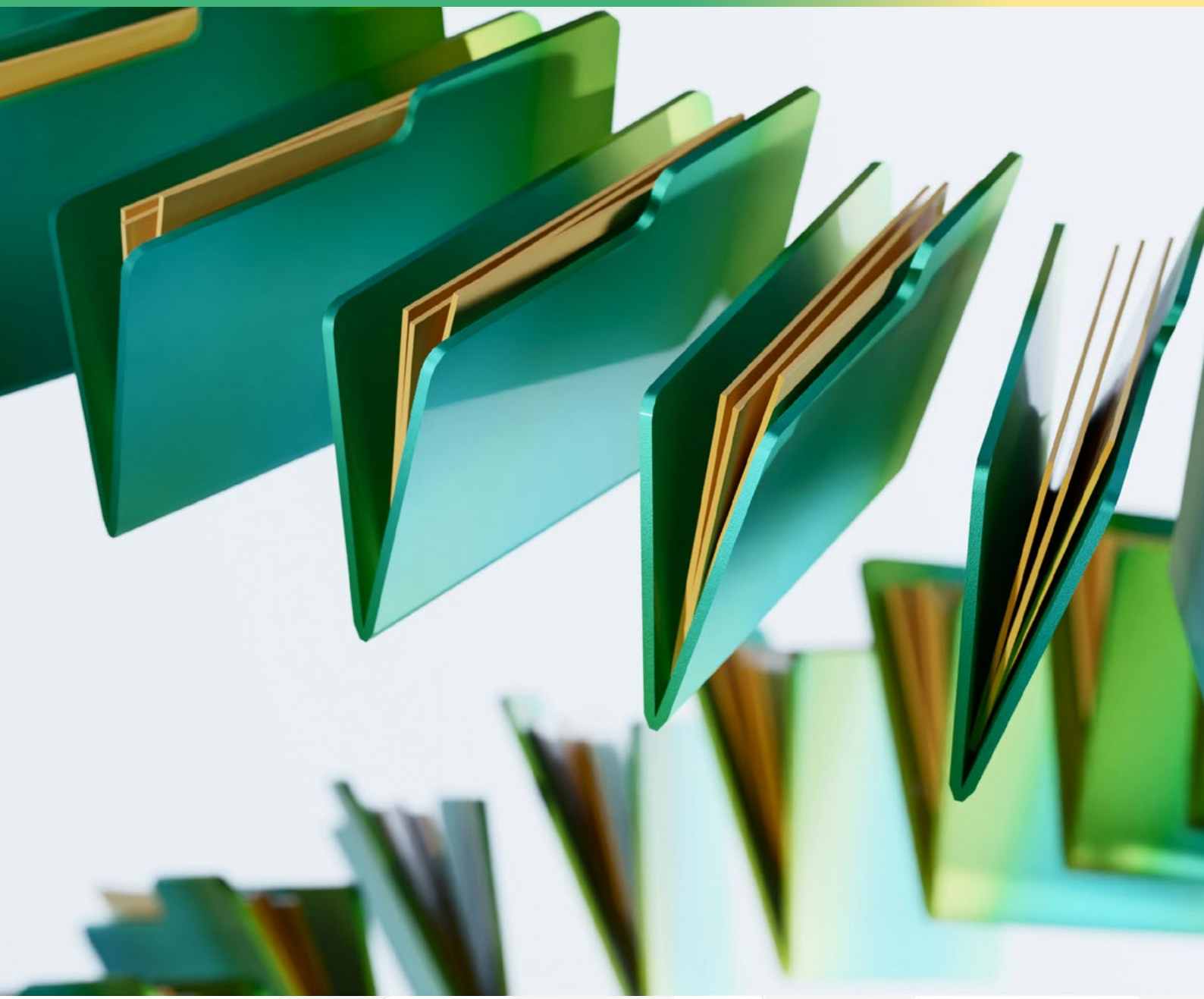

Highlights from Personal Data Protection Board Decisions:

47 Decision Summaries from Data Breaches to Explicit Consent

Sevgi Ünsal Özden
Ozan Akman
Gülnur Çakmak Ergene
Elvan Galatalı
Yağmur Bayiz
Tuğçe Polat

ERDEM & ERDEM
40 YEARS

Legend / Content Guide

Data Breaches

Decisions concerning incidents in which personal data was acquired, accessed or disclosed by unauthorized persons. In these decisions, the Personal Data Protection Board ("Board") assesses the adequacy of the technical and organizational measures taken by the data controller and the breach notification process.

Ransomware and Malware: Incidents in which data was encrypted, acquired or leaked through malware such as ransomware or Trojans.

Unauthorized Access and Phishing: Incidents in which unauthorized access to data was gained, or allegedly gained, through phishing e-mails, compromised user accounts or security vulnerabilities in systems.

Human or Technical Error: Breaches arising from the data controller's own processes without any external attack, such as sending data to the wrong recipient, misconfiguration or software errors.

Compliance and Rights

Decisions concerning, independently of any security incident, the legal basis on which and the manner in which personal data is processed, and how data subjects' requests are handled.

Explicit Consent, Marketing and Sending Commercial Electronical Messages: Decisions concerning the validity of explicit consent, making services conditional upon consent, requesting consent where it is not required, and sending commercial communications without consent.

Data Subject Requests: Decisions concerning whether data controllers have fulfilled data subjects' requests, such as access to their data, erasure of their data and the right to be forgotten.

Monitoring and Special Categories of Personal Data: Decisions concerning monitoring through camera and audio recording, and the processing of special categories of personal data such as biometric, health and political opinion data.

Obligation to Inform and Conditions for Personal Data: Decisions concerning whether individuals were informed about the processing activity and whether the processing was based on one of the processing conditions set out in the PDPL.

