Resolution of the Personal Data Protection Board, numbered 2022/266 and dated February 11, 2026, Regarding the Use of a Loyalty Card Holder's Mobile Phone Number or Loyalty Card Number by a Third Party During a Purchase

Within the scope of Loyalty Card Programs operated by data controllers in various sectors; a purchase was made by a third party sharing the mobile phone number of the relevant individual, who is the loyalty card holder, with the cashier during the transaction; this purchase transaction conducted via the loyalty card was carried out by the cashier without entering any transaction approval code into the system; despite the data subject not being present at the checkout during the transaction and lacking both knowledge and consent, the data controller facilitated the use of personal data—specifically the data subject's mobile phone number—shared by a third party to enable a purchase via the loyalty card; Additionally, invoices and other documents related to the purchase were issued in the individual's name, constituting unlawful data processing activities and a breach of personal data security. Reports and complaints regarding these matters were submitted to the Personal Data Protection Authority (Authority) through various channels, and it has become necessary for the Personal Data Protection Board (Board) to issue a Principle Decision on the matter.

As a result of the investigation conducted on this matter;

- It was found that the practice in question is widespread within loyalty card membership programs operated by data controllers active in various sectors such as food, cosmetics, technology, home improvement, apparel, etc.;

- Generally, loyalty cards are issued by data controllers under the terms of the membership agreement for the personal use of the relevant individuals;

- Loyalty card membership is established by sending a one-time verification code via SMS to the data subject's mobile phone number, or by using methods such as scanning a barcode or QR code via a mobile app or website;

- Purchases can be made using the loyalty card, and discounts and promotions can be availed of by providing the relevant individual's mobile phone number or loyalty card number to the cashier;

- Regarding the use of the loyalty card during a purchase for purposes such as discounts, promotions, or earning points; without the data controllers establishing any verification mechanism to determine whether the purchase was made directly by the relevant individual or with their knowledge and consent, it is common practice to complete the purchase transaction via the loyalty card simply by providing the relevant individual's mobile phone number or loyalty card number to the cashier,

- On the other hand; regarding transactions involving the redemption of points earned through loyalty card usage, verification mechanisms such as providing the cashier with a one-time verification code ( ) sent via SMS to the relevant individual's mobile phone number, or scanning a barcode/QR code provided through a mobile app or website at the checkout, are widely used;

- The invoice or similar document issued as a result of a purchase made using the loyalty card is frequently issued in the name of the relevant individual who is the loyalty cardholder, and the customer transaction details related to the purchase (purchased product/service, purchase date, etc.) are recorded in the relevant individual's records; Therefore, it has been determined that personal data breaches may occur if a third party uses the cardholder's phone number or loyalty card number for a purchase without the cardholder's knowledge or consent, resulting in erroneous customer transaction information being recorded in the cardholder's records or membership account, or an invoice being issued for a purchase the cardholder did not make and about which they had no knowledge or consent.

Upon reviewing the relevant legal provisions;

- Article 4 of the Personal Data Protection Law No. 6698 (the Law), titled "General Principles," states that personal data may only be processed in accordance with the procedures and principles set forth in the Law and other laws; in the processing of personal data, the principles of "compliance with the law and the rules of good faith," "accuracy and, where necessary, up-to-date status," "processing for specific, explicit, and legitimate purposes," "being relevant, limited, and proportionate to the purpose for which they are processed," and "retention for the period prescribed by applicable legislation or necessary for the purpose of processing" are mandatory.

- Paragraph (1) of Article 5 of the Law, titled "Conditions for the Processing of Personal Data," stipulates that personal data may not be processed without the explicit consent of the data subject; Paragraph (2) states that processing is permitted if it is "expressly provided for by law," "necessary to protect the life or physical integrity of the data subject or another person where the data subject is unable to express consent due to actual impossibility or where legal validity is not recognized for their consent," "the necessity of processing personal data belonging to the parties to a contract, provided that such processing is directly related to the conclusion or performance of the contract," "the necessity of processing to enable the data controller to fulfill its legal obligations," "the data having been made public by the data subject," "the processing of data is necessary for the establishment, exercise, or defense of a legal claim," or "the processing of data is necessary for the legitimate interests of the data controller, provided that such processing does not infringe upon the fundamental rights and freedoms of the data subject," it has been established that the processing of personal data is permissible without the data subject's explicit consent.

