ASC law
AKSU ÇALIŞKAN BEYGO ATTORNEY PARTNERSHIP

2 June 2026

Principle Decision on the Processing of Biometric Data for Time and Attendance Tracking Purposes

On 2 June 2026, the Personal Data Protection Board's ("**Board**") Principle Decision dated 29 April 2026 and numbered 2026/921 (the "**Principle Decision**"), which sets forth the Board's approach regarding the conduct of employee attendance tracking in workplaces through the processing of biometric data, was published in the Official Gazette.

I. EXECUTIVE SUMMARY

The key principles determined by the Principle Decision are as follows:

1. Although tracking working hours constitutes a legal obligation for employers, fulfilling this obligation does not require the processing of biometric data.

2. Under the current legal framework, the processing of biometric data for attendance-tracking purposes is, as a general rule, not considered lawful.

3. Due to the imbalance of power inherent in the employer-employee relationship, explicit consent obtained from employees may not, on its own, constitute a sufficient legal basis, the processing of biometric data raises concerns with respect to the principle of proportionality.

4. Employers should prefer less intrusive alternative methods instead of biometric authentication systems when carrying out employee attendance-tracking activities.

Further details regarding the Principle Decision are provided below.

II. GENERAL ASSESSMENT

In its Decision, the Board noted that the Personal Data Protection Authority has recently observed an increase in complaints and reports concerning the use of biometric systems for employee attendance tracking. The Board emphasized the inherently high-risk nature of biometric data, the particular significance of the imbalance of power in the employer-employee relationship when assessing the validity of explicit consent, and the need to evaluate biometric data processing activities carried out for attendance-tracking purposes in light of the general principles set out under the Law on the Protection of Personal Data No. 6698 (the "**Law**").

The fundamental approach adopted by the Principle Decision is that, although employers are legally required to monitor working hours, there is no explicit legal provision requiring or mandating the

processing of biometric data for the fulfilment of this obligation. Accordingly, the Board stated that relying solely on explicit consent is insufficient for the processing of biometric data for attendance-tracking purposes and that such practices must also be assessed against the general principles set out under Article 4 of the Law.

In this regard, the Board concluded that, under the current legal framework, the processing of biometric data for attendance-tracking purposes should generally not be considered lawful. The Board further stated that employers should instead prefer less intrusive alternatives, such as password-protected card systems, PIN-based systems, traditional attendance sheets and signature logs, RFID/NFC identification cards, or manually maintained attendance records under supervisory control.

The Board's key findings and assessments under the Principle Decision are explained in detail below.

III. BOARD'S ASSESSMENT ON THE CONCEPT OF BIOMETRIC DATA AND ITS NATURE AS SPECIAL CATEGORIES OF PERSONAL DATA

Under the Principle Decision, the Board first assessed the legal nature of biometric data and emphasized that such data is subject to a stricter protection regime compared to other categories of personal data due to its classification as special categories of personal data.

In this regard, the Board noted that biometric data is expressly regulated as a special category of personal data under Article 6 of the Law. Although Turkish legislation does not contain a comprehensive definition of biometric data, the Board stated that, based on various legislative provisions and international regulations, biometric data should be regarded as data relating to the physical, physiological, or behavioural characteristics of an individual that enable the unique identification or verification of that individual's identity.

The Principle Decision lists fingerprints, palm vein patterns, retina and iris data, facial geometry, voice characteristics, signature dynamics, and keyboard usage patterns among examples of biometric data. The Board further highlighted that, unlike many other categories of personal data, biometric data is immutable and irreversible in nature. While a compromised password or username may be changed, biometric identifiers such as fingerprints, facial geometry, or iris data generally cannot be altered or rendered unusable once compromised. This significantly increases the risks that may arise for data subjects in the event of unlawful processing or a security breach involving biometric data.

Accordingly, the Board stated that it is not sufficient for the processing of biometric data merely to rely on one of the legal grounds set out under the Law. Rather, such processing activities must also be subject to a stricter assessment in light of the principles of necessity, proportionality, and data minimisation.

IV. LEGISLATION GOVERNING ATTENDANCE TRACKING AND THE BOARD'S ASSESSMENT OF THE CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

Within the scope of the Principle Decision, the Board first examined the legislative framework governing employers' obligations regarding the monitoring of working hours and stated that employers are required under various legal provisions to monitor employees' entry and exit times and to document working hours.