Labels:

Decision Instructing the Data Controller to Take Specific Action: Decisions in which the Board instructed the data controller to take corrective action, such as destroying the data or ceasing the processing. In some decisions, the instruction was issued together with an administrative fine.

Administrative Fine: Decisions in which the Board imposed an administrative fine on the data controller.

No Action: Decisions in which the Board decided that no further action was required.

Decision	Details
Data Breach Caused by a Ransomware Attack Occurring Abroad Board Decision dated 28 March 2025 and numbered 2025/601	• As a result of a ransomware attack targeting the accommodation reservation databases of a Hong Kong-based hotel management company, various personal data relating to approximately 909 customers residing in Türkiye, including name, contact details and payment card information, were subject to unauthorized access. • The Board considered that the company had no legal entity, employees or technological infrastructure in Türkiye, that all personal data were processed in Hong Kong, and that the data subjects did not benefit from the services in Türkiye. Accordingly, applying the "effects principle", the Board decided that the company was not subject to the personal data breach notification obligation under the PDPL and that no further action was required under the PDPL at this stage.
Data Breach Caused by Unauthorized Access to Customer Data Through Malware Board Decision dated 9 January 2025 and numbered 2025/88	• Cyber attackers infiltrated the computer of an IT manager employed by a restaurant chain and fast-food company through malware, obtained usernames and passwords stored in the browser, accessed the company's systems, and obtained the names and surnames, gender, e-mail addresses, telephone numbers and city information of 505,337 customers. • The Board took into account that the data controller lacked alarm and monitoring mechanisms capable of detecting unauthorized access, that basic security measures such as two-factor authentication, SIEM and firewall systems were implemented only after the breach, and that it had not been demonstrated that employees had received adequate training on data security. On this basis, the Board concluded that the data controller had failed to take the necessary technical and organizational measures to ensure data security. • The Board imposed a total administrative fine of TRY 1,000,000 on the data controller, comprising TRY 800,000 for failure to implement the necessary security measures and TRY 200,000 for failure to notify the data subjects of the data breach within the shortest possible time.

Decision	Details
Ransomware Attack Due To Inadequate Technical Security Measures Board Decision dated 26 December 2024 and numbered 2024/2196	• A ransomware attack targeting the systems of a company manufacturing plastic household goods and cleaning products resulted in a personal data breach affecting numerous categories of personal data, including employees' salary, bank account, identity and passport information, as well as special categories of personal data. The data controller submitted varying and inconsistent statements to the Board regarding the individuals and personal data affected by the breach. • The Board found deficiencies in data security on the grounds that the encryption of special categories of personal data and the use of cryptographic keys had only been implemented after the breach, the relevant log records could not be accessed, vulnerability testing had been inadequate, and two-factor authentication and security measures such as appropriate network segmentation had not been implemented to a sufficient extent before the breach. • Concluding that the necessary technical and organizational measures have not been taken to ensure data security, the Board imposed an administrative fine of TRY 250,000 on the data controller.
Ransomware Attack Due To Inadequate System Monitoring Board Decision dated 7 November 2024 and numbered 2024/1898	• A ransomware attack targeting the server hosting the order management system of a company operating in the pharmaceutical and healthcare products sector resulted in a personal data breach affecting identity, contact, personnel and customer transaction information relating to 196 current employees, 303 former employees and 17 customers/business partners. • The Board found that the attackers had carried out multiple actions on the server, including downloading malicious software and running files and code. It also found that the method of initial access could not be conclusively determined that the measures relating to network and server security and user authorization were inadequate, and that sufficient care and diligence had not been exercised in monitoring personal data security. Accordingly, the Board imposed an administrative fine of TRY 350,000 on the data controller.
Data Breach Resulting from a Trojan Attack Board Decision dated 9 October 2024 and numbered 2024/1718	• A Trojan virus infected the network server of a cosmetics and personal care company, resulting in a data breach affecting 325 copies of identity documents belonging to foreign nationals residing in Türkiye and identity and contact information relating to 107 brand ambassadors. • The Board found that the data controller had implemented EDR solutions for detecting malware only after the breach, had not conducted penetration testing, and had failed to provide any security scan report demonstrating that the systems were subject to regular monitoring and controls. Accordingly, the Board imposed an administrative fine of TRY 500,000 on the data controller.

Decision	Details
Data Breach Caused by the Spread of LockBit Ransomware to Servers in Türkiye, as Reported to the Authority by the Data Controller Board Decision dated 6 March 2024 and numbered 2024/415	• A LockBit ransomware attack targeting servers on which the data controller's data were stored and managed by a business partner in France spread, through the connection between France and Türkiye, to eight servers of the data controller located in Türkiye. The breach affected a total of 43 individuals, including employees, customers and end users, as well as more than 100,000 records, and involved personal data in the transaction security, financial and marketing categories. • The Board assessed that the malware had spread across network resources because access between network components had not been adequately and appropriately restricted and the network had not been segmented into sub-networks. It also found that no penetration testing had been conducted before the breach and that no security scan report had been submitted demonstrating that the systems were regularly monitored and controlled. Accordingly, the Board imposed an administrative fine of TRY 430,000 on the data controller for failure to implement the necessary technical and organizational measures.
Disclosure of Employee Data Following a Ransomware Attack Targeting a Group Company Abroad Board Decision dated 6 March 2024 and numbered 2024/413	• Following a ransomware attack targeting the systems of the data controller's group company abroad, which resulted in data being leaked on the dark web, identity, contact, personnel and health data relating to 56 employees of the data controller, which operates in the manufacture and trade of agricultural machinery, were affected by the breach. • The Board assessed that the ransomware attack leading to the breach could have been prevented through multi-factor authentication, but that the data controller had implemented basic security measures such as multi-factor authentication and security patches only after the breach. It further found that access between network components had not been sufficiently restricted or segmented and that the use of a common server system by different data controllers constituted both technical and organizational deficiency. Accordingly, the Board imposed an administrative fine of TRY 150,000 on the data controller.

