INSTRUCTION

No.11, date 08/09/2011

ON

"PROCESSING OF DATA OF EMPLOYES IN PRIVATE SECTOR" AMENDED TO INSTRUCTION No. 28, DATE 27.12.2012

Pursuant to letter "c" of point 1 of Article 30 of letter "ç" and "f" of Article 31 of Law No. 9887, date 10.03.2008 "On the protection of personal data" amended to Law No. 48/2012[1],

INSTRUCTS

1. The instruction herein determines the rules on the processing of personal data of employees (collection, registration, storage, ranking, adaption, correction, counseling, exploitation, use, blocking, deletion or destruction, transmission, etc.) employed in private sector.
2. This instruction applies to the processing of personal data of employees dealing with the information acquired by the employer within the procedure of hiring employees and throughout the working process in pursuance of employment contracts with the employees.
3. Processing methods are related to:
   a) Employees' personal data (recruited or dismissed), biometric data, photos and sensitive data related to third parties, specific data related to religious belief or adherence to unions, data on the state of health, in the composition of medical certificates or other documents that serve for special permits or to justify absences at work as well as benefits provided in collective agreements.
   b) Information closely related to the development of the work activity, such as the type of contract (fixed or indefinite, full or partial time, etc.), qualification and professional level, personal payments, payments for "special" merits, remuneration, working hours, vacations and personal leave (used or remaining), absences and services in cases provided by law or collective labor contracts, transfers to other jobs, procedures and disciplinary decisions.
4. These data are carried:
   a) In acts and documents produced by employees for employment (referring to the information collected through notices that constitute job offers, or during the employment report);
   b) In documents or files processed by (or on behalf of) employers depending on the employment relationship for the purpose of completing the employment contract and collected and stored in personal files, archives on paper or electronically of private entities.
   c) In books and board decisions, still used by private entities.
5. Adherence to the principles of personal data protection.

5.1. Information containing personal data should be processed by the employer to the necessary extent during the employment relationship, so that they are necessary for the

[1] Amended by Instruction no. 28 dated 27.12.2012 "On some additions and changes to Instruction no. 11 dated 8.9.2011 "On data processing of employees in the private sector"

implementation of the requirements provided in the applicable legislation (regulations, contracts and collective agreements).

5.2. In any case, important and not redundant information should be processed and all provisions of law no. 9887 dated 10.03.2008 "On the protection of personal data" amended by law no. 48/2012[2].

5.3. Personal data processing to be performed:

a) fairly and lawfully;
b) be sufficiently accurate to be maintained in such a way as to allow the identification of the data subject for as long as is necessary for the purpose for which they were collected or processed;
c) informing utterly and in advance the interested;
d) meeting the legal processing criteria;
e) respecting the requirements regarding the handling of sensitive or judicial data;
f) With security measures able to protect data from cases of damage, loss, access and unnecessary use, etc.

5.4. Processing of personal data (including sensitive, judicial, etc.,) referring to specific employees, is lawful, if it is intended to resolve obligations arising from individual contracts, collective labor contracts or special laws.

5.5. The purpose specifically pursued by the employer on the basis of personal data processing should not be incompatible with the purposes for which they were collected.

6. Personal and sensitive data processing officer.

6.1. The head and responsible for processing for the purpose of personal data protection should pay an important role to the appointment of employees who with different titles can process the data, defining the respective tasks, in special regulations or in parts of general regulations.

6.2. Particular importance should be given to the definition of tasks related to the processing and protection of sensitive data related to health, by the physician (of the private entity) in compliance with the laws in the field of insurance and occupational hygiene.

6.3. The competent doctor performs preliminary and periodic checks on employees and maintains (making updates) a health card for each employee. This card is stored with “professional secrecy” in mind. A copy is given to the employee at the time of termination of the employment contract or when he requests it. In case of termination of the employment contract, when these cards are required by the institutions responsible for prevention and safety at work should be sent in the original and in a sealed envelope.

