Focus on professional messaging at work

A professional messaging system has now become an essential tool for employees to carry out their work duties.

However, the widespread use of this type of electronic communication device does not absolve employers from complying with the provisions on the protection of personal data, and although they may, in certain cases, decide to control or monitor the use of the messaging system made available to their employees, particularly for security reasons, they are also bound by the obligation to respect employees' private lives.

What about privacy employee?

In the Principality, in accordance with article 22 of the Constitution, « *Everyone has the right to respect for his private and family life and to the confidentiality of his correspondence* ».

Similarly, in the *Niemietz v Germany* ruling of December 16, 1992, the European Court of Human Rights (ECHR) enshrined the right to privacy in the workplace on the basis of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, which states that *« Everyone has the right to respect for his private and family life, his home and his correspondence* ».

A few years later, the same Court clarified the conditions under which an employer may consult an employee's electronic communications in its 2017 *Bărbulescu v. Romania* ruling.

In this case, an employee who had communicated with his family from his workstation, on an email account intended for professional use, had been dismissed, on the grounds that he had failed to comply with the internal rules prohibiting the use of company resources for personal purposes.

However, the Court held that the dismissal was contrary to the right to protection of privacy enshrined in Article 8 of the Convention, since while the employer is entitled to monitor its employee's electronic communications, the extent of the monitoring and the degree of intrusion into the employee's private life must not be disproportionate to the aim pursued.

In addition, it is up to the courts to check that access to the content of communications was only put in place because there were no less intrusive measures available, and to ensure that the consequences of the surveillance for the employee are not disproportionate to the aim pursued.

For what purposes can an employer set up a professional messaging system?

Personal data may be collected for **several purposes**, provided that these purposes are:

- **determined**;
- **explicit**;
- **legitimate**; and
- **not further processed** in a manner incompatible with these purposes

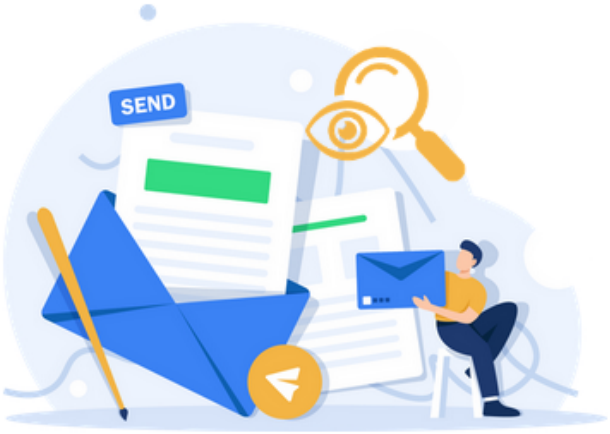
By virtue of this principle of **purpose limitation**, the APDP considers that the implementation of a professional messaging system can meet the following objectives:

- exchanging electronic messages internally or externally;
- keeping a record of incoming and outgoing electronic messages;
- managing e-mail contacts;
- managing e-mail folders and archived messages;
- creating and reading log files;
- managing e-mail access authorizations;
- managing the agenda;
- establishing evidence in the event of a dispute with a customer/employee (if an order is contested, etc.).

In addition, when surveillance is implemented in the workplace, professional messaging may also be used for the following purposes:

- the implementation of a graduated monitoring procedure;
- the monitoring of incoming or outgoing electronic messages using analysis software.

What about the notion of surveillance or control?
An employer may decide to monitor or supervise the use of the professional messaging system made available to its employees. In this respect, the APDP considers that the concept of monitoring or surveillance of electronic messaging is « *any activity which, carried out by means of software for analyzing the content of incoming and/or outgoing electronic messages, consists of the observation, collection or recording, on a* non-occasional *basis, of the personal data of one or more persons, relating to movements, communications or the use of electronic messaging* ».



What justification is needed for the implementation of a professional messaging system ?

To be lawful, automated processing of personal data must meet at least one of the requirements set out in Article 5 of Law no. 1.565 of December 3, 2024.

The APDP thus considers that the implementation of an authorization management system can be justified by:

- ***Compliance with the data controller's legal obligations***

Certain data controllers are subject to specific obligations of **vigilance** and **traceability of transactions**. For banking or similar institutions, such obligations are set out in the following texts, among others:

- Law no. 1.338 of September 7, 2007 on financial activities and its implementing Sovereign Order;
- Law no. 1.362 of August 3, 2009 on the fight against money laundering, terrorist financing and corruption and its implementing Sovereign Order;
- Law no. 1.314 of June 29, 2006 relating to the carrying on of business as a custodian or administrator of financial instruments;
- Ministerial Order no. 2012-199 of April 5, 2012 relating to the professional obligations of credit institutions acting as custody account-keepers for financial instruments.

