

The Turkish Data Protection Board's Principle Decision on Monitoring Employees' Corporate Communication Channels

A. Introduction

The Turkish Personal Data Protection Board (the “**Board**”), through its Principle Decision dated 16 September 2026 and numbered 2026/2035 (the “**Principle Decision**”), has set out the procedures and principles that employers must follow under the Personal Data Protection Law No. 6698 (the “**Law**”) when monitoring corporate e-mail accounts and other work-related communication channels provided to employees.

Published in the Official Gazette dated 8 October 2026 and numbered 33394, the Principle Decision clarifies how employers' right to manage and supervise their operations should be balanced against employees' right to the protection of their personal data and freedom of communication. The Principle Decision is available [here](#).

B. Legal Framework

Under Article 399 of the Turkish Code of Obligations No. 6098 (the “**TCO**”), employers may establish general rules on the performance of work and employees' conduct in the workplace and issue specific instructions to employees. This provision is one of the legal bases for employers' managerial authority, which includes the power to set rules governing the performance of work, issue orders and instructions, and supervise work processes.

In this context, employers may need to monitor communication tools used in the course of business, particularly corporate e-mail accounts, for purposes such as ensuring the efficient operation of business processes, maintaining

corporate information security, and verifying compliance with workplace rules.

However, the need for such monitoring does not mean that employers may exercise their managerial authority without limitation. Article 417 of the TCO requires employers to protect employees' personality rights, while Article 419 imposes restrictions on the use of employees' personal data.

Corporate communication tools may contain employees' personal data and private correspondence in addition to information relating to business processes. Accordingly, the fact that such tools are provided by the employer does not permit unrestricted examination of communications conducted through them. Monitoring activities must be carried out in compliance with the Law, with due regard to employees' fundamental rights and freedoms.

The monitoring of corporate e-mail accounts provided to employees has also been considered by the Turkish Constitutional Court (the “**Constitutional Court**”) in the context of the right to the protection of personal data guaranteed under Article 20 of the Constitution and freedom of communication under Article 22. In its decision dated 17 September 2020¹, the Constitutional Court found that accessing an employee's corporate e-mail correspondence without adequate prior notification constituted a violation of rights. In its decision dated 12 January 2021², however, it concluded that no violation had occurred where the rules governing the use and monitoring of the corporate e-mail account had been clearly established in advance, the examination had been confined to a specific

¹ Decision of the Turkish Constitutional Court dated 17 September 2020 (Application No. 2016/13010).

² Decision of the Turkish Constitutional Court dated 12 January 2021 (Application No. 2018/31036).

allegation, and the data obtained had been used in accordance with its intended purpose.

Similarly, in *Libert v. France*³ and *Bărbulescu v. Romania*⁴, the European Court of Human Rights (the “ECHR”) emphasised the importance of prior notification and the principle of proportionality in employer monitoring of communications.

In its decision dated 25 November 2021 and numbered 2021/1187, the Board also found that accessing a former employee’s corporate e-mail account without providing the required privacy notice was unlawful and imposed an administrative fine on the data controller.

These decisions show that employees must be informed in advance of any monitoring of corporate communication tools, that monitoring must pursue a legitimate purpose, that less intrusive means of achieving that purpose must be considered, and that a fair balance must be struck between the parties’ interests. The Principle Decision further specifies these requirements in terms of the obligations of data controllers under the Law.

C. Findings and Assessments of the Board

a) Legal Basis for Monitoring

The Board stated that, as a rule, explicit consent should not be preferred as the primary legal basis for processing personal data, given the inherent power imbalance in the employment relationship and employees’ dependence on their employers. Depending on the circumstances of the particular case, processing may be based on the legal grounds set out in Article 5(2)(ç), (e) or (f) of the Law. However, the existence of any such legal ground does not confer an unrestricted right of monitoring on the employer. Monitoring must

pursue a specific, explicit and legitimate purpose and must be relevant, limited and proportionate to that purpose.

b) Scope of Monitoring and the Principle of Proportionality

The Board emphasised that monitoring should be carried out in stages. Where the employer’s objective can be achieved through examination of access logs, technical filtering or other methods that do not require access to the contents of communications, directly examining correspondence may be contrary to the principle of proportionality.

