblowing necessarily occurring in situations when determined by criminal and procedural law.

e) Entity responsible for evaluating the whistleblowing reports

Using the same line of argument that was defended with regard to the capacity of the individuals whose behavior is being reported, namely compliance of the processing with regard to the purpose accepted by this Portuguese Data Protection Authority (CNPD), the establishment of a line of internal reporting - whose management and evaluation is the responsibility of the persons whose behavior is being reported - is not considered as being consequential.

Thus, in accordance with the Governance Code of Companies of the Securities Market Commission (CMVM), the management and preliminary evaluation of the reports presented must be restricted to independent auditing entities, which are responsible for - among other duties - controlling the procedure whereby the company complies with the current laws with regard to the possibility of employees reporting wrongdoing.

In this case, it is appropriate to make a distinction of systems:

- a) either this entity is provided in the corporate structure, without prejudice to the exercise of functions described with independence and whose confidentiality is assured, without resorting to the use of subcontractors, thereby applying the system of the entity responsible for processing the data¹²;
- b) or an entity outside the corporate structure is used, in which case the system of subcontracting already described in this resolution is applied, in accordance with and for the purposes described in Article 14 of Law 67/98¹³.

Lisbon, September 21, 2009

Ana Roque, Luís Barroso, Helena Delgado António, Carlos Campos Lobo, Vasco Almeida, Luís Paiva de Andrade.

Luís Lingnau da Silveira (chairman)

¹² See pages 10 and 11 of this decision.

¹³ Cf. the subcontracting best system described on page 12 of this decision.