Personal Data Protection Board's Decision No. 2023/567 dated April 11, 2023, regarding "The mandatory requirement to store credit/debit card information for making purchases on an e-commerce site"

Date of Decision : April 11, 2023

Decision No : 2023/567

Subject Summary : Regarding the mandatory requirement to save bank/credit card information in order to make purchases on an e-commerce site

In summary, the complaint received by the Authority states:

- When the individual attempted to make a purchase through the e-commerce site, the "add credit/debit card" button appeared on the payment screen, requesting the individual to save their credit/debit card information; saving such information was made mandatory for the individual to complete the purchase, and the "continue" buttons did not function without entering the relevant information, making the purchase impossible;
- There is no valid legal basis for processing personal data under the Law on the Protection of Personal Data No. 6698 (the Law) for the data controller to store credit/debit card information, and the user has not provided explicit consent to the data controller,
- Furthermore, it was noted that the data subject was not provided with any information regarding this processing, and it was requested that the necessary actions be taken against the intermediary service provider under the Law.

As part of the investigation initiated regarding this matter, the data controller was requested to submit a defense, and in the response provided by the data controller, it was summarized as follows:

- The company, which operates as a service provider and intermediary service provider, processes billing address and credit/debit card information (card number, cardholder's first and last name, and expiration date) for the purpose of completing payment transactions,
- It is possible to browse the website without creating an account or becoming a customer; customers are not required to add credit card information to their wallets in any way before creating an account or during the account creation process. However, similar to other retail companies in Turkey's online marketplaces, the data controller requires payment information to receive payments for customers' orders,
- When a customer wishes to make a purchase through the website, if there is no payment method in their wallet, they must add their card information to their wallet before selecting the "Proceed to Payment" option, These details are used to ensure the payment is processed in accordance with the customer's request; the processing of card information falls under the provision of Article 5(2)(c) of the Law, which states: "The

processing of personal data belonging to the parties to a contract is necessary provided that such processing is directly related to the conclusion or performance of the contract,"

- When the customer completes a purchase transaction, the Company processes the information related to this transaction to fulfill the legal obligations it has assumed under the Law No. 6563 on the Regulation of Electronic Commerce, both as a service provider and as an intermediary service provider, personal data is processed within the scope of the condition set forth in Article 5(2)(c) of the Law, which states that "processing is necessary for the data controller to fulfill its legal obligations,"
- In addition, the Company processes card information;
    - In order to detect fraud and abuse and protect the security of its customers, the Company, and other individuals, pursuant to the provision in Article 5(2)(f) of the Law stating that "the processing of data is necessary for the legitimate interests of the data controller, provided that it does not infringe upon the fundamental rights and freedoms of the data subject,"
    - In order to collect the monthly Prime membership fee from customers who are Premium members on the Company's website, the Company processes data in accordance with the provision in Article 5(2)(c) of the Law, which states that "the processing of personal data belonging to the parties to a contract is necessary provided that it is directly related to the conclusion or performance of the contract,"
- Customers who have added payment method information can remove their cards and update their information at any time via account settings; this demonstrates the control customers have over their accounts; customers who choose not to remove their card information from their wallets can easily make subsequent purchases without needing to re-enter the same information,
- Customers can view, edit, and completely remove their payment method information via their profile page; if a payment method is removed, the customer can continue to use their account on the website,
- The company clearly fulfills its obligation to inform data subjects regarding its data processing activities; the Privacy Notice states that payment information is processed for the purpose of conducting payment transactions, The Privacy Notice is published in accordance with Article 10 of the Law and the Communiqué on the Procedures and Principles to Be Followed in Fulfilling the Duty to Inform; this text is displayed at the bottom of every page customers visit on the website, on the account creation page, and on the login page, thereby allowing customers to review this text before sharing their personal data with the Company,
- It has been stated that, within this scope, the Company conducts its personal data processing activities in compliance with the Law.

As a result of the investigation conducted on the matter, pursuant to the Decision No. 2023/567 of the Personal Data Protection Board dated 04/11/2023;

