apdcat

Autoritat Catalana de Protecció de Dades

Recommendation 1/2013

of the Catalan Data Protection Authority on the use of email in the work environment

Generalitat de Catalunya

Introduction

Use of the information and communication technologies (ICT), especially email systems, in the management of public administrations has undoubtedly meant a huge advance in the efficiency of public sector activity. The immediate nature of communication, immense volume of material that flows around the net, possibility of accessing information outside the workplace and reduction in costs that results from using email systems have turned this tool into an indispensable element in any administrative organisation. However, the undeniable positive aspects inherent in these technologies should not lead to an underestimation of the risks involved for information security and the protection of personal data in the use of emails.

According to that established in Article 8.2e) of Law 32/2010, of 1 October, of the Catalan Data Protection Authority, it is the responsibility of this Authority's director to draft the instructions and recommendations necessary to bring personal data processing into line with the principles of current legislation in the area of information privacy. It is therefore appropriate to offer guidelines and best practices in the use of these communications systems through a Recommendation.

This Recommendation is addressed to Catalan public administrations, as well as to other institutions that fall within the Catalan Data Protection Authority's scope of action. Regardless of their public or private nature and the kind of contractual relationship they establish with their employees, these bodies adopt the legal position of the employer. In this Recommendation we therefore refer to all such entities with the term *company*.

In particular, the Recommendation is aimed at those responsible for information and/or security, and at employees of these institutions who undertake work related to the configuration of ICT systems and information security within the company. It is intended to be an aid to reflection prior to taking information-related decisions.

This Recommendation is complemented by the *Manual on the Proper Use of Email*, which is published alongside it. The Manual can be downloaded from the Authority's website and is addressed to all employees in these institutions who need to use email to carry out their duties. It will encourage them to adopt practices that ensure the appropriate handling of their own personal information, as well as the privacy of that pertaining to third-parties.

The purpose of this Recommendation, which does not have the status of a law, is precisely to provide guidelines to help organisations regulate and supervise the use of email in the work setting. Consequently, it includes suggestions which can facilitate the adoption of best practices and contribute towards better security and greater respect for people's rights, especially that of the protection of their personal data. This is a task that each organisation must carry out in accordance with its needs when handling the information for which it is responsible. The establishment of rules for the use of email is therefore fundamental to this question.

In any case, given the changing nature of technology and, consequently, of the matter which is the subject of this initiative, this Recommendation is not considered something static, but rather as a dynamic tool whose application will be subjected by the Catalan Data Protection Authority to a continuous process of analysis to monitor the results of its implementation and to adapt its provisions to any new issues that may arise.

I. The email

1 Email systems

Email is a messaging system which allows the transmission of messages between users without their needing to be connected at the same time. There are various applications that enable emails to be managed and which can be grouped, basically, into two categories:

- ❑ Email client

  These are programs (e.g. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.) that manage the sending and receipt of messages. The program downloads all messages and stores them in the computer memory, without detriment to certain protocols (e.g. IMAP) that can hold them on the server. The program can be installed in different devices (desk-top computer, laptop, smartphone, tablet, etc.).

- ❑ Webmail

  There are also other systems, usually called webmail or web-based mail. While still being able to receive messages through an email client, these applications also enable the email server to be accessed via an Internet browser and the http or https protocol, thus facilitating the sending and receipt of mail through a website from any location with Internet access. The messages are stored in the server where the email account is located.

  Email servers may be located in third countries which perhaps lack an acceptable level of personal data protection and, especially in the case of webmail, their conditions of use can be established and modified unilaterally by the provider. When such services are offered free of charge these conditions often include authorisation for the processing of information for advertising or other purposes. The servers also frequently carry out automatic analysis of message content, which may be useful, for instance, in detecting viruses. It should be noted however that providers can also use the information to offer related advertisements in the same mail application.

Recommendation

✓ Allocate an email address to those employees who need one in the performance of their duties, be it through the email client system or webmail. In the latter case, ensure the provider has adequate privacy and security policies in place through the corresponding contract conditions and that these are binding on all parties involved.

