INFORMATIVE NOTE

PLMJ
SOCIEDADE DE ADVOGADOS, RL

TELECOMMUNICATIONS, MEDIA AND TECHNOLOGY/ EMPLOYMENT & LABOUR LAW

PROCESSING OF EMPLOYEES' DATA BY COMPANIES

NEW GUIDELINES

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) - referred to here by its Portuguese initials "CNPD" – is the national regulatory authority responsible for personal data. At its plenary session on 16 July 2013, the CNPD approved Resolution no.1638/2013; however, the full text of the Resolution was only published on 14 November.

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) - referred to here by its Portuguese initials "CNPD" – is the national regulatory authority responsible for personal data. At its plenary session on 16 July 2013, the CNPD approved Resolution no.1638/2013; however, the full text of the Resolution was only published on 14 November. This important decision reviewed CNPD Resolution of 29 October 2002 on the same issue, which is the processing of personal data by the employer resulting from the use of the employer's information technologies by employees for private purposes.

What is at issue here is the use of the employer's telephones, electronic mail accounts and Internet access by employees for non-professional purposes. The essential issue here is to find an adequate balance between the employer's power of the management and the right to privacy of the employees.

On the main issues - the applicable legal principles and the procedures to be followed - there are no significant differences between the decisions of 2002 and 2013. What is new in the 2013 decision is the establishment of a number of rules that must be respected by employers. Another change lies in the fact that the CNPD has, for the first time, created specific technical and organisational measures that must be followed by the data controllers. This note will describe the new guidelines established by the CNPD.

Resolution no. 1638/2013 is not binding for data controllers. However, when processing of personal data takes place that requires prior authorisation by the CNPD, the CNPD will follow its own guidelines to decide whether it approves specific processing and the impact of this new CNPD Resolution on companies is notable for this reason.

In this decision, the CNPD did not address the processing of personal data resulting from geo-localisation systems and this issue will be subject to a separate and specific Resolution.

I - THE EMPLOYEE'S RIGHT OF PRIVACY IN THE CONTEXT OF THE EMPLOYMENT RELATIONSHIP

The employer's power of management of is limited by the rights and guarantees of the employee. This means it is necessary to find a fair balance between the right of privacy of employees and the freedom of management and organisation that the law grants to employers. The CNPD emphasises article 22 of the Employment Code, section 1 of which prohibits the employer from having access to the content of personal messages and information that is non-professional in nature when the employer's means of communication are used. Article 22 (2) gives the employer power of control by establishing rules on the use of work resources. However, this power does not include communications that the employee makes through accounts (electronic mail, social networks or of any other type) that the employee has signed up for on a personal basis, even if he or she accesses them through their work computer.

When it comes to the possibility or admissibility of prohibiting the use of work resources for personal purposes, the CNPD makes it clear that it is unrealistic and impossible to do so absolutely.

It also adds that the means of control used must follow the principles of need, proportionality and good faith. The employer must demonstrate that it has chosen the forms of control with the least possible impact on the fundamental rights of their employees.

II - DATA PROCESSING: GENERAL RULES

A. Legal principles on the protection of data

The control of use for private purposes of information and communication technologies in the work context results in true data processing. This collection of data must have specific, explicit and lawful purposes which, in the work context, may consist of the management of the resources of the company and the productivity of its employees. The data collected in this way may not later be processed in any way that is incompatible with the purposes that were initially defined.

The data processing must not be abusive or disproportionate and this data must be appropriate and limited to what is strictly necessary to achieve the purpose of its collection, and this must be on the basis of «a serious business interest». It is, therefore, made clear that, whenever possible, employers must give preference to generic methods of control and avoid the individualised consultation of personal data.

The CNPD also emphasises that the employer may have access to traffic data associated with employees' communications, because the employer holds such records. This data is covered by secrecy of communications and, for this reason, there must be no individualised checking. This means that extracting information from communication lists is prohibited in order to protect traffic data that reveals the private life of the employee. The CNPD considers that the processing of only certain data such as the time and duration of the communication is sufficient for the purposes of control.

One relevant change is the specification of the period for conserving data obtained in the context of this type of processing. The CNPD considers that this period should be a maximum of six months. However, the employer may retain this data during the course of any disciplinary or legal proceedings.

B. Conditions for legality

The CNPD makes it clear that the grounds for processing the personal data of employees resulting from their use of the employers information systems for personal purposes is established in the law, specifically in article 22 (2) and article 97 of the Employment Code.

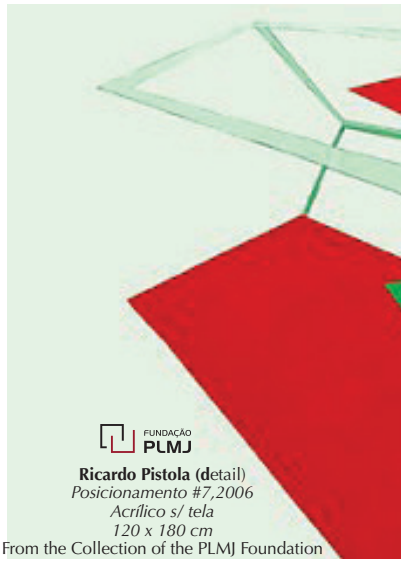
C. Interconnection and communication of third party data

The CNPD considers that the objectives of employers may be achieved without the need for recourse to interconnections that are deemed disproportionate. This means that the processing of data must not be subject to interconnections with other data processing that are the responsibility of the employer, (such as, for example, human resources databases), or of third parties.