- To verify the claims of the data subject and the statements of the data controller, the system was tested by creating a generic account on the website in question and attempting to place an order,
- In the "Add a Payment Method" step—the second step of the purchase process—there is a section labeled "Add a credit card or debit card." When this section is clicked, a window opens displaying two options: "Cancel" and "Add your card" ; clicking the "Cancel" option prevents the payment from being processed, thus preventing the purchase from being completed; clicking the "Add Your Card" option adds the card whose details were entered as the payment method, and proceeding to the next step in the purchase process is only possible after entering this information; after payment is made and the order is completed, it is observed that the card details saved in the "My Account-Wallet-Cards and Accounts" section, where the card information saved for the purpose of paying the completed order remains stored; it is understood that the relevant card information can be removed from the wallet by clicking the "Edit" option in this section,
- Consistent with the individual's claim, it is understood that the purchase cannot be completed without the card information being saved to the system, and that the card information remains stored in the wallet section even after the purchase is completed,
- It is necessary to assess whether the processing conditions put forward by the data controller regarding the mandatory storage of card information to complete the transaction and the continued storage of card information entered on the data controller's website for a previous transaction after the transaction is completed are valid,
- In the "Recommendation No. 02/2021 on the Conditions for Processing Credit Card Data Solely for the Purpose of Facilitating Subsequent Online Purchases," adopted by the European Data Protection Board (EDPB) on May 19, 2021," states that consent is the legal basis that can be relied upon for the continued processing of card information to facilitate purchases,
- and given that the data controller has indicated that individuals who have added a payment method can easily make subsequent purchases, the data controller has established a new purpose for data processing,
- In accordance with the principles of "purpose limitation, proportionality, and necessity" and "processing for specific, explicit, and legitimate purposes" set forth in Article 4 of the Law, a change in purpose indicates a new data processing process; therefore, when the purpose changes, the data processing condition must also be determined in a manner appropriate to the purpose,

- The data controller stated that entering card information is necessary to complete the transaction and relied on various processing conditions set forth in paragraph (2) of Article 5 of the Law; however, it is not possible to rely on the same processing conditions for the continued processing of card information in the membership account after the transaction is completed, the processing conditions put forward by the data controller are valid only within the scope of the data subject's current transaction; as stated in the data controller's declaration, since continuing to process card information to facilitate future purchases constitutes a change in purpose, an appropriate processing condition must also exist to achieve this purpose,
- The continued processing of card information after the current purchase transaction is completed can only be carried out within the scope of the data subjects' explicit consent obtained in accordance with the Law,
- However, the system currently implemented by the data controller does not operate in this manner; first, the card information is recorded, and subsequently, customers who wish to do so can remove their card information from their account, thereby ensuring control over the data; however, this situation misleads the data subjects in a manner inconsistent with the principle of "compliance with the law and the rule of good faith" set forth in Article 4 of the Law under the heading "General Principles,"
- Consequently, the card information required to complete a transaction within the scope of the membership account on the data controller's website continues to be processed in the relevant individual's wallet account after the transaction is completed, while such data processing could be carried out under the condition of explicit consent as stipulated in paragraph (1) of Article 5 of the Law, the data controller required the card information to be stored in the system and subsequently allowed the relevant individuals to delete this information, thereby, not only was valid explicit consent under Article 5 of the Law not obtained for the recording of card information, but the principles of "compliance with the law and the principle of good faith," "processing for specific, explicit, and legitimate purposes," and "processing that is limited and proportionate to the purpose for which it is carried out,"
- Since it was concluded that the data controller did not rely on a valid processing condition under Article 5 of the Law regarding the processing of the relevant individuals' card information, no separate investigation was conducted at this stage regarding whether an information notice was provided during this process; on the other hand, based on the assessment that the aforementioned data could only be processed within the scope of the relevant individuals' explicit consent,
- The card information required to be entered to complete a purchase within the scope of the membership account on the data controller's website was continued to be processed in the data subject's wallet account after the purchase was completed, for the purpose of facilitating subsequent purchases, while data processing for this purpose could be carried out under the explicit consent requirement set forth in Article 5(1) of the Law, the data controller mandated that card information be recorded in the system at and

subsequently allowed the data subjects to delete this information, thereby, neither was valid explicit consent obtained under Article 5 of the Law for the recording of card information, nor were the principles of "compliance with the law and the principle of good faith," "processing for specific, explicit, and legitimate purposes," and "processing that is limited and proportionate to the purpose for which it is processed," and that the data controller has thus failed to fulfill its obligations regarding data security under Article 12(1) of the Law,an administrative fine of 500,000 TL was imposed under Article 18(1)(b) of the Law, taking into account the unlawfulness of the offense, the data controller's fault, and its financial circumstances;

- Furthermore, considering that the continued processing of card information recorded during a transaction in a membership account is only permissible if the relevant individuals have provided their explicit consent in accordance with the Law, the data controller is instructed to develop a system that ensures the relevant individuals actively consent to the recording of credit card information in the membership account and to inform the Board of the outcome;
- Since it has been determined that the credit card data of the relevant individuals may only be processed in membership accounts under the condition of explicit consent, it has been decided to instruct the data controller to make the necessary amendments in the privacy notices regarding this matter and to inform the Board of the outcome.