2 The email address

2.1 The email address as personal data

The email address is a set of words or symbols that identify the sender or recipient of an email message. These are usually chosen by the address owner or the organisation to which that person belongs, with the sole limitation being that this address must not coincide with any other. It is made up of identification of the user, followed by the @ symbol and then the domain (identification facilitated by the service provider, with a dot and certain letters that indicate the organisation's activity (e.g. ".org") or the letters corresponding to the country (e.g. ".uk" or ".cat").

It is possible to distinguish between:

❑ Personalised addresses

The address directly contains information about its owner: name and surname, initials, post, identification number, and so on.

✓ Name_Surname_@domain_name
joanidentitat@gencat.cat

✓ Initials_@domain_name
E.C@gencat.cat

✓ Post@domain_name
Directoraautoritat@gencat.cat

✓ Identification number@domain_name
000000000857346@gencat.cat

In these cases, the email address directly identifies the account holder and must therefore be considered personal data.

The allocation of this type of email address can generate false expectations of privacy in both its holder as well as in the people with whom he or she communicates. Consequently, in cases where the use of email for personal matters is to be strictly prohibited, it may be better not to allocate personalised addresses.

❑ Non-personalised addresses

Although the address is linked to the email account of a specific individual, it does not appear to contain information about the account holder (it employs an alphanumerical combination which is abstract or has no particular significance):

Akatombe80@gmail.com

Abc123@terra.net

In these cases, the address in itself does not identify the person who is its holder. It can make them easily identifiable however without too much effort, either because the address may appear together with other details that enable such identification, or due to the content of the message, or through the data held by the server. This type of address must also be considered personal information.

❑ Generic addresses

The email address corresponds to a generic account with shared use or pertaining to a certain area of the organisation:

enquiries@gencat.cat

In these cases, the email address cannot be linked to an identifiable individual, and may be attended to by various different users. It is not, therefore, considered personal data. The expectations of privacy disappear with an address of this type, both on the part of the employee as well as and especially on that of people who communicate with it, given that it can be employed by multiple users.

2.2 Publication of the email address on the Internet/Intranet as contact information

Publication of a work or professional email address which can be associated with an individual or individuals constitutes the communication of personal information and must therefore be subject to the rules governing communications provided for in data protection legislation. This means that the employee's consent must be obtained for such communication or it must be authorised by a regulation with the status of law.

Where publication of the work or professional email address is necessary as part of the functions entailed in a certain post, such publication must be deemed covered by Articles 6.2 and 11.2.c) of the Law on the Protection of Personal Data (LOPD) and Article 2.2 of the Regulation implementing that law (RLOPD).

However, in the case of lists of persons belonging to professional associations, which are considered sources with public access according to Articles 3.j) of the LOPD and 7 of the RLOPD, the email address which forms part of the details included in that source may be processed to satisfy the legitimate interest pursued by the data controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised (Art. 6.2 LOPD).

Recommendations

- ✓ Wherever possible, establish email accounts linked to procedures, services or areas of activity, rather than to specific persons. This is especially recommendable when email accounts are issued to employees of external organisations that provide services in the company on a regular basis.
- ✓ Limit the dissemination of employees' email addresses to those cases in which it is necessary for the functions attributed to each of them. In other cases, publish the address only on the Intranet.
- ✓ Include a reminder of admissible uses of email addresses in the place where these addresses are published.
- ✓ Incorporate mechanisms to avoid the indexing of email addresses when they are published on the website, to avoid their being used for bulk emailing (spam) campaigns. In this regard, it may be advisable to avoid including the email address in the website presentation page. Instead, establish a link providing access to a page which includes an anti-indexing instruction and contains the email address. This will enable the indexing of the homepage content without also indexing the address.
- ✓ Do not use email addresses that form part of the corporate directory or give them to third-party persons for purposes other than those which are necessary for the company to carry out its functions and activities.

3 Email content

An email contains various pieces of information that may be considered personal data inasmuch as they provide knowledge of an identifiable person:

- ❑ Email address of the sender and recipient or recipients

  The email address can easily be linked to a natural person. On occasions, the address itself facilitates such identification. In other cases, identification of the person who is its owner appears in the address field, together with it or even replacing it.

- ❑ Subject line of the email

  The subject line should describe the nature or content of the message concisely and, if possible, without including personal details.