6.4. The competent physician is obliged to process the health data of the employees, proceeding with the appropriate notes on the health cards, taking care of the possible security measures to maintain the secrecy of the processed information in the report, the purpose and the manner of processing.

6.5. Employees' medical records cannot be opened by the employer, he just has to seek to provide effective protection, always respecting the "professional secret".

6.6. The employer is obliged, in the opinion of the competent doctor (or when the doctor informs about the anomaly or the appearance of risks), to take precautionary and protective measures for the interested employees. He may not fully recognize the possible pathologies, but only the final assessment of the employee's (health) condition, for his ability to perform his duties.

[2] Amended by Instruction No. 28, date 27.12.2012

6.7. Communications for various institutions of health cards in case of termination of employment contract are performed excluding any recognition of them by the employer.

6.8. Special measures should be taken to process employees' sensitive data regarding their health status. For such information are prepared (except personal data protection regulation) special agreements to specify, the data with which the employer may be acquainted to implement the employment contract.

6.9. The employer performs data processing in cases of treatment of diseases (from performing visits to specialists or clinical analyzes) that determine the impossibility of work (temporary or final, as a result of suspension or termination of the contract). It can handle data related to disability, of protected categories, in ways and for purposes described in existing field norms.

6.10. The employee is obliged to communicate with the employer and the disease prevention institutions not only to justify the expected legal and economic processing, but also to allow the employer or the preventive body to verify the real conditions of his health according to the law.

6.11. To implement these obligations, is used a standard model (a certificate of illness to be submitted to the employer), only with indicators of the onset and duration of the disease and “Diagnosis” which is submitted by employees, to institutions charged by law in cases where he has the right to receive compensation for illness.

6.12. When medical certificates are completed differently from the standard model where data and diagnosis are not shared, employers have the duty to take steps to take appropriate action to prevent their submission to unauthorized persons.

6.13. When the employer must report to certain bodies according to the laws on accidents and occupational diseases of employees even though it is legitimate to recognize the diagnosis for his part, he should communicate to the body designated by law only health information about the reported pathology and not the health data that have been verified during the employment relationship, as it would be redundant and not within the purpose.

6.14. The employer processes health data with which it is notified the health status of employees when the latter seek to participate in programs rehabilitation or treatment while retaining the job (free of charge) when forced to submit (according to the provisions of the collective agreement) specific medical documents.

6.15. The employer must communicate the data regarding the health status of employees, public entities (prevention and assistance bodies) to meet specific obligations (arising from the law, norm, rules, contractual provisions), within the limits of information only necessary for the purpose.

7. Security measures for sensitive data.

7.1. The employer is obliged to take security measures (article 27) on the protection the employees’ personal data processed in the domain of labor relation, paying attention to sensitive data.

7.2. Sensitive data should be kept separate form any other personal data of the employee. This should apply, with the personal information of employees, the establishment of special rules dedicated to the protection of sensitive data and employee health. They are kept separate in ways that do not allow a long unwanted consultation along ordinary administrative activity.

7.3. In cases where employees submit various medical certificates, the employer should take appropriate measures to prevent obvious diagnoses in the structure of the certificates, in order to prevent any abusive entry into such data by persons who are not assigned as responsible or in charge of processing this data.

7.4. The employer assigns special persons in charge of processing employee's personal data, who must have full knowledge about the protection of personal data and constantly receive the necessary information in this domain. In the absence of adequate information from those in charge of processing personal data, respect for the privacy of employees in the workplace can never be guaranteed.

7.5. The employer, among other things, must take organizational and physical measure to guarantee:

a) the places where the processing of personal data of employees is performed should be protected from unnecessary interference;
b) personal communications with employees should be made in such a way as to exclude the involvement of third parties or non-designated entities as in charge;
c) provide clear instructions to the responsible person regarding the confidentiality of data, even for employees of the same employer who do not have the right to be informed of specific personal information;
d) to prevent the receipt and reproduction of electronically processed personal data (in the absence of proof or authorization) of documents containing personal information by unauthorized entities;
e) to prevent the unintentional taking of personal information by third parties or other employees by taking measures to place it in a particular form of offices;
f) take appropriate measures to prevent the spread of information by respecting the security distance or by processing confidential information in enclosed spaces and not in open spaces.