Decision	Details
Ransomware Spreading to 797 Servers Through Software Downloaded by an Employee and Affecting the Personal Data of 4,885 Individuals Board Decision dated 23 December 2022 and numbered 2022/1375	• An employee of the U.S. entity of an industrial company installed an audio file conversion program downloaded from the internet on their computer, as a result of which ransomware infected the company network. The malware spread to 797 global servers and encrypted certain files stored on those servers. The breach affected 4,885 data subjects comprising employees, customers and suppliers; the personal data subject to the breach included identity and contact information, as well as IBAN, photograph, passport and blood group information. • The Board found that the data controller had failed to demonstrate that the urgent and critical security vulnerabilities identified in the penetration test conducted prior to the breach had been remedied, and that the necessary measures had not been taken in terms of password and access security, updates, network segmentation and employee awareness. Due to the inadequacy of the data security measures, the Board imposed an administrative fine of TRY 800,000 pursuant to Article 18/1(b) of the PDPL for breach of Article 12/1 of the PDPL, and a further administrative fine of TRY 200,000 pursuant to Article 18/1(b) of the PDPL for breach of Article 12/5 of the PDPL due to the personal data breach having been notified with a delay of 20 days, amounting to a total administrative fine of TRY 1,000,000.
Encryption and Disclosure of Personal Data Relating to 660 Individuals in a Ransomware Attack Carried Out Through a Service Provider Account Board Decision dated 21 July 2022 and numbered 2022/711	• The systems of an automotive safety and electronic systems manufacturer were compromised through a user account belonging to a service provider, resulting in a ransomware attack. The breach affected the identity, contact, payroll, leave and health data of 660 individuals, including customer and supplier representatives as well as current and former employees, and some of the data were published. • The Board stated that the attack activities could not be detected until the data were encrypted and that the necessary measures had not been taken to ensure the security of the service provider account. It therefore assessed that the data controller was jointly responsible for these deficiencies and imposed an administrative fine of TRY 500,000 pursuant to Article 18/1(b) of the PDPL on the grounds of breach of Article 12/1 of the PDPL.
Unauthorized Access to a Newsletter Distribution Platform Board Decision dated 2 May 2025 and numbered 2025/833	• Unauthorized access to a newsletter distribution platform operated by a non-profit organization resulted in a breach affecting the names, surnames and e-mail addresses of 15 individuals residing in Türkiye. The data controller became aware of the breach following notification by the data processor, temporarily suspended the platform, informed the affected individuals and took steps to implement additional security measures, including enabling multi-factor authentication. • The Board took into account the limited number of affected data subjects and data categories, the absence of any indication that the data had been misused for purposes such as fraud or identity theft, and the measures taken by the data controller following the breach and accordingly decided that no further action was required under the PDPL at this stage.

Decision	Details
Data Breach Caused by Unauthorized Access to a Marketing Account Board Decision dated 7 November 2024 and numbered 2024/1899	• Following the compromise of a user account used for marketing purposes by a company providing corporate support services to group companies in Europe, unauthorized access was gained to an FTP server from an IP address that was on a blacklist and, in some instances, configured as "publicly accessible". The breach affected the names and surnames, e-mail addresses, contact details and address information of approximately 70,000 individuals. • The Board found that the date of the breach could not be determined that files containing personal data had been left publicly accessible, that no strong password policy had been implemented prior to the breach, and that unauthorized access had remained undetected for an extended period. The Board therefore imposed an administrative fine of TRY 700,000 on the data controller.
Data Breach Due to a Phishing Attack and Security Vulnerability Board Decision dated 10 September 2024 and numbered 2024/1523	• An employee of a hotel clicked on a link contained in a phishing e-mail, because of which the employee's computer came under the control of unauthorized persons and the shift schedule stored on the computer, containing the names of 450 employees, was compromised. • Although the Board noted that the breach was limited to a single computer, it found that the data controller's systems contained update and configuration deficiencies, were not sufficiently protected against spam e-mails, used weak passwords, and lacked an advanced identity verification mechanism for access to servers. Accordingly, the Board imposed an administrative fine of TRY 500,000 on the data controller.
Data Breach Resulting from Exploitation of the Same Security Vulnerability Twice Board Decision dated 8 June 2023 and numbered 2023/1017	• An attacker exploited a security vulnerability in the systems of a digital gaming and entertainment platform hosting approximately 69 million active and former user accounts and carried out two separate breaches through the same vulnerability. The breach affected approximately 90,182 users residing in Türkiye and involved personal data including username, name, address, date of birth, gender, country and IP address. Children were also among the affected individuals, and the attacker offered the data for sale. • The Board found that the data controller had not been able to detect the breach through its own security systems, had not conducted penetration testing before the breach or implemented a patch management policy, and had failed to prevent the second breach carried out by exploiting the same vulnerability. Accordingly, the Board imposed an administrative fine of TRY 1,500,000 on the data controller.

