MARIF

Advisory **5 June, 2026**

Client Alert

Personal Data Protection Authority's Principle Decision on the Processing of the Biometric Data for the for Working-Time Tracking

Introduction

Turkish Personal Data Protection Board's (the "**Board**") Principle Decision (the "**Decision**") dated 29 April 2026 and numbered 2026/921 was published in the Official Gazette on 2 June 2026. With this Decision, it was concluded that reliance on employees' explicit consent would not in itself resolve the lawfulness issue, particularly where less intrusive alternatives are available.

In the published Decision, it was stated that one of the most frequently encountered issues in the notices and complaints submitted to the Personal Data Protection Authority (the "**Authority**") is the increasingly widespread use of biometric data by institutions and organizations for the purposes of digitalizing working-hour tracking and enhancing security. In particular, given the serious doubts as to whether explicit consent is based on free will in light of the imbalance of power inherent in employer-employee relationships, it was concluded that this method should not be used, on the grounds that biometric data processing activities must comply not only with a legal basis but also with the principles of (a) proportionality, (b) necessity, and (c) data minimization.

Scope of the Decision

The Board determined that biometric data constitutes one of the special categories of personal data listed under Article 6 of the Personal Data Protection Law No. 6698 (the "**Law**") and emphasized its importance due to the sensitive and irreversible nature of such data and the possibility that, if disclosed, it may lead to victimization of individuals. The Decision referred to similar judgments of the Constitutional Court and the Council of State holding that the use of fingerprint registration systems and palm vein readers did not satisfy the criteria of being relevant to the purpose, limited, and proportionate as required under the Law.

The Decision is directed particularly at institutions and organizations using biometric data for the purpose of working-hour tracking, especially data controllers. As also stated in the Decision, pursuant to the relevant article of the Law, data controllers are obliged to take all necessary technical and administrative measures to ensure an adequate level of security in order to prevent the unlawful processing of personal data, prevent unlawful access to personal data, and ensure the preservation of personal data. The Law defines the data controller as the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Key Reasoning of the Court

The Board examined the lawfulness of the use of biometric data for the purpose of tracking working hours in terms of the criteria of being relevant to the purpose and limited, as well as proportionality.

The Board concluded that, in terms of the principle of being relevant to the purpose and limited, where alternative methods exist for working hour tracking, the processing of biometric data cannot be characterized as the least intrusive method. Indeed, in practice, methods such as password protected cards or PIN-based systems, traditional signature and paper-based attendance sheets, RFID/NFC identity cards, or manual entry under supervisor monitoring are available; therefore, the use of sensitive data such as biometric data cannot be regarded as the least intrusive method.

In the assessment under the principle of proportionality, the Board acknowledged that employers are required under labour legislation to monitor and document working hours. However, it emphasized that this obligation does not expressly require or authorize biometric data processing.

Conclusion

Through this Decision, the Board has set forth its position regarding the processing of special categories of personal data under the Law and clarified the criteria it takes into account when assessing whether an activity constitutes a violation in terms of personal data protection. The Decision significantly clarifies the Board's approach to the lawfulness of biometric attendance systems in workplaces. Employers using biometric systems for working-time tracking should reassess these systems, consider less intrusive alternatives, review retained biometric templates/data, and update their privacy notices, data inventory and retention/destruction practices.

The full text of the Decision is available at this link.