  The confidentiality level of data included here will be lower than that of information contained in the message body, as simply viewing the inbox or outbox enables the subject to be read.

- ❑ Date and time of the email

  The date and time of the email also constitute personal data, since they allow us to establish the very moment it was sent and can even enable us to know where the sender was at that time.

- ❑ Message body

  The body contains the content of the message, which can consist in formatted or unformatted text, or in images, which may include personal data. It may also contain links to websites or documents that contain personal information.

- ❑ Signature footer

  This is the text that appears underneath the identification of the writer. It usually offers information about the sender's post and the organisation to which he or she belongs.

  Email systems usually provide the option of automatically including a signature footer in messages.

- ❑ Attachments

  Email systems enable users to attach images, documents, videos and audio to the message. The volume of personal information these attachments can include is extremely high, so great care must be taken to avoid improper disclosures when attaching files. Moreover, the security of these data must be ensured and, if necessary, the use of technical measures such as encryption should be considered to guarantee the content will not be intercepted by third parties.

II. The use of email

1 Rules for the use of email

To avoid the improper use of email which could compromise the security of the information involved, the company must establish rules for its use and make them known to employees. It should also define the conditions in which, if necessary, the company email system may be employed for private purposes.

The rules should contribute to establishment of an email use policy which enables employees to be sure about the level of confidentiality they can expect when using these technologies. In contrast, the lack of such a policy may lead to employees or third-party persons forming confidentiality expectations that give rise to conflictive situations.

Wherever possible, employees' representatives should participate in the drafting of these rules.

Staff must be informed of the existence of the rules. As well as publication on the company intranet, to ensure all employees know about them they could be included as an appendix to the employment contract, form part of the Staff Handbook for new employees or be sent to them as circulars or instructions.

In addition to their participation in drafting the initial set of rules, employees' representatives should be informed of any additions or modifications that may be approved.

The company must train its employees in the use of email and, especially, in application of the privacy options offered by the system it employs.

Email-use rules must be updated in line with the evolution of available technology, company activity and employee needs.

At the very least, these rules should address the following aspects:

- ❑ Object and purpose of the document.
- ❑ Specifications of the email system (equipment and programs).
- ❑ General instructions for the use of email.
- ❑ Allowed and prohibited uses of the professional email address and, where applicable, of the personal email address facilitated by the company. In the event that a certain amount of private use is permitted, the circumstances in which this is possible should be established (amount of use for private purposes, identification of private messages, their storage, elimination of the signature footer on private emails, etc.).
- ❑ Allowed uses of the mediums and mobile or portable devices facilitated by the company which enable email access.

- ❑ Possibility of employing webmail systems in the workplace, be it for professional or strictly personal purposes, or of receiving messages from other accounts in that of the company.
- ❑ Aspects related to the message content: header, formal aspects, language, legal warnings, signature footers, maximum file size, and so on.
- ❑ Allowed uses of the addresses published in the company directory.
- ❑ Applicable security measures:
  - Measures for user identification and authentication: password policy and assignment.
  - Measures that employees must adopt to ensure confidentiality of the information and, where applicable, professional secrecy.
  - Procedure for authorising data transmission via the Internet.
  - Use of the digital signature and encryption mechanisms.
  - Protocol to be followed by employees and by the company itself should an incident occur in the use of email.
  - Other security measures.
- ❑ Length of time information is kept in the inbox, sent mail file and bin in email client systems.
- ❑ Information which must be conserved for a longer period and centralised or, for instance, saved on back-up copies, for technical management of the network or "log" files.
- ❑ Solutions to ensure the continuity of activity in the event of the employee's absence, with special reference to automatic response messages.
- ❑ How inappropriate received emails should be treated.
- ❑ Email supervision measures that the company can employ:
  - Filter mechanisms.
  - Programs and devices for supervision and monitoring, if they are justified.
  - Circumstances and procedures for access by the company to email accounts.
- ❑ Consequences for the employee in the event of improper use of email.
- ❑ Other rules addressed to employees for the proper use of email, and rules of general behaviour on the net or *netiquette*. In this respect, the Authority has also published the *Manual on the Proper Use of Email*, aimed specifically at employees who use email systems.

