

Principle Decision on Processing Biometric Data for Timekeeping Purposes

The Personal Data Protection Board (“**the Board**”), through its Principle Decision dated 29 April 2026 and numbered 2026/921 (“**the Principle Decision**”), has determined that practices involving the processing of biometric data for employee timekeeping purposes are, as a general rule, unlawful data processing activities. The Principle Decision was issued in response to the increasingly widespread use by employers of biometric identification systems, — such as fingerprint, facial recognition, iris, or retina scanning — for employee attendance tracking, driven by technological developments.

The Board emphasized that, although labor law legislation imposes obligations regarding the monitoring and documentation of working hours, there is no explicit statutory provision requiring that such monitoring be carried out through the processing of biometric data. Accordingly, the Board concluded that biometric data processing conducted for timekeeping purposes cannot be grounded in the “explicitly provided for by law” processing condition set out forth in the Personal Data Protection Law (“**the Law**”).

The Board further noted that explicit consent obtained for timekeeping purposes may, in many cases, be deemed invalid as freely given consent due to the structural power imbalance inherent in the employer-employee relationship. It also stressed that even where such consent is considered valid, data processing activities must comply with the general principles enshrined in the Law — in particular, the principle of being relevant, limited, and proportionate to the purpose.

In this context, the Board concluded that the conducting timekeeping through biometric data processing is incompatible with the proportionality principle in particular. This is because employee attendance tracking can be achieved through alternative methods that do not require the processing of biometric data — which constitutes special categories of personal data — and that, in the event of a breach, pose more limited risks to the individuals concerned. In this regard, the Board recommended that employers adopt less intrusive alternatives, such as password-protected card or PIN-based systems, traditional signature sheets and attendance records, RFID/NFC identity cards, or manual recording methods under supervisory oversight.

In line with the Principle Decision, employers who continue to process biometric data for timekeeping purposes face the risk of administrative fines. It is therefore important that employers review their current practices and consider transitioning to alternative timekeeping methods as a matter of urgency.

JUNE 2026

JURISDICTION

Türkiye

PRACTICE AREA

Personal Data
Privacy