The APDP believes that in order to comply with their obligations, these data controllers or their representatives may implement procedures for monitoring or controlling IT authorizations, in strict compliance with the principles defined by Law no. 1.565 of December 3, 2024, in particular the principles of **proportionality** and **transparency**.

➢ ***The fulfilment of a legitimate interest pursued by the data controller or a third party***

The APDP considers that a procedure for monitoring or controlling professional messaging systems may also be justified by a **legitimate interest** of the data controller or a third party, such as:

- the optimization of the performance of its employees' work assignments;
- the security and proper technical operation of the computer network or system;
- monitoring compliance with internal rules on the use of electronic communication tools, internal regulations, etc.;
- the protection of the economic, commercial or financial interests of the data controller or its representative;
- the protection against any act likely to give rise to civil or criminal liability, or to prejudice it;
- the prevention of unlawful acts.

The latter justification is the one most often used by data controllers. However, they have to strike the **right balance** between apparently contradictory, but nonetheless reconcilable, interests: on the one hand, their prerogatives as an employer, and on the other, their employees' right to privacy and secrecy of correspondence.

In view of the existence of a **subordinate or contractual relationship** between the employer and the employee, the latter's consent cannot constitute justification for the implementation of this type of processing.

What safeguards should be put in place to respect employees' privacy?

For the APDP, respect for the confidentiality of private correspondence in the workplace is an **intangible** principle. Accordingly, employers may not access the content of private messages sent or received by their employees via their work e-mail system unless the employee is present and expressly agrees.

However, for messages to be considered personal, employees must identify them as such, for example:

- by specifying key words such as « ***private*** », « ***[PRV]*** » or « ***personal*** » in the subject line of the message;
- by including a reference in the subject line of the message that clearly implies that the message is private, such as « *holiday in Japan* »;
- by storing messages in a folder entitled « *personal* » or « *private* ».

The APDP therefore considers the practice of an employer receiving all messages sent or received by its employees to be excessive, since this practice does not make it possible to distinguish between the employees' professional and personal messages.

Furthermore, only a judge's authorization can allow the employer to lawfully access the private messages of its employees when the latter have not authorized the employer to read their private messages, even if the employer has legitimate grounds to suspect acts of unfair competition or any other infringement of its interests or of the law. This may take the form of a court order instructing a bailiff to access or even record the private messages in question.

What information may be collected?

In accordance with the provisions of Article 4 of Law no. 1.565 of December 3, 2024, the collected personal data must be "*adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed* ".

The APDP therefore considers that only the following personal data may be collected and processed:

- Data common to all messaging systems :

- identity : surname ; first name, identifier;
- messages : date, time, sender/recipient information, content, subject ;
- contact management : surname, first name, company name, (…) ;
- electronic identification data : e-mail address ;
- access logging : connection logs for staff authorized to access the system ;
- log files : date and time of message, number of incoming and outgoing messages, messages cleaned, spam ; volume, format, attachments, domain names of message senders, (…).

- Data specific to messaging systems used for monitoring or control purposes:

- Alert management : receipt of automatic alerts based on the hierarchical levels concerned.

How long can data collected and processed by a professional messaging system be kept?

The personal data collected **cannot be kept indefinitely** in a form that allows the data subjects to be identified.

The APDP therefore asks employers to provide for the following data retention periods:

- **With regard to the administration of the messaging system (identity, contact management, electronic identification data)**: **a maximum** of 3 months after the user's definitive departure.

In this respect, the APDP points out that when a user leaves the company for good, their mailbox must be « ***blocked*** » immediately, i.e. they must no longer be able to receive or send e-mails, with the exception of an automatic message which will be sent to each person who has sent an e-mail to the address concerned.

The purpose of this automatic message is to inform the sender of the e-mail that the person to whom it was sent no longer works within the entity, and that from now on they should send their e-mails to such and such an address. This can be done for a maximum of 3 months, depending on the duties and degree of responsibility of the former employee.

At the end of this maximum three-month period, the former employee's nominative e-mail address will be deactivated (deleted).