A sample set of rules for the use of email in the workplace may be found in the Appendix I to this Recommendation. It is intended to assist companies in drafting their own set of standards, which should be tailored to each organisation's particular needs as regards the processing of information.

2 Identification and authentication mechanisms

❑ Identification

Procedure to establish a user's identity, in this case that of the email user. A name is assigned to each user for this purpose.

❑ Authentication

Procedure to confirm a user's identity. In an email system this is normally done through the introduction of a password in addition to the user's identification, though other methods can also be used, such as a digital certificate.

❑ Password

Confidential information made up of a chain of characters. The strength of the password depends on the characteristics required for its establishment (password policy). A password can be considered strong if:

- It contains at least 8 characters.
- It has been chosen at random and cannot be found in any dictionary.
- It can only be deduced by its user.
- Inordinate effort is needed to ascertain it.
- It includes letters, numbers, upper and lower case and, if permitted by the system, symbols.

In contrast, a password should be considered weak if:

- It easily identifies the user.
- It contains fewer than 8 characters.
- It is predetermined by the system or the system administrator.
- It is easily identifiable using dictionaries, or consists in proper names, significant dates, familiar numbers or simple variations of words.

In the event of a user forgetting the password, some programs enable it to be retrieved or modified by answering a question established by the same user. Password strength also depends on the complexity of the reply to that question.

In order to guarantee the unmistakeable and personalised identification of any user, the company should establish an appropriate policy on passwords in the rules for the use of email.

Recommendations

- ✓ Establish a mechanism for email account access that guarantees the unmistakeable and personalised identification of any user and its authentication by means of a strong password.
- ✓ Do not create users who are identified by the email address, since this will facilitate the user's identity and provide a third party with the possibility of blocking the account.
- ✓ Use an unintelligible system to store usernames and passwords, or at least the passwords, employing encryption techniques.

- ✓ Maintain the confidentiality of the assigned username and password when these are first communicated to the user.
- ✓ Avoid risks when processing passwords in the email server by employing secure transmission systems, such as encryption.
- ✓ Establish the regularity with which the password should be modified, which should never be more than a year.
- ✓ When the periodical change in password is made, do not allow previous passwords to be repeated.
- ✓ Expressly prohibit the unauthorised use of other users' email addresses by means of user exchange or shared users.
- ✓ Install blocking systems in the computer which can be easily activated in the event of absence from the keyboard, or which oblige the user to reintroduce the password following a determined period of inactivity.
- ✓ Inform users of the following:
  - Their obligations in relation to the preservation of passwords and the frequency of their modification.
  - The personal and non-transferable nature of usernames and passwords.
  - The liability they can incur in the event of loss, fraudulent alteration or impersonation in authentication systems.
- ✓ Establish an appropriate protocol for the withdrawal of access permission when an employee leaves the organisation.

3 Communications security

The use of email does not in itself ensure the authenticity or integrity of the communication. In other words, it does not guarantee the identity of the person who appears as the sender or that the content sent coincides with the content received. This can produce problems both in respect of impersonation (identity spoofing), as well as regarding the alteration of messages and attached files.

The digital signature is one way of guaranteeing the authenticity and integrity of communications.

❑ Digital signature

The digital signature is an integrated set of electronic data, linked and logically associated with other electronic data, which can be used by the signatory as their means of identification through a system of asymmetric cryptography. This mechanism authenticates the identity of the sender and the integrity of the message.

The digital signature can be generated on the basis of a digital certificate, or document signed electronically by a certification service provider, which links signature verification data to a signatory and confirms their identity.

Every administration, with the collaboration if necessary of the Catalan Certification Agency (CATCERT), must provide its staff with digital signature systems which will identify post-holders or their position and the administration in which they work.

The Catalan Data Protection Authority website offers information about how to use the digital signature in different email systems.

Furthermore, the confidentiality of the information transmitted must also be taken into account by ensuring that it is accessed solely by the persons it is intended for.

❑ Encryption

Encryption can be employed to guarantee the confidentiality of communications.

This consists in the transformation of a message using a code which makes it unreadable by anyone who does not have the decryption key.