Decision	Details
Unauthorized Access to a Mobile Application Database and Failure to Notify the Data Breach Board Decision dated 16 May 2024 and numbered 2024/790	• Unauthorized access was gained to the database of a software and technology company's mobile application, which contained 7,823 registered users. While the database included information such as names and surnames, e-mail addresses and telephone numbers, certain data in the application had been altered, and due to insufficient log records, it could not be conclusively determined how unauthorized access had occurred. • The Board considered the encryption of the database password, the change to the password policy only after the breach, and the lack of sufficient log records preventing determination of how unauthorized access occurred to constitute deficiencies in data security. Accordingly, it imposed an administrative fine of TRY 250,000 on the data controller. • The data controller did not notify the data subjects on the grounds that the personal data had not been harmed, and data integrity had not been altered. The Board emphasized that a personal data breach may arise not only from a loss of data integrity, but also from a breach of confidentiality or availability, and imposed a further administrative fine of TRY 100,000 for failure to comply with the notification obligation.
Data Breach Resulting from Member Information Being Sent to an Attacker Following a Phishing E-mail Board Decision dated 9 May 2024 and numbered 2024/728	• An employee of an international professional organization operating in the finance and accounting sector mistook a phishing e-mail appearing to have been sent by the organization's President and CEO for a genuine message and sent the attacker the names and surnames, membership numbers, and, for certain members, e-mail addresses of 217 Turkish members, resulting in a personal data breach. • The Board assessed that, prior to the breach, the data controller had failed to adequately consider the risks arising from phishing attacks and had not configured the security system used to verify incoming e-mail addresses with sufficient strictness. It further considered that, although employees had received training, the disclosure of personal data without first verifying the authenticity of the suspicious e-mail demonstrated that data security awareness had not been sufficiently embedded among employees. Accordingly, the Board imposed a total administrative fine of TRY 1,000,000 on the data controller, comprising TRY 750,000 for failure to implement the necessary technical and organizational measures to ensure data security and TRY 250,000 for failure to notify the Board within 72 hours of becoming aware of the breach.

Decision	Details
Erasure and Unauthorized Acquisition of User Data Following a Cyberattack on a Database Board Decision dated 25 January 2024 and numbered 2024/133	• Following a cyberattack targeting the database system of a provider of online food ordering, restaurant integration and delivery/courier services, the data stored in the database were erased and obtained by the attackers. Personal data relating to 1,362 users, including identity data (name and surname) and contact data (telephone number, address and e-mail address), were affected by the breach, and the attackers demanded a ransom in relation to the compromised personal data. • The Board assessed that saving the management panel password in the browser demonstrated that the data controller had failed to exercise the necessary care and diligence in relation to password security, while the failure to restrict access to the database management software by IP address had enabled unauthorized access and demonstrated that the necessary measures had not been implemented, and accordingly imposed an administrative fine of TRY 250,000 on the data controller pursuant to Article 18/1(b) of the PDPL for failure to implement the necessary technical and organizational measures to ensure data security under Article 12/1 of the PDPL.
Transfer of Data Relating to 31,179 Data Subjects to a Germany-Based IP Address and Publication on the Dark Web Due to a Security Vulnerability in the Customer Management Panel of Sales and Accounting Software Used by a Hosting Company Board Decision dated 21 March 2023 and numbered 2023/412	• A security vulnerability in the customer management panel of the sales and accounting software used by a hosting company was exploited, because of which the data on the main server were transferred in bulk to an IP address located in Germany and published on the dark web. The breach, which was detected approximately six months later, affected 31,179 customers, users and employees. Personal data in the identity, contact, customer transactions and financial categories, as well as e-mail content containing certain passwords, domain name registration documents and credit card information, were subject to the breach. • The Board found that, prior to the breach, the data controller had not used an intrusion detection and prevention system or a solution capable of preventing bulk data downloads and had not implemented two-factor authentication or a strong password policy. It further determined that credit card information contained in log records had not been masked and that unnecessary data had been recorded, meaning that appropriate data masking measures had not been implemented and the principle of data minimization had not been observed. Accordingly, the Board imposed an administrative fine of TRY 350,000 on the data controller for failure to take the necessary technical and organizational measures to ensure data security.

Decision	Details
Use of Customer Contact Information Obtained by Unauthorized Persons for Fraudulent Purposes Board Decision dated 28 December 2022 and numbered 2022/1407	• Unidentified persons unlawfully obtained the telephone numbers of customers of a fashion textile company and requested money transfers on the allegation that enforcement proceedings would be initiated due to undelivered shipments. The incident was detected after a customer notified the data controller. • The Board assessed that it could not be established that the personal data had been leaked from the data controller's systems and that the data in question may have been obtained from the systems of other data controllers, such as e-commerce platforms, cargo companies or financial institutions. It also assessed that the data controller had taken reasonable technical and organizational measures proportionate to the nature of the personal data processed, including penetration testing, three-factor authentication for access to the ERP system, a data breach response plan, confidentiality undertakings and agreements concerning the establishment of data security. Considering also that the data controller made an announcement on its website and social media accounts on the day it became aware of the breach, the Board decided that no further action was required under the PDPL.
Review Conducted Following a Threat E-mail Alleging Unauthorized Access to Personal Data Within the Scope of a Data Breach Notification Submitted to the Board by a Technology Company Acting as the Data Controller Board Decision dated 7 October 2022 and numbered 2022/1087	• Unidentified persons threatened a technology company by e-mail, claiming that they had accessed the company's databases and obtained certain information. In response, the data controller had two independent security firms conduct detailed analyses and penetration tests on its systems. No findings indicating a personal data breach were identified in the examinations, and it was also determined that the sample data provided in the e-mail did not match the personal data stored in the company's systems. • The Board considered that the forensic examination and penetration testing reports prepared by the independent firms did not identify any findings indicating a personal data breach and decided that no further action was required under the PDPL at this stage.

