

BOARD DECISION

From the Personal Data Protection Authority:

**PRINCIPLE DECISION ON THE PROCEDURES AND PRINCIPLES TO BE
OBSERVED IN PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT BY
MONITORING COMMUNICATION CHANNELS USED FOR THE CONDUCT OF
BUSINESS, PARTICULARLY CORPORATE E-MAIL ACCOUNTS ALLOCATED TO
EMPLOYEES BY EMPLOYERS**

Decision No: 2026/2035

Decision Date: 16/09/2026

As is known, paragraph six of Article 15 of Law No. 6698 on the Protection of Personal Data (“Law No. 6698”) provides that “*Where, as a result of an examination carried out upon a complaint or ex officio, it is established that the violation is widespread, the Board shall adopt a principle decision on the matter and publish such decision...*”. Furthermore, subparagraphs (e), (f) and (g) of paragraph one of Article 22 of Law No. 6698, which governs the duties and powers of the Personal Data Protection Board (the “Board”), respectively vest the Board with the power to carry out regulatory actions on matters relating to the Board’s field of duty and the functioning of the Authority, for the purpose of determining obligations relating to data security, and in relation to the duties, powers and responsibilities of data controllers and their representatives.

Within this framework, the Board has made the following findings and assessments with respect to personal data processing activities carried out by monitoring communication channels used for the conduct of business, particularly corporate e-mail accounts allocated to employees by employers.

A corporate e-mail account allocated to an employee is, beyond being a means of communication, a data source containing the employee’s professional and, at times, personal network of relationships, working patterns and the content of correspondence. The monitoring of such accounts by the employer is a personal data processing activity that requires a balance to be struck between the employer’s managerial prerogative and the employee’s right to request the protection of personal data and freedom of communication, as safeguarded under Articles 20 and 22 of the Constitution. Moreover, communication channels used in the workplace are not limited to corporate e-mail accounts. In-house messaging applications, corporate instant messaging accounts, customer relationship or request management systems, and the chat and recording features of meeting platforms are also among the communication channels that may be subject to monitoring, depending on the circumstances of the specific case. Furthermore, with respect to applications that also lend themselves to personal use, whether the account in question has been allocated by the employer for business purposes,

whether it is used through the employee's personal account, and the employee's reasonable expectation of privacy must be assessed separately.

Even where the employer processes only the traffic/log records without accessing the content of the employee's e-mail, this in itself constitutes a personal data processing activity. Therefore, e-mail monitoring, whether directed at traffic data or at content, is subject to the general principles set out in Article 4, the processing conditions set out in Articles 5 and 6, the obligation to inform set out in Article 10 and the data security obligations set out in Article 12 of Law No. 6698.

The fact that communication tools belong to the employer or are located at the workplace does not, in itself, confer upon the employer an unlimited and absolute power of monitoring. Indeed, the decisions of both the Constitutional Court and the European Court of Human Rights on the matter establish that the employer's power of monitoring is subject to the criteria of the employee having been clearly informed in advance, the monitoring being based on a legitimate aim and being limited and proportionate to that aim, and less intrusive means being given priority; and that the monitoring of content requires a weightier justification than the monitoring of traffic data.

Within this framework, with respect to personal data processing activities carried out by monitoring communication channels used for the conduct of business, particularly corporate e-mail accounts allocated to employees by employers:

1. The monitoring of corporate e-mail accounts constitutes, in itself, a personal data processing activity even where only traffic/log records are processed without accessing content, and is in any event subject to the processing conditions, the general principles and the obligations to inform and to ensure data security under Law No. 6698; and the fact that communication tools belong to the employer or are used at the workplace does not confer upon the employer an unlimited power of monitoring;
2. In determining the scope of the monitoring activity, the distinction between "business use" and "private use" must be taken into account according to the purpose for which workplace communication tools are used; and whether the employer has prohibited private use, permitted it within certain limits or made no explicit rule on the matter may lead to different outcomes in the assessment of the lawfulness of the monitoring;
3. Within the scope of its managerial prerogative, the employer may lay down rules on the private use of workplace communication tools; however, such rules must be clear, comprehensible and capable of being known by the employee; where private use is prohibited, restricted or made subject to specific conditions as to time, scope and method, this must be explicitly communicated to the employee; even where private use is prohibited, the employer's power of monitoring is limited by the principle of proportionality; monitoring conducted in the form of continuous and uninterrupted surveillance cannot be regarded as proportionate; where a breach of the prohibition on private use can be established from non-

content elements, additional access to the content of correspondence cannot be regarded as necessary and proportionate; where private use is permitted and business and private communications can be distinguished from each other, monitoring must be confined to business communications only and the employee's private correspondence must be excluded from monitoring; and where business use and private use cannot be distinguished from each other, the employer's power of monitoring must be interpreted more narrowly;

4. The fact that the employer has technical authority over a particular device, session, network or corporate system does not mean that it may freely access the content of correspondence held in the employee's personal e-mail account, personal instant messaging application, social media inbox or similar private communication spaces; therefore, the technical ability to access must be distinguished from the legal authority to access;

