

Client Alert

Turkish Personal Data Protection Board's Principle Decision on Employee Email and Workplace Communications Monitoring



Introduction

The Turkish Personal Data Protection Board's ("**Board**") Principle Decision ("**Decision**") dated 16 September 2026 and numbered 2026/2035 was published in the Official Gazette on 8 October 2026. The Decision sets out the principles governing the monitoring of corporate email accounts and other communication channels provided to employees for work purposes.

The Decision emphasises that employers must balance their legitimate business interests and management rights against employees' rights to privacy and freedom of communication. An employer's access to corporate communication tools does not automatically entitle it to monitor employees' communications. Employees should know whether messages and logs are checked and how the findings may be used, including in disciplinary decisions.

Key Principles

The key requirements for monitoring workplace communications are:

- **Prior information and transparency:** Employees must be informed before monitoring takes place. The notice should explain what is monitored and why, how checks are carried out, when message content may be accessed, the legal basis, retention period and employees' rights under the Turkish Personal Data Protection Law No. 6698 (the "**Law**"). A general statement that corporate email accounts may be monitored may not be sufficient. Employers can cover this in a clear, detailed employee privacy notice.
- **Lawful basis and employee consent:** Monitoring must rely on a valid legal ground under the Law. In an employment relationship, consent is not automatically the right basis for monitoring. Any consent must be freely given.
- **Necessity and proportionality:** Monitoring should have a clear, legitimate purpose and go no further than needed. Employers should start with less intrusive options and avoid collecting unnecessary data.
- **Monitoring of communication content:** Employers should generally read messages only where a specific concern or incident gives them a legitimate reason to do so. The review should stay focused on that issue, not become broad or continuous monitoring.
- **Work-related and private communications:** Employers should set clear rules on personal use of work communication tools. Even a ban on private use does not allow unrestricted monitoring; if work and private messages are mixed, checks should be narrower. Being able to access personal email, messaging or social media accounts does not itself give an employer the right to read them.
- **Access controls and data security:** Only authorised staff should have access to monitoring data, with access logged and kept confidential. Employers should also consider the personal data of third parties that may appear in communications, including sensitive personal data.
- **Retention and termination of employment:** Monitoring data should be kept only as long as needed. Employers must separately assess access to former employees' work email and related data; leaving the company does not justify indefinite access or retention.

Recommended Actions for Employers

Employers should check that their monitoring policies and privacy notices match what happens in practice. They should explain the checks to staff in advance, record their purpose and legal basis, favour less intrusive options, limit access to messages and results, and set retention and post-employment access rules. Non-compliance may lead to regulatory action.

The full text of the Decision is available at this [link](#).