Decision	Details
Compromise of a Senior Executive's E-mail Account and Sending Malicious Content to Customers Board Decision dated 21 July 2022 and numbered 2022/714	• The e-mail account of a senior executive of an agricultural commodities company was compromised, and the attackers used the account to send approximately 1,000 people e-mails appearing to contain fake invoices that redirected recipients to a malicious website. The breach, in which some customers were considered to have been exposed to a phishing attack, was detected 2–3 days later following a warning from a customer. • The Board considered the fact that the number of individuals affected by the breach could not be determined as an indication that the data controller had failed to maintain control over the personal data. It noted that data loss prevention software, advanced authentication mechanisms and systems capable of detecting attacks or anomalies had not been used prior to the breach, and that the breach could not be detected by the data controller due to the lack of regular monitoring of access and log records. The Board also found that the password management policy had not been designed and effectively implemented so as to prevent the use of the same password across different platforms. For these reasons, the Board imposed an administrative fine of TRY 200,000 on the data controller for breach of Article 12/1 of the PDPL due to its failure to take the necessary technical and organizational measures to ensure data security.
Accidental Sharing of Employee Data with a Third-Party Application Board Decision dated 22 May 2025 and numbered 2025/881	• A company accidentally enabled integration with a different application in the tool used to track employees' business travel expenses. As a result, the names and surnames, business e-mail addresses and business telephone numbers of 488 employees were shared with a third-party application company. After identifying the breach, the data controller immediately disabled the synchronization and requested erasure of the shared data. • The Board considered that the relevant employees were immediately informed of the incident, prompt remedial measures were taken following the breach, and the likelihood of adverse consequences for the affected individuals was low. Accordingly, it decided that no further action was required under the PDPL at this stage.
Disclosure of Customer E-mail Addresses to Other Recipients Board Decision dated 12 March 2025 and numbered 2025/536	• In 14 informational e-mails sent to customers by a company manufacturing small domestic appliances, the recipients' e-mail addresses were not concealed, allowing customers to see one another's e-mail addresses. An estimated 500 customers were affected by the breach, and once the data controller became aware of the incident, it initiated steps to recall the e-mails. • The Board considered that the e-mails were recalled after the breach was identified, that only e-mail addresses were affected, and that the likelihood of adverse consequences for the data subjects was low. Accordingly, it decided that no further action was required under the PDPL at this stage.

Decision	Details
Disclosure of Customer Information to a Third Party Due to a Packaging Error by a Data Controller Engaged in the Retail Sale of Ready-to-Wear and Textile Products Board Decision dated 9 May 2024 and numbered 2024/756	• Due to an error by packaging personnel at the warehouse of a ready-to-wear company, a customer's shipment and invoice were delivered to another customer. The personal data affected by the breach consisted of identity data (name and surname), contact data (address, mobile telephone number and e-mail address) and customer transaction data (order information). Only one customer was affected by the breach. • The Board took into account that the data subject had been notified of the breach and that the risk of adverse consequences for that individual was low. Accordingly, it decided that no further action was required under the PDPL at this stage.
Bulk Sending of Employee Data Due to Menu Confusion in a Human Resources Application Board Decision dated 28 September 2023 and numbered 2023/1675	• An employee of an industrial kitchen equipment manufacturer's human resources department selected the bulk sending menu instead of the individual sending menu while issuing an address update notification. As a result, the names and surnames, Turkish ID numbers and address information of 1,522 employees were sent to 1,589 employees. The breach was detected on the same day following feedback from employees of the data controller. • The Board considered that the human error was understandable in the ordinary course of events given the similar design of the relevant menus, that the human factor constitutes the weakest link in information security, that the data controller had provided its employees with adequate information security training, established confidentiality undertakings and disciplinary arrangements, and implemented an appropriate level of technical measures to ensure the security of personal data. Taking into account also that the breach was detected on the same day following employee feedback, the Board decided that no further action was required under the PDPL at this stage.

Decision	Details
Customers Viewing Each Other's Profile Information Due to a Technical Error in a Mobile Application Board Decision dated 21 July 2022 and numbered 2022/707	• Due to a technical error in the mobile e-commerce application of a retail company acting as the data controller, some customers were able to view the names and surnames, telephone numbers, e-mail addresses and masked credit card information of other customers. The breach was identified following a notification from a customer and was remedied within a short period of time. • The Board assessed that the personal data subject to the breach had not been disclosed to the public and that the likelihood of misuse was low, that the confirmed number of individuals affected by the breach was 17 and that no more than 136 individuals could have been affected, and that both the amount of data that could be viewed per individual and the likelihood of misuse of the data were low. The Board also took into account that the data controller had begun investigating the source of the problem in the system before receiving the customer notification, shut down the system shortly after becoming aware of the breach, remedied the technical error and notified the data subjects, and decided that no further action was required at this stage under Article 12/1 of the PDPL.
Exposure of Customer Data Due to a Technical Error on a Clothing Retailer's Website Board Decision dated 19 October 2023 and numbered 2023/1796	• Due to a technical issue arising from the cache configuration within the CDN service provided by the data processor engaged by a clothing retailer, the name and surname, membership information and telephone number of one customer became accessible to an unlimited number of persons on the retailer's website. After being contacted by third parties and receiving a message concerning an order that did not belong to them, the data subject checked their account and discovered that another person had logged into the system using their membership information, changed the address information and placed an order. • The Board stated that the fact that the technical issue originated from the data processor from which services were received did not eliminate the data controller's obligations and that the data controller and the data processor were jointly responsible for taking the necessary technical and organizational measures to ensure data security. It found that the necessary detailed tests had not been carried out before the change was deployed to the live environment and that the update had not been checked and decided to impose an administrative fine of TRY 200,000 on the data controller.
Sending Unsolicited SMS Messages and Making Calls for Advertising and Marketing Purposes Board Decision dated 10 June 2026 and numbered 2026/1183	• A savings financing company recorded the telephone numbers of third parties obtained from its customers under a brand ambassador program and sent SMS messages and made voice calls for advertising and marketing purposes without first informing the data subjects or obtaining their valid explicit consent. • The Board found that the data subject's expression of interest in the campaign during the telephone call and continuation of the conversation did not constitute valid explicit consent and determined that the processing of personal data had commenced before explicit consent was obtained. Accordingly, the Board imposed an administrative fine of TRY 1,000,000 on the data controller.