- Under paragraph (1) of Article 12 of the Law, titled "Obligations Regarding Data Security," it is stipulated that the data controller must take all necessary technical and administrative measures to ensure an appropriate level of security prevent unlawful access to personal data, and ensure the protection of personal data.

In this context, based on research conducted and after consulting representatives from various sectors, the Board has evaluated the practice in question—which is understood to be widespread within Loyalty Card Programs—and concluded that:

- The act of a third party disclosing the relevant individual's mobile phone number or loyalty card number to the cashier during a transaction—without the individual's knowledge or consent—to carry out a purchase transaction on the individual's behalf cannot be justified under any of the data processing conditions set forth in Article 5 of the Law and constitutes an unlawful processing of personal data;

- The issuance of invoices, etc., in the name of the data subject regarding a purchase transaction not made by the data subject themselves, without their knowledge or consent, using the data subject's mobile phone number or loyalty card number; and/or recording customer transaction information (such as which store, on what date, and which product was purchased) in the data subject's records or membership account, constitutes a violation of the principle of "accuracy and, where necessary, up-to-date nature" as stipulated in Article 4 of the Law,

- Although data controllers have imposed a responsibility on data subjects under the Loyalty Card Membership Agreement to ensure that loyalty cards issued for their personal use are not made available to third parties, it has been determined that this does not eliminate the obligation to ensure the security of personal data, as stipulated in Article 12 of the Law, in the personal data processing activities conducted by data controllers;

- The practice of enabling a transaction via the loyalty card by having a third party disclose the data subject's mobile phone number or loyalty card number to the cashier during a purchase—without the data subject's knowledge or consent—which is deemed unlawful under the Law, must be discontinued;

- To ensure that personal data processing procedures related to transactions conducted via loyalty cards comply with the Law, data controllers must implement the necessary technical and administrative measures as stipulated in Article 12 of the Law;

- To verify that a transaction conducted by providing the cardholder's mobile phone number or loyalty card number to the cashier was carried out with the relevant individual's knowledge and consent; To verify the use of loyalty cards for any purpose (such as creating an account, earning points during a purchase, using points, or

benefiting from discounts/promotions), the one-time verification code sent via SMS to the relevant individual's mobile phone number must be provided to the cashier; the QR code provided through the mobile app or website; QR code provided via the mobile app or website; presenting or scanning the physical loyalty card at the register; entering the loyalty card PIN into the register terminal; and, when using a loyalty card through an online membership account created under the loyalty card program, providing only the mobile phone number to confirm consent for which transactions (earning points during shopping/benefiting from discounts or promotions/redeeming points) are authorized , and

- Considering that the primary objective is to use the most appropriate verification methods to prevent personal data breaches that may occur during personal data processing activities carried out by a third party using the mobile phone number or loyalty card number of a data subject with a loyalty card membership without the data subject's knowledge or consent; data controllers must opt for verification mechanisms that serve this purpose; in this context, alternative verification mechanisms may be offered for different groups of individuals; in the loyalty card application, different verification mechanisms may be used depending on the type of transaction—such as membership verification, earning points/discounts/promotions, or spending points—and the risk level associated with these transactions,

- A six-month compliance period is provided for data controllers to establish the aforementioned verification mechanisms, effective from the date of publication of this Principle Decision;

- The public and sector representatives shall be informed that data controllers who fail to implement the aforementioned measures, continue this practice in violation of the provisions of the Law, or are found not to act in accordance with the matters specified in this Principle Decision, will be subject to proceedings under the provisions of Article 18 of the Law;

- It has been decided by unanimous vote to publish this Decision, adopted in accordance with the sixth paragraph of Article 15 of the Law, in the Official Gazette and on the Authority's website.