LBF Partners

KVKK Principal Decision: Verification Mechanisms Now Mandatory for Loyalty Card Programs

A. Introduction

The Personal Data Protection Board ("**Board**") issued its Decision No. 2026/266 ("**Decision**") on 11 February 2026, addressing the practice whereby third parties use another individual's mobile phone number or loyalty card number to transact under that individual's loyalty card programme. The Decision was published in the Official Gazette dated 28 February 2026, No. 33182.

The relevant Decision can be accessed here.

B. Background

In the context of loyalty card programmes operated by data controllers across various sectors, the Authority has received numerous reports through different channels indicating that third parties make purchases by providing the cardholder's mobile phone number to the cashier, without entering any confirmation code. These reports highlight that such transactions result in purchases being recorded and invoices being issued in the cardholder's name without their knowledge or consent.

The Authority's investigation revealed that this practice is widespread across multiple sectors, including food, cosmetics, technology, construction markets, and clothing. It was found that, in order to benefit from discounts, promotions, and point accrual, it was sufficient to simply provide the cashier with a mobile phone number or loyalty card number, with no verification mechanism in place to confirm whether the transaction was carried out by the cardholder or with their knowledge and consent. Notably, however, verification mechanisms such as SMS codes, barcodes, or QR codes were already widely used for point redemption transactions.

C. Evaluation of the Current Practice

The Board concluded that the data processing activities associated with the above-described loyalty card usage violate the principle of "accuracy and, where necessary, being up to date" set out in Article 4 of the Personal Data Protection Law No. 6698 ("**Law**"), and that such processing cannot be justified under any of the lawful processing conditions in Article 5 of the Law, rendering it unlawful. The Board further held that contractual provisions in loyalty card agreements that place liability on cardholders for unauthorised third-party use of their cards do not relieve data controllers of their obligation to ensure data security under Article 12 of the Law.

D. Obligations Imposed

The Board first ordered the cessation of the practice whereby third parties make purchases using loyalty cards without the cardholder's knowledge and consent.

To that end, data controllers are required to implement verification mechanisms, such as the following, to confirm that the transaction is carried out with the cardholder's knowledge and consent:

(i) A one-time verification code sent via SMS to the cardholder's registered mobile phone number, which must be provided to the cashier;

(ii) A barcode or QR code generated through the mobile application or website, which must be scanned at the checkout;

LBF Partners
Esentepe Mah. Büyükdere Cad. No:108/1 K:7 34394 Şişli İstanbul Türkiye

(iii) Presentation or scanning of the physical loyalty card at the checkout;

(iv) Entry of the loyalty card password into the transaction device at the checkout;

(v) Where purchases are made by providing only a mobile phone number, an opt-in mechanism allowing the cardholder to consent to specific transaction types (point accrual, discounts/promotions, point redemption).

The Board further noted that data controllers may offer different verification mechanisms to different categories of cardholders and may adopt tiered verification approaches based on the transaction type and associated risk level.

E. Compliance Process

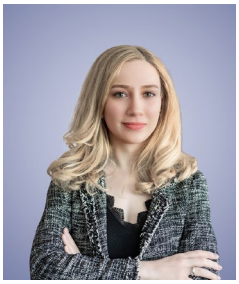
The Decision entered into force upon its publication in the Official Gazette on 28 February 2026, granting data controllers a six-month compliance period to establish the required verification mechanisms. The compliance deadline is therefore 28 August 2026. Data controllers that fail to implement the prescribed measures and continue to operate in breach of the Law will be subject to administrative sanctions under Article 18 of the Law.

F. Conclusion

The Board's Decision No. 2026/266 establishes a clear legal framework for personal data processing activities conducted under loyalty card programmes and requires data controllers operating such programmes to implement verification mechanisms. It is essential that the necessary technical and administrative measures are put in place without delay during the six-month compliance period commencing on 28 February 2026.

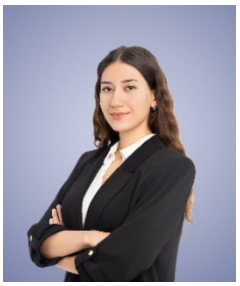
Data controllers across all sectors that operate loyalty card programmes, particularly in food, cosmetics, technology, construction markets, and clothing, should review their existing loyalty card infrastructure, identify and implement appropriate verification mechanisms, and complete the necessary administrative arrangements to ensure full compliance with the Law.

For further information and support, please contact us.



Elif Çopur Çelebi
Partner
e.copur@lbfpartners.com

Ceren Baranalp Atbaş
Senior Associate
c.baranalp@lbfpartners.com



Büşra Karabudak
Associate
b.karabudak@lbfpartners.com