Decision	Details
Making In-Flight Internet Services Conditional upon Explicit Consent Board Decision dated 15 August 2024 and numbered 2024/1393	• Passengers wishing to use the internet service offered during the flight were asked to provide their surname and seat or ticket number through the internet service provider's portal, and this information was verified through the airline's systems. The internet service provider also requested passengers' explicit consent for this data sharing. • The Board considered the verification process to constitute a transfer of personal data and determined that the airline and the internet service provider acted as separate data controllers in respect of this process. • The Board found that the relevant processing activity could be based on the conditions that it was directly related to and necessary for the establishment or performance of a contract, necessary for the data controller to comply with its legal obligations, and necessary for the establishment, exercise or protection of a right. Accordingly, no separate explicit consent was required for this processing activity. • Despite this, the internet service provider's request for the data subjects' explicit consent was found to be misleading and deceptive, and therefore contrary to the principle of processing personal data lawfully and fairly. The Board consequently imposed an administrative fine of TRY 90,000 on the internet service provider.
Explicit Consent Practices for Security Cameras, Cookies and Advertising and Marketing Purposes Board Decision dated 8 August 2024 and numbered 2024/1361	• The Board examined the practices of a private educational institution concerning explicit consent practices for security cameras, website cookies and advertising and marketing purposes obtained through its contact form. • The Board found that there was no evidence that audio was being recorded through security cameras and noted that the video recording was carried out based on a legal obligation. It therefore decided that no further action was required in this respect. • The Board determined that non-essential analytics cookies used on the website were operated without obtaining users' explicit consent, contrary to the PDPL. • The Board found it unlawful that, in the case of individuals who merely wished to obtain information from the institution, consent to the use of their contact details for advertising, promotion and campaign purposes was obtained under the same single option as the information request. It concluded that making the information service conditional upon explicit consent for advertising and marketing purposes did not satisfy the requirements that consent relate to a specific matter and be freely given. • The Board further found that the obligation to inform had not been duly fulfilled and imposed a total administrative fine of TRY 265,000 on the data controller, comprising TRY 250,000 for unlawful processing of personal data and TRY 15,000 for breach of the obligation to inform.

Decision	Details
Sending Frequent Marketing and Informational SMS Messages Board Decision dated 8 August 2024 and numbered 2024/1350	• An electronic communications operator sent more than 20 SMS messages containing the same or similar content to a subscriber whose contract was due to expire, between 8 May 2023 and 26 July 2023. The messages continued despite the data subject stating during calls with the call center that they were not interested in campaigns or offers. • The Board found that informing the subscriber of the expiry of the campaign and the tariff to be applied fell within the data controller's legal obligations. However, it concluded that sending a large number of SMS messages with the same content at short intervals exceeded the data subject's reasonable expectations and amounted to an abuse of rights. Accordingly, the Board imposed an administrative fine of TRY 100,000 on the data controller. • The Board also reminded the data controller that including an explicit consent text within the agreement concerning the processing of personal data could be misleading for data subjects and could undermine the elements of valid explicit consent, and that it would therefore be appropriate to present the explicit consent text separately from the agreement.
Obtaining Unnecessary Explicit Consent in a Subscription Agreement Board Decision dated 22 February 2024 and numbered 2024/282	• Following a change of address, a telecommunications company requested the data subject to provide their identity document again in connection with the conclusion of a new subscription agreement necessitated by a change in the internet infrastructure. The internet service was terminated after the data subject did not provide the required documents. • The Board found that requesting identity information for the conclusion of the new agreement was lawful on the grounds that the processing was necessary for the establishment of the contract and for compliance with the data controller's legal obligations. The request for erasure of such data was also rejected, as the reasons requiring the processing of the identity information continued to apply. • However, the Board concluded that obtaining separate explicit consent within the subscription agreement, despite the existence of other conditions for processing the personal data, was misleading and deceptive and therefore contrary to the principles of lawfulness and fairness. Accordingly, the Board imposed an administrative fine of TRY 350,000 on the data controller. • The Board also instructed the data controller to remove provisions constituting explicit consent from the agreement, to obtain explicit consent separately from the agreement and the privacy notice where explicit consent is required, and to provide the data subject with a list of the group companies to which their personal data had been transferred.

Decision	Details
Making Access to Live Match Broadcasts Conditional Upon Consent to Receive Commercial Communications Board Decision dated 21 September 2023 and numbered 2023/1610	• An online legal sports betting and games-of-chance platform made access to its live match streaming service conditional upon consent to receive commercial electronic communications. A user who met the other applicable conditions but did not provide such consent filed a complaint with the Board on the grounds that they were unable to use the service. • The Board assessed that making the live streaming service conditional upon consent to receive commercial communications undermined the requirement that explicit consent be "freely given" and that the relevant data processing activity was not based on any of the processing conditions set out under the PDPL. Accordingly, the Board imposed an administrative fine of TRY 250,000 on the data controller for failure to implement the necessary technical and organizational measures to prevent unlawful processing of personal data and decided that the practice should be discontinued and that the Board should be informed of the outcome.
Rejection of a Request for Access to Telephone Call Recordings Board Decision dated 18 April 2024 and numbered 2024/592	• A bank employee requested access to the recording of a telephone conversation with a bank customer, which the employee alleged contained insulting remarks, for the purpose of pursuing legal remedies. The bank rejected the request on the grounds that the recording contained information constituting customer secrets. • The Board assessed that the right to request information concerning personal data also encompasses the right of access to such data and that the employee's request concerned a call recording containing their own personal data, rather than customer secrets. Accordingly, the Board instructed the bank to provide the data subject with both a written transcript and a digital copy of the call recording, after masking the banking transaction data relating to the third party that constituted customer secrets.
Request for Erasure of Information Relating to a Repaid Debt from a Risk Report Board Decision dated 14 March 2024 and numbered 2024/444	• The data subject requested that information concerning a debt repaid in full in 2017 be erased from the Findeks Risk Report. Kredi Kayıt Bürosu AŞ rejected the request, stating that Findeks reports are generated in parallel with the records maintained by the Risk Center of the Banks Association of Türkiye (Risk Center). • The Board determined that Kredi Kayıt Bürosu AŞ acts as the data controller in respect of the Findeks service and that information relating to repaid debts is processed by the Risk Center on the condition that such processing is expressly provided for by law and retained for ten years from the date on which the debt is repaid. • Considering that the data subject's debt had been repaid in 2017, the Board found that the data could continue to be processed and shared with Risk Center members until 2027 and decided that no further action was required under the PDPL.