The use of data encryption mechanisms or any other method which guarantees that the information is not intelligible or manipulated by third parties is compulsory in the transmission of personal data over public networks or via wireless electronic data communication systems, when processing requires the application of high-level security measures:

- Personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin, health or sex life.
- Data obtained for police purposes without the consent of the data subjects.
- Data derived from acts of gender violence.

Information on how to use encryption in different email systems may be found on the Catalan Data Protection Authority website.

The email system must ensure the security of the information for which it is being used. In this sense, it should be remembered that the sending of personal information by email, be it in the message body or in attachments, must be duly authorised by the data controller or in the security document.

Users should also be aware that certain websites and emails can contain web bugs (small embedded images that provide information about our IP address and email access), or invisible hyperlinks that allow our email address to be transmitted to a third party.

The protocol in the company's rules for the use of email must establish mechanisms for employees who detect some kind of incident or have doubts about the system's security to communicate their concerns immediately to the person responsible for security. Such notification should include a brief description of the incident and the date and time it was detected, so that it can be resolved and/or the email operating system checked.

Recommendations

- ✓ Establish a default security configuration in email equipment and programs appropriate to the nature of the most sensitive data it is anticipated they will process.
- ✓ Always protect access to the mailbox with a system that guarantees identification and authentication, especially when using mobile devices.
- ✓ Protect the content of messages by pointing computer monitors away from the view of third-party persons who may be visiting the workplace.
- ✓ Configure mobile devices to become automatically blocked, so that if they are lost nobody else can gain access to the email messages they contain.
- ✓ Prohibit the installation of software not authorised by the company.
- ✓ Install an antivirus program, anti-spam filters and other mechanisms to reduce the receipt of unsolicited messages.
- ✓ Require the provider to ensure that communication between the mail access device and the server is encrypted.
- ✓ Demand that messages which may contain a virus or malware are eliminated immediately. Complete elimination also requires their removal from the recycle bin.
- ✓ Establish an adequate process for the resolution of any security issue that may be detected in the system.
- ✓ Include instructions on digital signatures and message encryption in the rules for the use of email.
- ✓ Train staff in the use of digital signatures and message encryption.

4 Use of email for private purposes

The work involved in many posts makes the allocation of an email account essential. It can often prove difficult however to completely separate employees' private lives from their professional activity. This is not always the fault of the employee, but can also be due to the needs of the company itself. Moreover, account holders do not always have control over the messages that arrive in their inbox. This is especially evident in the case of mobile devices and remote access systems established, precisely, to enable these mediums to be used outside the workplace and working hours.

It is therefore possible to distinguish different types of email account, according to their purpose:

- ❑ Corporate account for professional use: such accounts are owned by the company or institution in which the employee works. The company chooses the user, the provider and the domain, and also defines the purposes and conditions of use to which the account will be subjected. The allocation of this type of email account is made for strictly employment-related reasons.
- ❑ Corporate account for personal use: the company may allocate an email account to an employee strictly for his or her personal use. Such use may be limited, but the email content may not be monitored.
- ❑ Private or personal account: these accounts are provided by a service provider, either free of charge or in exchange for payment, or by the company or institution in which the employee works. This type of account is for strictly personal use.

An email address qualified as a corporate or work account is allocated strictly for employment-related reasons. Nonetheless and as mentioned above, since in many cases it is difficult to separate private and personal life there is a certain degree of acceptance regarding the possibility of using these mediums for personal purposes, except when the company expressly establishes otherwise.

It is advisable however for the company to stipulate in its rules for the use of email whether the private use of this medium is acceptable, and to what extent (times, volume of messages sent or received, etc.).

When the use of email for personal purposes is accepted, the employee's conscientious behaviour will ensure respect for his or her own privacy. In this regard, it is essential that dissemination of the professional email address is limited to strictly professional purposes, that messages are properly configured and organised, and that a regular check is made of those which should be deleted.

On the other hand, in order to make prohibition on personal use of the professional email address compatible with the private life of individuals, when circumstances so warrant it may be advisable to allocate not only a corporate or professional account, but also another for private or personal use. This will avoid, or at least reduce, one same address being employed for different purposes. The allocation of such an account can be replaced by authorisation to use a webmail system, with the limitations the company chooses to establish.