The employer must, however, allow the employee to retrieve any private e-mails that may be in his or her nominative professional e-mail box.

- **With regard to the content of messages sent and received:**

The APDP recognizes that employees' electronic messages may be kept for several years, particularly in the case of banking and similar establishments, for the purposes of tracing financial transactions, or in the event of suspicions of illicit activities.

It therefore requests that messages be regularly sorted and that an archiving policy be put in place until it is no longer necessary to keep them.

- **With regard to access logs and log files:** maximum 1 year, depending on the activity carried out.

- **With regard to alerts when the messaging system is set up for surveillance purposes**: the APDP requests that these be extracted and secured (non-alterable). Data relating to an event that does not highlight an incident must then be deleted once the verification concluding that there was no incident has been carried out.

  In the event of a confirmed incident, the data must be kept **only for as long as is necessary** to carry out the associated investigation, in accordance with internal procedures and applicable legislation.

In any event, the APDP recommends, where possible, adopting a shorter retention period, once the data processed are no longer necessary to achieve the purpose(s) for which they were initially collected.

Finally, it points out that in the context of the initiation of legal proceedings, any necessary information resulting from the processing may be retained until the end of the said proceedings.

How to inform data subjects?

- ***Procedure for informing users***

Any employer must make users aware of their responsibilities with regard to the protection of their personal data.

In the interests of **transparency** towards users, as well as **fairness** in the collection and processing of personal information, the APDP therefore recommends that employers introduce a charter for the use of electronic communication tools, specifying in particular:

- the methods for identifying private messages;
- the procedure for access to the messaging system by authorized persons in the event of the user's temporary or permanent absence, in order to ensure business continuity.
-

- ***Information to third party recipients***

The APDP recommends that an information notice be inserted at the bottom of all outgoing electronic messages, informing third party recipients of the purpose of the processing and their rights.

Example of notice :
[Name of the entity to be filled in] processes your personal data in the context of exchanges via its professional electronic messaging service. The messages exchanged are kept [add retention period(s)] *To exercise your rights of access, rectification and deletion of your data, you may send an e-mail to [e-mail to be completed] or a letter to [address to be completed].* *For further information, you can consult [Link to more complete information to be added].*

Who can access the data from the messaging system?

Access to data from the messaging system must be restricted to **only those people** who, as part of their job(s), can **legitimately be aware of them in view of the objectives of the system**.

In addition to employees, who have full rights to their own email, other internal departments may also have access to information in a professional messaging system, such as agents authorized by account holders (by delegation), teams in charge of alerts or system administrators.

Similarly, an IT service provider may also have full rights to a professional messaging system for maintenance purposes.

In this case, the APDP points out that access rights must be limited to **what is strictly necessary for the performance of the service contract.** What's more, this service provider is subject to the same security and confidentiality obligations as those imposed on the data controller.

Arrangements in the event of employee absence
In order to ensure the continuity of the company's business during an employee's absence (leave, illness, etc.), the APDP considers that the employer can access the employee's professional messages using one of the following methods: • setting up an automatic response to the sender when the employee is absent, with an indication of who to contact in an emergency; • appointing a deputy with personalized access rights to his or her colleague's mailbox; • transferring all incoming messages to a deputy. In the latter two cases, however, the employee must be informed of the identity of his or her deputy and the deputy must not read messages identified as private or personal.

The APDP also considers that the communication of data to the Police Department (Direction de la Sûreté Publique) may be justified for the purposes of a judicial investigation.

In this respect, it points out that in the event of transmission, the aforementioned department may only have access to the information within the strict framework of its legally conferred missions.

Finally, the APDP considers that the Monegasque Financial Security Authority (Autorité Monégasque de Sécurité Financière or AMSF) and the Financial Activities Supervisory Commission (Commission de Contrôle des Activités Financières or CCAF) may, within the exclusive framework of the missions conferred upon them, be recipients of processed personal data.

What security measures should be put in place?

The APDP points out that the technical and organizational measures put in place to ensure the security and confidentiality of the processing with regard to the risks presented by the latter and the nature of the data to be protected must be maintained and updated, taking into account the state of the art, in order to maintain the high level of reliability expected throughout the period of operation of the processing.

Passwords must be **strong and regularly renewed**.

Remote access to professional messaging must be **secure**.

The employer must also regularly **make users aware** of e-mail security (for example: never open attachments from unknown senders, never click on hyperlinks in e-mails, never send sensitive or important data by unsecured email).