Decision	Details
Processing of Personal Data by Kredi Kayıt Bürosu AŞ and Request for Erasure Board Decision dated 22 February 2024 and numbered 2024/292	• The data subject alleged that their personal data had been unlawfully processed by Kredi Kayıt Bürosu AŞ, shared with third parties and used for commercial purposes, and that their request for erasure had been rejected. • The Board assessed that the data controller's response, stating that the sharing of data between banks and financial institutions was based on applicable legislation and that data processed through the Findeks platform would be retained for ten years following termination of membership, was clear and sufficient, and decided that no further action was required under the PDPL.
Processing of a Former Employee's Personal Data and Request for Access Board Decision dated 22 February 2024 and numbered 2024/284	• A former employee of a subsidiary of a public institution applied to the Board, alleging that, following the termination of their employment, their personal data had been unlawfully processed in respect of four matters: their corporate e-mail account, the employee and health data held in the Personnel Management System, data transfers and information notice practices. • The Board found that the employee's e-mail account had not been accessed directly after the termination of the employment relationship and therefore decided that no further action was required in this respect. The Board also found that the former employee's e-mails were stored in accordance with statutory retention obligations but considered the failure to include information on this processing activity in the privacy notice to be a deficiency and instructed the data controller to update the privacy notice accordingly. • The Board stated that deactivating the Personnel Management System account after termination of employment did not mean that the personal data had been erased. It therefore instructed the data controller to respond to the data subject's request for erasure of the personal data retained in the system. • The Board further reminded the data controller that access to employees' health data should be limited to people who genuinely need such access and that access rights should be restricted for positions, such as general manager, where access to such information is not necessary.

Decision	Details
Complaint Concerning the Erasure of Personal Data and the Right to Be Forgotten in Relation to a News Article Published in a Newspaper and Still Available in the Newspaper's Archive Board Decision dated 28 December 2023 and numbered 2023/2185	• The data subjects requested the removal from the newspaper's archive of a news article published in 2001, together with their personal data, stating that, despite the considerable time that had elapsed, the article remained accessible in the newspaper's online archive and continued to appear among the top search results when searches were conducted using their names and surnames. However, the data controller failed to respond to the request within the statutory period. • The Board assessed that the inclusion of personal data in the news article fell within the scope of freedom of the press and therefore constituted an exemption under Article 28/1(c) of the PDPL, and that no action could be taken under the PDPL in respect of the request to erase the data from the newspaper's archive. As regards the request to cease displaying the article in search engine results, the Board decided that, within the scope of the right to be forgotten, such request should first be directed to the relevant search engines pursuant to Articles 13 and 14 of the PDPL. The Board also reminded the data controller that applications submitted by data subjects must be responded to within the prescribed period.
Assessment of a Convicted Prisoner's Request for Access to Personal Data under the Statutory Exemption Board Decision dated 20 October 2022 and numbered 2022/1152	• A convicted prisoner held in a penal institution filed a complaint with the Board, stating that their requests for access to and rectification of their file and personal data had not been fulfilled, that correspondence sent by the Authority in sealed envelopes had been opened and delivered with delay, and that their personal data had been shared with other institutions and organizations without their consent. • The Board assessed that the processing activities relating to access to the file and personal data, as well as the opening of the sealed envelope, fell within the scope of the exemption under Article 28/1(d) of the PDPL, as they were carried out in connection with enforcement proceedings. It further decided that the allegation concerning delayed delivery of the correspondence did not fall to be assessed under the PDPL, while the allegation that personal data had been shared with other institutions and organizations without consent could not be assessed on the merits due to the absence of supporting documents.

Decision	Details
Workplace Monitoring Through Security Cameras Board Decision dated 28 March 2024 and numbered 2024/540	• A company installed security cameras in an area where theft incidents had previously occurred and where employees kept their personal belongings, informed employees accordingly, and retained the video recordings for 60 days. • The Board found that the use of cameras was lawful on the basis of the legitimate interest in ensuring workplace security and that retaining the recordings for 60 days was not contrary to the principles set out under the PDPL. • However, the Board instructed the data controller to revise the relevant information notices because the legal basis for processing had not been stated specifically in the privacy notice and the information and explicit consent processes had not been sufficiently separated. • The Board also reminded the data controller that, for applications submitted through an attorney under the PDPL, the power of attorney is not required to contain a specific authorization.
Publication of Election Poll Data Without Sufficient Anonymization Board Decision dated 22 February 2024 and numbered 2024/275	• As part of an election poll conducted by a local media outlet, participants' identity and contact details and voting preferences were collected. The poll results were then published online together with the initials of participants' names and surnames, partially masked telephone numbers and certain neighborhood information. The data controller argued that the data had been masked and that explicit consent had been obtained from the participants. • The Board found that publishing the election poll results in a publicly accessible manner together with data enabling the data subjects to be identified resulted in the processing of political opinion data, which constitutes special categories of personal data. It further determined that, since the text provided to the data subjects did not satisfy the requirements for valid explicit consent, the processing activity lacked a legal basis under Article 6 of the PDPL. Accordingly, the Board imposed an administrative fine of TRY 40,179 on the data controller pursuant to Article 12/1 of the PDPL.