As examining the contents of correspondence constitutes a more serious interference with employees’ freedom of communication, it may be justified only in exceptional circumstances involving a specific suspicion or need, provided that the examination is limited to the relevant allegation or purpose. In its decision dated 19 January 2023 and numbered 2023/86, the Board distinguished between the examination of traffic data and the examination of content and established that content monitoring is subject to stricter conditions. In that decision, the Board did not consider the examination of content following the identification of suspicious e-mails to be contrary to the principle of proportionality.

Accordingly, content examinations of undefined scope or conducted on a continuous basis, as well as covert monitoring activities, must also be assessed in light of the principle of proportionality. Methods such as recording employees’ keyboard and mouse movements, regularly capturing screenshots, and continuously tracking application use must be assessed in the same manner. Opinion 2/2017 of the EU Article 29 Working Party⁵ states that

³ The European Court of Human Rights, *Libert v. France* (Application No. 588/13), 2018.

⁴ Grand Chamber judgment in the case of *Bărbulescu v. Romania* (Application No. 61496/08), 2017.

⁵ Article 29 Working Party, Opinion 2/2017 on Data Processing at Work (WP249), dated 8 June 2017.

personal data processing through such technologies is disproportionate and that, in particular, recording employees' keyboard and mouse movements is extremely difficult to justify on the basis of an employer's legitimate interests.

Therefore, where employees' work activities can be monitored through less intrusive methods, continuous screenshot capture or tracking of keyboard and mouse movements may breach the principle of being relevant, limited and proportionate to the purposes of processing, as set out in Article 4(2)(ç) of the Law.

c) Obligation to Inform

The Board emphasised that monitoring must be foreseeable to employees. In this regard, a general notification stating merely that "corporate accounts may be monitored" is not sufficient on its own. Employees must be informed in advance of the purpose and legal basis of monitoring, the categories of data to be examined, whether monitoring will extend to traffic data or the contents of correspondence, the circumstances in which content may be accessed, and the applicable retention periods.

Although the requirement of prior notification considered in the Constitutional Court's case law and the obligation to inform under Article 10 of the Law have different legal bases, a comprehensive and duly provided privacy notice may help satisfy both requirements.

d) Distinction Between Business and Personal Use

The Board stated that the distinction between business and personal use is important in determining the limits of an employer's monitoring authority. Employers may prohibit or restrict personal use of corporate communication tools through internal policies. Nevertheless, such a prohibition does not permit unrestricted examination of employees' private

correspondence. In monitoring conducted for this purpose, it may be sufficient to determine whether corporate communication tools have been used for personal purposes; examining the contents of such communications may be contrary to the principle of proportionality.

e) Security of Personal Data

The Board noted that examining the contents of correspondence may also entail the processing of third parties' personal data and special categories of personal data within the meaning of Article 6 of the Law, in addition to employees' personal data. It is therefore important to keep the scope of monitoring as narrow as possible. The Board further stated that access to data obtained through monitoring must be restricted to authorised personnel, access activities must be logged, confidentiality must be maintained, and data must be retained only for as long as necessary.

f) Obligations Following Termination of Employment

The Principle Decision also addresses the management of corporate e-mail accounts allocated to former employees. Following termination of the employment relationship, corporate e-mail accounts must be closed to active use and further access, and data for which there is no longer a legal basis must be destroyed. However, measures such as automatic replies, forwarding, archiving or retention for a limited period may be assessed in light of the circumstances of the particular case where necessary to ensure business continuity, preserve corporate communications, exercise the right of defence in legal disputes or comply with statutory obligations. Finally, the Board stated that, in the event of non-compliance with these obligations, administrative action may be taken against the relevant data controllers under Article 18 of the Law.

D. Conclusion

The Principle Decision defines the limits of employers' authority to monitor corporate communication tools and gives concrete effect to the approach adopted in the Board's earlier decisions and in the case law of the Constitutional Court and the ECtHR. In this context, employers must establish rules governing the use of corporate communication tools in advance, inform employees of the scope and conditions of monitoring, and carry out

monitoring activities in accordance with the principle of proportionality.

Accordingly, monitoring should primarily rely on methods that do not require examination of content, and any examination of correspondence should be limited to specific needs. Employers should also review their internal policies governing corporate communication tools and employee privacy notices in light of the Principle Decision and establish procedures and principles for managing corporate accounts after termination of employment.

For further information and support, please contact us.



Ece Özçelik Tokmak
Senior Associate
e.ozcelik@lbfpartners.com



Büşra Karabudak
Associate
b.karabudak@lbfpartners.com