8. Biometric data and access to "reserved areas"

8.1. The use of biometric data in the workplace is realized especially for the control of entry and exit in specific areas of private entities (dangerous, important areas, where valuable materials are stored, etc.) as well as for the application of the rules of discipline at work by the employee side.

8.2. Biometric data are personal data (physical characteristics, digital data, fingerprints, etc.) that are collected according to a special procedure (partially automated) that results in a reference model, as a set of numerical values of the individual characteristics shown above, capable of identifying the individual through various operations and the numerical code collected at each input-output.

8.3. The use of biometric data, (especially digital traces), is done in respect of the principle of proportionality. These data, due to their characteristic nature, require taking high security measures to prevent possible consequences for employees, especially in relation to illegal uses that abusively determine the "reconstruction" of traces, based on the reference model and Further "use" without their knowledge.

8.4. The use of biometric data can only be justified in special cases, taking into account the purposes and the meaning in which they are treated, to take care of the entrances to "reserved areas" taking into account the nature of the activity that takes place, (production processes of dangerous, storage of important assets and valuable objects, secret documents, etc.).

8.5. Establishing a personal data archive (with biometric data) results in a disproportionate and unnecessary rule. Information systems should be configured to minimize the use of personal (biometric) data and exclude treatment when the goals pursued may be achieved in other ways that do not use biometric data (personal cards, entry sheets, special personnel etc.).

8.6. The site, biometric data processing modes, should be appropriate and sufficient to have efficient biometric data verification systems based on digital trace reading. The collected data is stored on the holder exclusively available to employees (smart card or analog slide) which excludes the use of identities being sufficient to give each employee an individual code.

8.7. Such a recognition mode ensures entry into the reserved area (restricted access area) only for authorized persons, leaving it to their choice to choose an analog card or slide. The model on the card or on the slide can be realized by following common procedures thus avoiding the formation of a biometric data archive.

Caution should be exercised in cases of loss of card or slide, as a possible circumstance of abuse in connection with memorized biometric data.

9. Security measures and storage time of biometric data.

9.1. The personal data needed to complete the model can only be processed during the registration phase. For their use, the controller must collect prior consent by informing the employees.

9.2. Adapt further measures for the protection of personal data, giving persons responsible for data processing special instructions, especially in cases of loss or removal of employees' cards or slides.

9.3. Access to memorized data should be allowed only to specific employees in compliance with security measures, only for the purpose of verifying and protecting them (also respecting the rules on remote control of employees).

9.4. The collected biometric data cannot be retained for a longer period of time than is necessary to meet the purposes for which the data were collected. This time limit can be legally extended, but in any case the appropriate mechanisms for automatic data deletion must be provided[3].

9.5. If the use of biometric data is not regulated by law, the personal data controller (employer) must first notify the Personal Data Protection Commissioner on the purpose and reasons for the collection and use.

10. Workplace surveillance camera.

10.1. The employer may use a continuous surveillance system in the workplace based on the use of technical equipment that transmits images or data (surveillance cameras) for the personal safety of employees and other persons in these premises for the protection of property and to prevent or investigate situations that endanger security.

10.2. The surveillance camera cannot be used to supervise an employee in the workplace. The surveillance camera cannot be used in toilets, changing rooms or other similar places, or in designated work rooms for the personal use of employees.

10.3. Notwithstanding paragraph 10.1, the employer may direct the surveillance camera to a particular workplace where employees are at work if the observation is essential to:

[3] Amended to Instruction No. 28 date 27.12.2012

a) prevent a significant threat of violence in connection with the work of employees, a significant harm, risk to the safety of employees or their health;
b) protect the interests and rights of employees, when the surveillance camera is based on the request of the employee who is subject to supervision and the matter has been agreed between the employer and the employee.