Where necessary, other persons who may reasonably be expected to come into contact with the email system should be informed of the exclusively professional nature of email addresses (e.g. through inclusion of a warning in all messages leaving the organisation, or in the corporate directory).

In any event, the allocation of an email address which does not include data linked to a specific person may help third-party persons to be aware of the exclusively professional nature of the email account.

When, in the case of absence, continuity of the service requires redirecting messages that arrive into the absentee's account to the address of another employee, the former should be advised in good time to enable him or her to adopt the corresponding measures and, if necessary, inform his or her contacts of the new situation.

Recommendations

- ✓ The rules for email use should establish whether employees can use the professional email account for personal purposes.
- ✓ Accept the use in the workplace of a system of web access to email for private purposes, established by the individual employee and with the limitations determined in the company's rules for the use of email.

In the event of allowing use of the professional email account for personal purposes:

Recommendations

- ✓ Establish a maximum time for the conservation of private messages in the company's rules for the use of email. On expiry of this period, employees must delete all unnecessary messages or those they have resent to a private email address and that remain in the system.
- ✓ Establish the rules for use outside working hours of mobile devices with access to email, such as smartphones and laptops.
- ✓ Create files in which to store emails identified as "private" or "personal". This can be done automatically by means of filters based on the message origin or the inclusion of these words or others in the message subject line, or manually on the basis of decisions made by the account holder.

5 Use of email for trade-union purposes

Freedom of information is an essential element in the fundamental right to freedom of association. Though employment legislation does not expressly provide for the technological means that the company makes available to employees to be used in the exercise of this right, trade union representatives may employ the company ICT resources for such purpose, provided this does not affect the normal course of business activity.

There is no specific legal provision covering the transmission of trade-union information to employees, be they members or not, via a company-provided email system. Nonetheless, if the company has such a system, workers' representatives may use it to send union information to their members and other company employees, in accordance with the company's rules for the use of email.

However, pursuant to established constitutional doctrine, this use by union representatives of a company-provided email system is subject to a series of limitations:

- The use of email for such purposes cannot be excluded in absolute terms.
- Such communication must not interfere with the company's normal business activity.
- This use may not result in charges or additional costs for the company.

Union representatives may, to the same end, also use the addresses that appear in the company directory, without the consent of the data subjects.

Employees may however exercise their right to opposition to the use of their email address for this purpose, by notifying the data controller.

Recommendations

- ✓ Authorise use of the email system as an instrument of communication and information between unions and workers, providing the activity and general characteristics of the company so allow, ensuring the inviolability of the communications in accordance with the applicable legal framework. However, an assessment should be made of the possibility of disseminating union information among employees by some means which eliminates the need to employ their email data, such as:
- ✓ Employing mailing lists that enable the union to send information without having access to such data.
- ✓ Making a union information window available to workers in the corporate intranet.
- ✓ Establish a simple procedure for employees to exercise the right to opposition to the use of their email address for this purpose against the union and/or data controller.
- ✓ If they have not already been informed, tell workers of the possibility of exercising this right when the data are given to the union representatives. Such notification will be without detriment to the union representative also duly informing the said workers.

III. Access to the email account by the company

The considerations contained in this section do not refer only to the email accounts in which the company's rules for use allow a certain amount of personal activity. They also concern those accounts for which exclusively professional use has been established, since irrespective of their own actions, employees cannot always avoid receiving personal messages from third-party persons.

The company may only access corporate email accounts allocated to their employees when this is justified and there is no other mechanism available which enables the objective to be achieved without resorting to such access.

The means and scope of control must be proportionate to the purpose pursued. Thus, wherever possible, it must be limited to details of the sender and recipient, the time and date of the communication and other data such as the number of messages sent, the volume of information or type of files attached, or other systems of automated analysis of received and sent messages which do not analyse content. Only if this information is insufficient to attain the pursued goal may the email content be accessed, providing the relevant guarantees are respected and avoiding opening messages that can be identified as personal. In the event that a message of this type is opened by mistake, it must be closed as soon as its private nature becomes evident.