In this regard, the Board noted that the Turkish Labour Law No. 4857 contains provisions concerning the determination of working hours, notification of such hours to employees, and the maintenance of employee records. Furthermore, the Regulation on Working Hours under the Labour Law requires employers to document working hours through appropriate means. Accordingly, the Board concluded that there is no doubt that monitoring employees' attendance and working hours constitutes a legitimate and legally necessary purpose for employers.

However, the Board also emphasized that the relevant legislation does not prescribe any particular method for monitoring working hours and, more importantly, does not contain any provision requiring or expressly authorizing the processing of biometric data for this purpose. In other words, while employers are legally required to monitor working hours, the legislation does not render the use of biometric authentication systems either mandatory or necessary for fulfilling this obligation.

Based on this assessment, the Board concluded that attendance-tracking activities involving biometric data processing do not fall within the scope of the legal grounds for processing special categories of personal data set out under subparagraphs (b), (c), (ç), (d), (e), (f), and (g) of Article 6/3 of the Law.

V. ASSESSMENT OF EXPLICIT CONSENT AND THE IMBALANCE OF POWER IN THE EMPLOYER-EMPLOYEE RELATIONSHIP

The Board observed that, in practice, biometric data processing activities conducted for attendance-tracking purposes are generally based on employees' explicit consent. However, the Board emphasized that, given the nature of the employer-employee relationship, the validity of such consent must be assessed separately.

Under the Law, explicit consent is defined as consent that is (i) related to a specific subject matter, (ii) based on informed choice, and (iii) given freely. Accordingly, for explicit consent to be deemed legally valid, the data subject must have a genuine choice and must be confident that refusing consent will not result in any adverse consequences.

The Board highlighted the inherent economic and administrative imbalance of power between employers and employees and stated that it should therefore be assessed whether employees are effectively guaranteed that they will not suffer any adverse consequences if they refuse the biometric data processing activity proposed by the employer or subsequently withdraw their consent.

The Board further stated that where (i) employees are not effectively given the opportunity to refuse consent, (ii) employees are not effectively given the opportunity to withdraw consent at a later stage, or (iii) refusing consent may result in direct or indirect adverse consequences for employees, it cannot be concluded that employees are making a genuinely free choice. Consequently, explicit consent obtained within the context of the employer-employee relationship cannot automatically be presumed to be freely given in all circumstances.

Accordingly, the Board concluded that, as a general rule, relying solely on explicit consent does not constitute a sufficient legal basis for the processing of biometric data for attendance-tracking purposes. In other words, obtaining explicit consent from employees in compliance with procedural requirements does not, by itself, render such processing activities lawful.

The Board's approach demonstrates that, when assessing the lawfulness of biometric data processing activities, consideration should be given not only to the legal grounds for processing under Article 6 of the Law but also to the general principles set out under Article 4 of the Law. Therefore, the Board stated that, beyond the issue of explicit consent, the processing of biometric data for attendance-tracking purposes must also be assessed against the principles established under Article 4 of the Law, particularly the principle of proportionality.

VI. THE PRINCIPLE OF PROPORTIONALITY, ALTERNATIVE METHODS AND THE BOARD'S FINAL ASSESSMENT

In the Principle Decision, the Board did not limit its assessment of biometric data processing for attendance-tracking purposes to the applicable legal grounds for processing and explicit consent. The Board also examined the processing activity in light of the general principles set out under Article 4 of the Law, namely (i) being relevant to the purpose of processing, (ii) being limited to the purpose of processing, and (iii) being proportionate to the purpose of processing.

The Board emphasized that, for a personal data processing activity to be considered lawful, it is not sufficient merely to rely on a valid legal basis for processing. The processing activity must also be relevant, limited, and proportionate to the intended purpose. In this regard, the Board stated that biometric data processing activities carried out for attendance-tracking purposes should be assessed against the following three criteria:

- Whether the method used is suitable for achieving the intended purpose;
- Whether the same purpose can be achieved through less intrusive means; and
- Whether a fair balance exists between the interference with the fundamental rights and freedoms of the data subjects and the legitimate purpose pursued.

While acknowledging that monitoring employees' entry and exit times and working hours constitutes a legitimate purpose, the Board concluded that the processing of biometric data is not necessary to achieve that purpose. The Board noted that alternative methods serving the same purpose are already available in practice, including password-protected card systems, PIN-based authentication methods, RFID/NFC identification cards, traditional attendance sheets and signature logs, and manually maintained attendance records under supervisory control.