No personal data may be communicated in anydata processing that involves passing information to third parties.

D. Right of access, rectification and elimination

The employer must inform the employees upon any individual request, of the conditions to exercise the right of access to their personal data, as well as the rights to rectify, delete or block it, and the employer must make all the information necessary for these purposes available.



Ricardo Pistola (detail)
Posicionamento #7,2006
Acrílico s/ tela
120 x 180 cm
From the Collection of the PLMJ Foundation

E. Procedures to be adopted by employers

The establishment of rules for use of means of communication, as well as the setting out of conditions for data processing and the forms of control, must appear in an Internal Regulation of the company. The preparation of these regulations requires the employer to consult the work council and for this regulation to be effective, it must be published and sent to the Employment Conditions Authority.

A further change is the obligation on the employer to carry out a prior assessment of the impact of the control measures it intends to implement (the CNPD speaks of a Privacy Impact Assessment).

Besides the approval and publication of internal regulations, the employer needs the prior authorisation of the CNPD before going ahead with the processing of personal data.

F. Security measures

The greatest change brought about by Resolution no. 1638/2013 probably lies in its specific definition of security measures. Among other measures, those responsible for data processing are under an obligation to implement a policy of a log analysis and to produce periodic reports on this analysis. The logs must be signed digitally and may only be retained for a period of one year.

III - PROCESSING OF SPECIFIC DATA

A. Control over telephone communication data and traffic data

The CNPD emphasises that in its internal regulations the employer must strictly define the degree of tolerance as to the use of telephones and the forms of control carried out.

A further change is the obligation on the employer to carry out a prior assessment of the impact of the control measures it intends to implement (the CNPD speaks of a Privacy Impact Assessment).

In general terms, the employer is prohibited from having access to the content of telephone communications, from the use of any listening devices or from storing, intercepting or monitoring communications. The recording of telephone calls may only occur in situations and under the terms defined in the law and established in Resolution no. 629/2010 of the CNPD, of 13 September. These include: for the purpose of proving the contractual relationship, emergency calls and monitoring of the quality of call answering. This processing may never be used for the purposes of management of resources and control of employee productivity.

According to the CNPD, a limited period must also be established for conservation of this data and this must not exceed the legal period for the payment of the invoice. It is possible, depending on each particular company, to ensure the existence of a line not connected to the telephone exchange, for use in personal communications.

B. Control of electronic mail and traffic data

The Resolution under analysis here provides that the employer does not automatically have the right to open electronic mail addressed to an employer, regardless of the rules of the company on the use of electronic mail for private purposes. One new provision is that the employer must require employees to create a specific folder in which they should file all electronic mail with personal content.

The Resolution also introduces a requirement to define the procedures that must be followed by the employer when it has access to the content of its employees' electronic mail accounts. According to the CNPD, access to electronic mail must always be done in the presence of the employee in question and, preferably, a representative of the work council or other employee representative. This access must be limited to looking at the addresses to which mail was sent, the subject and the date and time of sending. The employer must not consult the content of the messages as the mere registration of sending meets the processing objective.

New rules also exist for cases of prolonged absence or termination of the contract of employment. In the event of absence of the employee, an automatic response (out of office) mechanism must be put into place, with the indication of an alternative address. The reasons for having access to the absent employee's mailbox must be explained clearly and communicated to the employee in the internal regulations. This access must also take place in the presence of a representative of the workers' committee or some other person indicated by the employee in question.

If an employee leaves the employment of the company, that employee must be granted a period of time in which to remove any personal content stored in their electronic mail and the respective account must then be deleted. The employer must ensure that the same e-mail address is not later attributed to another employee.

C. Control of Internet browsing

According to the CNPD, the employer must use the internal regulations to guarantee that employees are duly informed of the limits on use of the Internet for private purposes. The CNPD also considers that a certain degree of tolerance should be allowed in relation to Internet access, specifically when this occurs outside the work timetable.

The CNPD recommends the use of filters that make it impossible to visit certain websites that are not authorised by employers, or to limit the periods in which use of the Internet is authorised. Such filters are to be used in preference to methods of checking which websites have been seen by employees.

Statistical processing of the most consulted sites is allowed, without identifying the respective workstations and it is also possible to record the average connection time, regardless of the sites consulted. In the case of excessive or disproportionate access, the employer must warn the employee in relation to the level of use.

The CNPD emphasises that in its internal regulations the employer must strictly define the degree of tolerance as to the use of telephones and the forms of control carried out.

The CNPD also emphasises that the daily access time and the sites consulted by each employer must only be checked in exceptional circumstances, including at the initiative of the employee (when the indications of the employer are called into question and the employee wishes to allow such access).

D. Remote access to the employee's computer

This is a new point in relation to the 2002 decision. The use by the employer of systems that make it possible to visualise, follow or monitor the actions carried out on the computer is prohibited, as is looking for or extracting any information stored there.

In the same way, systems that make it possible to search for and locate documents automatically and remotely, for example, through the use of key words, are prohibited.

Any procedures to make backup copies of the information contained on individual computers or to centralise professional documentation in a general archive, must guarantee that information of a private nature is not accessed and copied. This makes it necessary to ensure a clear separation of personal and professional folders.

The CNPD also emphasises that the daily access time and the sites consulted by each employer must only be checked in exceptional circumstances, including at the initiative of the employee (when the indications of the employer are called into question and the employee wishes to allow such access).