11. Transparency over camera surveillance.

11.1. When planning and implementing surveillance cameras, the employer must ensure that:

a) the use of other devices before the installation of the camera surveillance system has not achieved the purpose for which these devices were installed;
b) not have interfered in the private lives of employees more than is necessary to achieve the purpose of their use;
c) the use and processing of other records of persons obtained through supervision shall be planned and carried out in accordance with the provisions of the Law on Personal Data Protection;
d) records should be used only for the purpose for which the supervision was performed;
e) employees should be informed when surveillance with cameras will begin, how it will be implemented, as well as for camera locations;

11.2. The data retention period in a camera surveillance system is determined according to letter "c" of paragraph 4 of instruction no. 13, dated 22.12.2011 "On some addenda and amendments to instruction no. 3, dated 5.3.2010 "On the video surveillance system in buildings, premises and various premises", approved by the Commissioner for Protection of Personal Data "[4]

12. Communication and disclosure of personal data.

12.1. The employer must obtain the prior and specific consent of the employees in cases of communication and dissemination of personal data (regarding the circumstances of a possible employment, status, qualification, sanctions for discipline or employee transfers) for third parties such as:

a) companies (of the same category as well) of employers or former employees (also in the same private entity);
b) Acquaintances, family members and relatives.

12.2. The employer must regulate the ways of processing by defining the persons (internal or external, charged or responsible for processing), who can obtain knowledge of the data during the employment relationship, defining the functions and instructions where to rely.

12.3. The employer may communicate to third parties in anonymous form data collected from information related to employees or groups of employees such as the total number of overtime hours, non-working hours at the level of the private entity or within separate units of production, awarding of prizes, personal or group results, qualifications, professional levels, special functions or organizing groups.

12.4. Employee consent is required for the publication of personal information referred to him (photographs, civil status information or curricula) on the private sector network, required to perform the obligations arising from the employment contract.

12.5. In the absence of rules for the dissemination of personal data of employees, the controller may disseminate personal data of employees only if it is necessary to perform

[4] Amended to Instruction no. 28 date 27.12.2012

the obligations arising from the employment contract (of decisions on the boards of service orders, work tours or vacations, in addition to decisions regarding the organization of work and the assignment of tasks where there are special members and employees).

12.6. It is forbidden to disseminate personal information referring to employees through their publication on boards of private entities or in internal communications intended for employees, especially if it is not related to the performance of the obligations of the employment contract.

12.7. Disclosure is prohibited in cases of:

a) posters related to salaries or referring to special personal conditions;
b) disciplinary measures;
c) data or information related to litigation;
d) absences at work for illness;
e) registration or membership of special employees in associations, etc.

12.8. Identification cards are other forms of personal data dissemination when the information mentioned should be used on these cards placed on the employee's clothing or uniform (usually, in order to improve the relationship between employee, user or client).

12.9. For this, some clauses can be set in trade union-enterprise agreements, which may be part of the employment contract. In public relations, the placement of personal identification data on the card (identification code, name or role it covers) in accordance with utility, purpose and sufficiency is taken into account.

12.10. Excluding cases in which the forms and ways of using personal data derive from special legal provisions, the employer must use forms of personal communication with employees, taking measures that the communication of personal data, (especially if they are sensitive) to not for other entities other than the recipient and charge of treatment operations (e.g. by conducting communication with closed envelopes, inviting the interested party to personally withdraw the documents through the competent office, paying attention to individual electronic communications).

13. Information.

13.1. The employer is obliged to provide the employee, before proceeding with the processing of data related to him (also in cases where the law does not require consent), with individual information supplemented with the elements indicated in Article 18 of Law no. 9887, dated 10.03.2008 "On the protection of personal data" amended by law no. 48/2012[5].

13.2. For private entities in which, due to organizational or size reasons, it may be difficult for special employees to exercise their rights (according to articles 12-17 of law no. 9887 dated 10.03.2008 “On data protection personal “amended by law no. 48/2012[6]), a person specially responsible for handling such cases may be assigned, expressing it clearly in the information provided.

