

Data Protection Authority's Public Announcement Following Its Principle Decision on the Processing of Biometric Data for Employee Time-Tracking Purposes

In June 2026, the Turkish Personal Data Protection Board (the “**Board**”) published Principle Decision No. 2026/921 on the Processing of Biometric Data for Employee Time Tracking Purposes (the “**Principle Decision**”), addressing employers’ use of biometric systems, such as fingerprint and retina scanning, to track employees’ working hours.

In the Principle Decision, the Board held that employers cannot rely on the “expressly provided for by law” legal basis to process biometric data merely because they are statutorily obligated to record employees’ working hours. The Board also noted that, given the inherent imbalance of power in the employment relationship, employees’ explicit consent to the processing of biometric data for time-tracking purposes will, in most cases, fail to constitute valid, freely given consent.

Following the Principle Decision, and in response to requests for clarification, the Turkish Personal Data Protection Authority (the “**Authority**”) published a Public Announcement (the “**Announcement**”) on its official website on 27 August 2026, addressing employers’ questions on the practical application of the Principle Decision. The Announcement clarifies the following:

- Converting data collected through methods such as fingerprint or palm scanning into an employee-specific mathematical code does not remove its status as biometric data. Any data that enables the unique identification or authentication of an employee through a specific technical method qualifies as biometric data;
- No legal provision expressly permits employers to process biometric data for employee time-tracking purposes, and obtaining employees’ explicit consent for this sole purpose would violate the principle of proportionality; and
- Employers whose operations or facilities present security risks may use biometric identification systems as part of multi-layered security measures, including for identity authentication, authorization or access control to critical areas. Even so, employers must comply with the principle of proportionality and other requirements under the Turkish Law on the Protection of Personal Data (the “**LPPD**”), and must assess the necessity of biometric data use on a case-by-case basis.

The Announcement reaffirms that employers should not process biometric data solely for employee time-tracking purposes. Employers using fingerprint or similar biometric systems solely to track entry, exit or working hours should review their current practices and discontinue such use to mitigate the risk of administrative sanctions. Where an employer considers biometric data processing necessary for other purposes, such as security, it should assess the specific circumstances to determine whether its use of biometric systems complies with the LPPD’s requirements.