Decision	Details
Processing of Fingerprint Data by a University for Attendance Monitoring in Course Roll Calls Conducted by a University Board Decision dated 8 February 2024 and numbered 2024/197	• A university processed fingerprint data, which constitutes special categories of personal data, for the purpose of monitoring students' attendance. While attendance of students at the Faculty of Law who did not wish to provide fingerprint, data was monitored through manual roll calls, fingerprint-based attendance monitoring was used at the Faculty of Medicine. • The Board considered that, even where explicit consent had been obtained, the processing of fingerprint data, which constitute biometric data, for the purpose of course attendance monitoring was contrary to the principle of proportionality and was not based on a valid legal ground for processing. The Board emphasized that explicit consent obtained from the data subject would not render disproportionate processing of personal data lawful. In this context, the Board decided that the fingerprint-based attendance practice should be discontinued, the fingerprint data currently being processed should be destroyed, and disciplinary provisions shall be applied, pursuant to Article 18/3 of the PDPL, against the persons responsible for taking the necessary technical and organizational measures in accordance with Article 12/1 of the PDPL
Audio Recording Through Workplace Security Cameras Without a Legal Basis Board Decision dated 30 November 2023 and numbered 2023/2007	• Upon an employee learning during litigation that audio recordings had been made through a security camera at the workplace, the Board assessed that video recording was sufficient to ensure physical security and that recording audio in addition was not necessary. • The Board found that the audio recording was not based on any condition for processing provided for under the PDPL, imposed an administrative fine of TRY 125,000 on the data controller pursuant to Article 18/1(b) of the PDPL for breach of Article 12/1 of the PDPL, and decided that the unlawfully processed audio data should be destroyed and the Board informed accordingly.
Sending a COVID-19 Test Result to an Outdated Telephone Number Board Decision dated 19 October 2023 and numbered 2023/1787	• The data subject underwent a COVID-19 test at a stand set up by a healthcare company on a university campus as part of a school event and provided their current telephone number through a form for the test result to be sent. However, instead of being sent to that number, the test result was sent by SMS to an old telephone number belonging to the data subject's uncle, which had been recorded in the data controller's system since 2011. • The Board found that sending the COVID-19 test result to the old number recorded in the system, despite the data subject having provided an up-to-date number, was contrary to the principle of personal data being "accurate and, where necessary, kept up to date," and imposed an administrative fine of TRY 30,000 on the data controller. The Board also decided that the current telephone number should be recorded in the system, the old number belonging to the data subject's uncle should be destroyed and removed from the records, and the Board should be informed of the outcome.

Decision	Details
Processing of Personal Data by a Penal Institution in the Context of Execution Proceedings Board Decision dated 19 December 2024 and numbered 2024/2158	• Collection and disbursement receipts issued by a penal institution for convicted persons and detainees contained personal data such as name and surname, Turkish ID number, prison registration information and information relating to the person depositing the money. • The Board determined that the relevant processing activity was carried out by an enforcement authority within the scope of execution proceedings and, pursuant to the exemption set out under Article 28/1(d) of the PDPL, concluded that the provisions of the PDPL did not apply and that no further action was required.
Obtaining and Using Bank Account Information by an Insurance Company Board Decision dated 8 August 2024 and numbered 2024/1359	• Following a traffic accident, an insurance company obtained the data subject's IBAN information from the policyholder involved in the accident during the submission of a damage notification and subsequently used the same IBAN information to make a payment in connection with a loss-of-value claim arising from the same accident. • The Board found that the IBAN information had been lawfully obtained during the damage notification process and that its subsequent use for the loss-of-value payment relating to the same accident was based on the condition that processing was necessary for the establishment, exercise or protection of a right. Accordingly, the Board decided that no further action was required.
Complaint Concerning the Legal Basis for Processing Personal Data Within the Scope of Library Membership and the Obligation to Inform Board Decision dated 2 November 2023 and numbered 2023/1863	• A person wishing to use a municipal library filed a complaint with the Board, alleging that, during the membership process, personal data which they considered unnecessary for membership had been requested from them without any information being provided. • The Board assessed that, in the case subject to the complaint, the personal data were processed not on the basis of explicit consent, but on the legal grounds that processing was necessary for the establishment or performance of a contract and for the establishment, exercise or protection of a right, and that the obligation to inform had been fulfilled verbally by the library staff and, under the current membership systems, through links to the privacy notice available on the website and e-Government. Taking into account that the data subject's personal data had also been destroyed in accordance with the applicable legislation, the Board decided that no further action was required against the data controller under the PDPL.

Decision	Details
Breach of the Obligation to Inform in the Recording of Call Center Conversations Board Decision dated 26 October 2023 and numbered 2023/1818	• A customer of a company providing alarm and monitoring services filed a complaint with the Board on the grounds that their telephone conversations had been recorded without being informed and without their consent. • The Board found that the conversations had been lawfully recorded within the scope of the establishment, exercise or protection of a right and the legitimate interests of the data controller. However, it determined that the information provided regarding the recording did not meet the minimum requirements of the obligation to inform, imposed an administrative fine of TRY 15,000 on the data controller, and instructed the data controller to duly fulfil the obligation to inform.

Key Contacts

Sevgi Ünsal Özden, LL.M. CIPP/E
Managing Associate and Mediator

sevgiunsal@erdem-erdem.com

Tilbe Birengel, LL.M. CIPP/E
Managing Associate

tilbebirengel@erdem-erdem.nl

Ozan Akman, LL.M. CIPP/E
Senior Associate

ozanakman@erdem-erdem.av.tr

Istanbul
Ferko Signature, Büyükdere Caddesi, No. 175 Kat. 3, 34394, Esentepe - Şişli, İstanbul
+90 212 291 73 83 / +90 212 291 73 82
istanbul@erdem-erdem.av.tr

İzmir
1476 Sokak, No. 2, D. 27, Aksoy Plaza Alsancak, İzmir
+90 232 464 66 76 / +90 232 466 01 21
izmir@erdem-erdem.com

Amsterdam
Office 4.31, Strawinskylaan 457, 1077 XX Amsterdam
+31 (0)20 747 1113
amsterdam@erdem-erdem.nl

ERDEM & ERDEM 40 YEARS