14. Exercise of employees rights.

14.1. Interested employees may exercise against the employer the rights provided by articles 12-17 of the law "On personal data protection" as amended by law no. 48/2012[7],

[5] Amended to Instruction No.28 date 27.12.2012
[6] Amended to Instruction No.28 date 27.12.2012
[7] Amended to Instruction No.28 date 27.12.2012

as the right of access to the data related to them, to be acquainted with updates, adjustments, additions, deletions, transformation into anonymous form or blocking if they have been processed in violation of the law, to oppose the processing for legitimate motives.

14.2. The request for access that does not refer to a particular processing, data and specific data categories, should be considered to refer to all personal data related to the employee as they may have been processed by the administration and may also relate to information of the evaluative type, according to the conditions and within the limits of article 14 of law no. 9887, dated 10.03.2008 "On the protection of personal data" amended by law no. 48/2012[8]. This does not include contractual or professional information that does not have the nature of personal data in any way referring to identified or identifiable persons.

14.3. The employer to whom the request is addressed is obliged to give a full response to the request of the interested employee, without being limited only to the list of typology of the received data, but by communicating clearly and comprehensibly all the information in the possession of his.

14.4. The answer must be given within 30 days of receiving the request from the interested party (officially submitted).

14.5. The employer, especially in cases of employment of a significant number of employees, must undertake appropriate organizational procedures to fully implement the provisions of law no. 9887, dated 10.03.2008 "On the Protection of Personal Data" amended by law no. 48/2012[9], in the field of data entry and exercise of other rights, also through the use of special programs aimed at carefully selecting data for each employee and simplifying and shortening the response time.

14.6. The answer must be given in writing form and only in cases where the interested party agrees can it be given orally. With the consent of the applicant, the employer may transmit the answer to him by computer. The interested party must receive the communication of the answer in the workplace or his in his apartment.

14.7. The exercise of the right of access allows only the communication of the personal data of the applicant held by the head of processing and extracted from the acts and documents, not provides for employers to request direct and unrestricted access to documents and all types of acts, or the creation of non-existent documents in archives or their improvement according to the special ways presented by the interested party or further, to always keep copies of documents collected or claim specific ways of responding.

14.8. In cases where the amount of personal information held by the head of processing is high, the right to access the data can be made by making available to the interested party the personal file, from which later extracts of personal information can be extracted.

14.9. Display or submission of copies of acts and documents for personal data required may be performed by the processing head only in cases where the extraction of personal data from these documents is particularly difficult for the holder himself, then removing personal data that may be related to digestion.

[8] Amended to Instruction No.28 date 27.12.2012

[9] Amended to Instruction No.28 date 27.12.2012

14.10. In giving the response for a request for access to the formulation according to articles 12-17 of law 9887 dated 10.03.2008 "On Personal Data Protection" amended by law no. 48/2012, the head of processing must communicate the required and effectively retained data and is not obliged to retrieve or collect other data that are not at his disposal and are not subject to any form of actual processing by his side.

14.11. At his request, the employee may be acquainted with the update of his personal data, the completion of personal data in the professional profile of the claimed qualifications, the obligations deriving from the employment contract and the decisions of the judicial bodies related to it.

15. Confidentiality.

15.1. The employer, who is informed on the processed data of the employees, during the exercise of their functions, is obliged to maintain confidentiality and reliability. This data is not disseminated, except in cases provided by law.

15.2. This means that the persons responsible for processing the data of the employees should not inform any unauthorized person of personal data which they see or learn during the work. The obligation to maintain confidentiality lasts indefinitely. The obligation does not end when the persons no longer exercise their functions.

16. Failure to comply with the requirements of this instruction constitutes a violation of the law on personal data protection and is punishable under Article 39 thereof.[10]

All controllers of the private sector are obliged to implement this instruction.

This instruction enters into force immediately and is published in the Official Journal.

THE COMMISSIONER

Flora ÇABEJ (POGAÇE)

[10] Added by Instruction no.28 dated 27.12.2012