This access must be carried out in accordance with the rules for the use of email approved by the company, which should provide information on the mechanisms employed for monitoring the use of technologies which may affect individuals' privacy, the consequences that may derive from such monitoring and the guarantees offered to employees, in particular the right to be informed.

The system administrator and other persons who intervene in monitoring operations must be informed of their duties and obligations as regards security and, especially, the duty of secrecy. Without prejudice to the general obligation of confidentiality that derives from the legislation on data protection, it may be advisable to have the persons who take part in these operations sign a confidentiality agreement regarding the data to which they have access.

All access carried out in any of the circumstances described above must be duly reflected in the incident register.

Employees may exercise their rights of access, rectification, cancellation or objection with respect to any information the company obtains through the monitoring measures adopted.

Access must be limited to the information which is essential to achieve any of the following objectives:

1 Access to carry out maintenance of the email system

Access to corporate email accounts for the tasks of maintenance, technical support or system security must not entail access to the content of messages. It may be undertaken, taking into account:

- ❑ These operations may only be performed by staff authorised by the person responsible for security.
- ❑ Affected employees must be informed of the tasks to be carried out and the persons who will conduct them, as well as the possibility of their being present during the access operation.
- ❑ Once the maintenance or technical support tasks are completed, a report must be drafted specifying what has been done. If an anomaly has been detected it must be noted in the incident register and the competent body informed.

2 Access to ensure the continuity of activity in the absence of the corresponding employee (holidays, illness, etc.)

The absence of an employee, especially if long-term, may entail problems for the continuity of the company's normal activity if a certain email account cannot be accessed. Thus, where possible, measures should be in place which will be adopted to ensure continuity during the absence (e.g. the employee may delete or transfer all personal messages and authorise access by a colleague, adopting the appropriate changes, both at the beginning and the end of the absence, with regard to passwords).

If this is not possible, the following should be taken into account:

- ❑ The absent employee's superior must make a reasoned appraisal of the need to intervene to ensure the continuity of service.
- ❑ The employee must be informed in good time of the access to their email account. If this is not possible beforehand it must be done as soon as possible after the event.
- ❑ Access should be made under the supervision of the employee's superior and, if it has been possible to inform him or her, of the same employee or the person he or she designates, should the said employee choose to exercise this option.
- ❑ Absence of an employee is not sufficient reason to justify access to messages which can be clearly identified as private or personal.

3 Access when there are indications of possible misuse

The company may monitor email traffic (number of messages and their volume, attachments, etc.) for security reasons, without gaining access to analyse the content. This monitoring may be systematic or random, but in no case may it be discriminatory.

Should there exist indications of misuse of the email system by the employee through non-compliance with the rules approved by the company, said employee must be informed of same, except if doing so might hinder the corresponding investigations. If the misuse constitutes a crime or misdemeanour it must be reported to the Public Prosecutor's Office. Any of these circumstances may give rise to the opening of a classified information-investigative file or disciplinary proceedings in which measures may be adopted to resolve the problem, which may include blocking the messages in the email account.

In the case of such access, which must be proportionate to the type of risk that could derive for the company or third-party persons from the misuse, the following should be taken into account:

- ❑ Access must be conducted by the person designated by the head of security and in the presence of the employee or, if this is not possible, of the employees' representative and the investigating official or inspector.
- ❑ Once access has been made to the account a report must be drawn up specifying the action taken and results obtained. Where applicable, this report must be integrated into the corresponding disciplinary file.

4 Termination of the employee's relationship with company

When an employee ceases to provide services to the company, the competent body in the field of human resources management must immediately inform the head of security so that the corresponding username and password can be cancelled. If necessary, an automatic response message can be established for incoming mail indicating the new address to which professional correspondence should be addressed.

The company must enable the employee to obtain personal messages from the email account, providing they do not exceed the maximum period of conservation for messages of this nature established in the rules for the use of email. Messages must be accessed in the presence of the employee, in order to identify those of an exclusively personal nature.

Once the period granted to the employee has elapsed without the said employee declaring his or her intention to remove or destroy the personal messages in the account, these may be deleted or transferred to another email address.

In the event of the employee's death, personal messages may be deleted or maintained, duly blocked, should the circumstances so warrant.