According to the Board, where such alternative methods are available, resorting to biometric authentication systems that require the processing of employees' special categories of personal data does not satisfy the principle of proportionality. The Board further stated that attendance tracking essentially serves an administrative purpose, whereas biometric data is highly sensitive and irreversible in nature. Therefore, the Board concluded that processing biometric data for the purpose of monitoring employee attendance does not strike a fair balance between the intended objective and the intrusion into employees' privacy rights. Moreover, the level of risk associated with biometric data was considered to constitute a more intrusive measure than necessary for a limited purpose such as attendance tracking.

Accordingly, the Board concluded that, under the current legal framework, the processing of biometric data for attendance-tracking purposes should, as a general rule, not be considered lawful. The Board further stated that employers should instead prefer less intrusive alternatives such as password-

protected card systems, PIN-based authentication methods, RFID/NFC identification cards, traditional attendance sheets and signature logs, manually maintained attendance records under supervisory control, or similar methods.

VII. PRACTICAL IMPLICATIONS AND ASSESSMENT FOR DATA CONTROLLERS

The Principle Decision is of particular significance for data controllers that use fingerprint recognition, facial recognition, palm vein recognition, or similar biometric authentication systems for the purpose of monitoring employees' attendance and working hours.

Although the Principle Decision does not introduce a new prohibition, the Board has clearly expressed its view that the processing of biometric data for attendance-tracking purposes cannot be regarded as lawful under the current legal framework. Therefore, attendance-tracking practices based on biometric systems may be considered high-risk during inspections and investigations conducted by the Board and may ultimately result in the imposition of administrative fines.

One of the most noteworthy aspects of the Decision is the Board's explicit statement that obtaining employees' explicit consent does not, on its own, constitute a sufficient legal basis for such processing activities. The Board emphasized that, due to the imbalance of power inherent in the employer–employee relationship, there are legitimate concerns as to whether employees' consent can genuinely be regarded as freely given. Furthermore, the Board stated that even where explicit consent is deemed valid, the processing of biometric data may still violate the principle of proportionality. Accordingly, the legal risks associated with existing biometric attendance-tracking systems that rely on employees' explicit consent have significantly increased.

At the same time, it should be noted that the Principle Decision is limited to biometric data processing activities carried out for attendance-tracking purposes. It does not contain any direct assessment of biometric data processing activities conducted for different purposes, such as access control to workplace premises, authorization for entry into critical areas, or operational processes requiring enhanced security.

In this context, data controllers processing biometric data for employee attendance tracking should:

- Review their existing attendance-tracking systems and the categories of data processed within those systems;
- Reassess whether the use of biometric authentication systems for attendance tracking is genuinely necessary; and
- Evaluate the feasibility of implementing less intrusive alternative methods capable of achieving the same purpose.

In conclusion, through the Principle Decision, the Board has adopted a strict approach towards the processing of biometric data for attendance-tracking purposes, particularly due to the fact that biometric data constitutes a special category of personal data. Accordingly, employers using biometric authentication systems within employee attendance-tracking processes should reassess their current practices and consider planning a transition to alternative methods in order to mitigate potential regulatory compliance risks and administrative sanctions.

For any further information, you may contact us.

KEMAL TAĞA
Senior Partner
kemal.taga@aschukuk.com

SAMET EŞER
Associate
samet.eser@aschukuk.com

MEHMET ARSLAN
Associate
mehmet.arslan@aschukuk.com

This newsletter has been prepared as of 2 June 2026 for informational purposes regarding the Personal Data Protection Board's Principle Decision dated 29 April 2026 and numbered 2026/921.

The assessments contained in this newsletter do not constitute legal advice or legal opinion, and no liability whatsoever can be attributed to Aksu Çalışkan Beygo Law Firm due to these assessments. It is recommended that you obtain legal counsel regarding any questions or issues within the scope of this newsletter.

ASC law
AKSU ÇALIŞKAN BEYGO ATTORNEY PARTNERSHIP

Address	Telephone	Fax	E-Mail / Internet Address
Harmancı Giz Plaza Kat: 3-8-15-16	+90 212 284 98 82	+90 212 284 98 83	info@aschukuk.com
Levent İstanbul		+90 212 279 63 32	www.aschukuk.com