5. In assessing the lawfulness of the monitoring, the employee's having been informed in advance of the monitoring activity is one of the determining factors; nevertheless, the notification required under the case law of the Constitutional Court and the obligation to inform set out in Article 10 of Law No. 6698 are not identical concepts; not every notification may qualify as fulfilment of the obligation to inform within the meaning of Law No. 6698; however, a duly provided privacy notice that contains the elements stipulated in Article 10 of Law No. 6698 and clear information on the purpose, scope and method of the monitoring activity may also satisfy the requirement that the employee be informed of the monitoring in advance;

6. The privacy notice to be provided by the employer must go beyond an abstract and general statement and set out, in a clear, comprehensible and concrete manner, the legal ground, purpose and scope of the personal data processing activity, whether the monitoring will be conducted through the review of traffic/log records or through content monitoring, the circumstances in which content may be accessed, the retention period of the data and the rights of the data subject under Article 11 of Law No. 6698;

7. Where the employee has not been informed in advance of the monitoring activity and has not been provided with a privacy notice in accordance with Article 10 of Law No. 6698, it must be borne in mind that the employee will have a reasonable expectation that his or her personal data and freedom of communication will not be interfered with; and general statements merely indicating that the corporate e-mail account may be monitored by the employer will neither satisfy the "notification" requirement nor result in the fulfilment of the obligation to inform under Article 10 of Law No. 6698;

8. In view of the dependency inherent in the employment relationship and the imbalance of power between the parties, the employee's explicit consent should not, as a rule, be relied upon as the primary legal basis for e-mail monitoring; where explicit consent is relied upon, whether such consent was given freely must be separately assessed in light of the specific case; personal data processing activities carried out in the course of monitoring may, depending on the circumstances of the specific case, be based on the processing conditions set

out in subparagraph (ç) of paragraph (2) of Article 5 of Law No. 6698, namely “*processing of data is necessary for the data controller to fulfil its legal obligation*”, subparagraph (e), namely “*processing of data is necessary for the establishment, exercise or protection of a right*”, and subparagraph (f), namely “*processing of data is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed*”; however, the existence of such processing conditions does not confer upon the employer an unlimited power of monitoring;

9. In accordance with the general principles set out in Article 4 of Law No. 6698, monitoring must be conducted in conformity with the law and the principle of good faith, based on a specified, explicit and legitimate purpose, in a manner that is relevant, limited and proportionate to that purpose, and the data obtained must be retained only for the period required by that purpose;

10. Monitoring is governed by the principle of gradation; where the employer can achieve the legitimate aim it pursues through less intrusive means, it may not resort to a more intrusive monitoring method; access to content may come into question only in exceptional cases where monitoring of traffic data proves insufficient and access to content is necessary; and where misuse of communication tools allocated to the employee for work purposes can be prevented by technical means (filtering, blocking, etc.), no general right of monitoring arises for the employer;

11. Since monitoring of content constitutes the most intensive interference with the employee’s private life and freedom of communication, it requires a stronger and concrete legitimate justification; content monitoring may be resorted to only where there is a concrete suspicion and only to the extent limited to the allegation concerned; and content reviews that are indeterminate in scope, general and continuous in nature must be avoided;

12. In content monitoring, regard must be had to the risk of processing special categories of personal data within the meaning of Article 6 of Law No. 6698 in the body or attachments of the communication subject to monitoring; furthermore, since correspondence frequently also contains personal data of the counterparties, the impact of the monitoring on the data of third parties must also be taken into account;

13. Monitoring conducted through covert surveillance methods of which the employee has not been informed in advance, or through tools that indiscriminately record all of the employee’s activities, shall be deemed unlawful; and monitoring must be conducted with the employee’s knowledge and within a foreseeable framework;

14. Access to the data obtained through corporate e-mail accounts and communication channels used for the conduct of business must be restricted to a limited number of personnel authorised for this task; access authorisations must be determined by job descriptions; access logs must be maintained; and persons accessing the data must be bound by a duty of confidentiality;

15. Following the termination of the employment relationship, the legal basis for personal data processing activities relating to the corporate e-mail account allocated to the employee must be assessed separately; as a rule, the account concerned must be closed to the employee's active use and to new access, messages received in the account must not be made viewable by unrelated persons, and personal data for which no legal basis remains must be destroyed; nonetheless, for the purposes of ensuring business continuity, preventing the disruption of corporate communications, exercising the right of defence in legal disputes or fulfilling obligations arising from the relevant legislation, forwarding, auto-reply, archiving or retention practices relating to the corporate e-mail account that are limited, time-bound, subject to defined access authorisations and recorded may be assessed in light of the circumstances of the specific case;

16. Where non-compliance with the aforementioned obligations is established, the necessary examination shall be carried out taking into account the particulars of the specific case, and administrative action shall be taken against the relevant data controllers pursuant to Article 18 of Law No. 6698,

the Board has decided, by majority vote, to inform the public of the foregoing matters and, in this context, to adopt a Principle Decision pursuant to paragraph six of Article 15 of Law No. 6698 on the Protection of Personal Data, and to publish this Principle Decision in the Official Gazette and on the website of the Authority.