ERDEM & ERDEM

Personal Data Protection Bulletin

2022

Third Quarter

Recent Updates from Turkey

Announcement on the Draft Guideline on Issues to be Considered in Processing of Genetic Data Has Been Published

The Turkish Personal Data Protection Authority **("Authority")** published the Draft Guideline on the Issues to be Considered in the Processing of Genetic Data **("Draft")**, on its website on 24.08.2022.

The purpose for the Draft is to ensure that genetic data are processed in accordance with certain rules and procedures and to raise public awareness on this issue, based on the fact that genetic data are sensitive data that may cause national strategic consequences that could affect the entire society as a result of their processing. Opinions and evaluations were collected until 24.09.2022 and the final version of the Draft Guideline is expected to be published in the coming days.

Guideline on Personal Data Protection in the Banking Sector Have Been Published

The Authority published the Guideline Regarding Best Practices on Protection of Personal Data in the Banking Sector ("Guideline") on 05.08.2022. The purpose of the Guideline is to ensure that the personal data processing activities carried out by the data controller banks comply with the legislation and to provide banks with best practice examples.

You may find the Guideline here (in Turkish) and the client alert regarding the matter here.

Our Recent Related Newsletter Article:

Guidelines on Personal Data Protection in the Banking Sector Published by the Turkish Personal Data Protection Authority

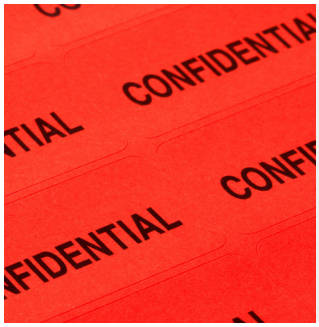
Defne Pırıldar, September 2022

Regulation on the Sharing of Confidential Information Has Been Published

On 11.08.2022, the Banking Regulation and Supervision Agency published Circular No. 2022/1 regarding Explanations on the Implementation of the Regulation on Sharing Confidential Information ("Circular"). The Circular aims to eliminate any hesitations that may arise in the implementation of the Regulation on the Sharing of Confidential Information ("Regulation").

In this context, the Regulation defines confidential data and sets out the scope, form, procedures and principles regarding the disclosure and transfer of bank and customer secrets.

You may find here the Circular (in Turkish) and the client alert regarding the issue **here**.



Our Recent Related Newsletter Article:

BRSA's Circular on Disclosure of Confidential Information Regulation

İdil Yıldırım Günaydın, September 2022

Important Decisions of the Board

The Board's Decision on Processing of 'Hand Geometry' Information to Enter the Building Without Explicit Consent:

In the relevant decision regarding a complaint that allegedly processed palm and fingerprint information obtained through a device called Hand Geometry Terminal without explicit consent, the Board determined that hand geometry data is biometric data. Moreover, it was pointed out that this data can only be processed if the data subject has explicit consent or the processing activity is expressly stipulated in the law. In addition, since processing biometric data, which is of special categories of personal data, without fulfilling the conditions stipulated under Art. 6 of the KVKK is unlawful, the Board decided to impose an administrative fine and ordered that such practice is immediately ceased, the data collected in the past is destroyed. In making this assessment, the Board also considered the number of people affected by the practice.

You can find the summary of the relevant decision here (in Turkish).

The Board's Decision Evaluating That the Application of Special Discounts to the Loyalty Card Does Not Mean the Imposition of Explicit Consent as a Service Condition

In the complaint submitted before the Authority, it is stated that special discounts unique to the loyalty card were applied to some products sold in the store of the data controller, thus special discounts were conditional, the personal data of the customer were requested for membership to the loyalty program and card supply, and explicit consent was imposed as a condition. The Board determined that the possibility of shopping from the stores is not blocked for the persons who do not want to be included in the loyalty card program or do not want to give their explicit consent, and that the products/services within the scope of the loyalty program continue to be sold at non-discounted prices to the customers who are not members of the loyalty program. As a result, the Board decided that offering products/services at a discount with additional benefits within the scope of the loyalty program does not mean the imposition of an explicit consent as a condition.

You can find the summary of the relevant decision here (in Turkish).

The Board's Decision on the Processing of the Personal Data of the Data Subject, whose Employment Contract was Terminated, by the Data Controller Company

It was reported in the complaint petition that when the data subject wanted to apply to the data controller company regarding his/her personal data, the company did not have an application form and did not provide information about the application methods, the clarification obligation was not fulfilled, his/her sensitive personal data was processed without his/her explicit consent, the data controller company used fingerprint and face scanning system, different firms of the group company have branches abroad and when the data subject visited the foreign branch, his/her personal data was transferred abroad without his/her explicit consent and there has been no privacy policy on the website of the data controller company.

The Board assessed that (i) the clarification and explicit consent statements should be issued separately and thus, otherwise clarification is not deemed to be proper, and (ii) since the explicit consent statement regarding the processing of sensitive personal data is presented to the data subject in combination with the employment contract, the explicit consent to the processing of sensitive personal data was not provided on free will. Also, the Board concluded that the processing of fingerprint and face scan data of the data subject is disproportionate with the aim of ensuring the security of the company employees, and that the processing of biometric data by the data controller is not in accordance with the principle of proportionality, one of the general principles of the KVKK, since it is possible to achieve the same purpose with methods such as magnetic card readers and checklists that do not require the processing of biometric data.

You may find the summary of the relevant decision here (in Turkish).

The Board's Decision on Sending the Invoice to the Wrong Recipient Upon an Online Order

In the petition submitted before the Authority, it was reported that a person with the same name as the data subject became a member of the data controller providing services over the internet and placed an order, this person used the e-mail address of the data subject while placing the order, the data controller sent the invoice for the order to the data subject without checking and confirming the accuracy of the e-mail address

while membership application process. The Board took into account that the data controller caused the processing of the e-mail address of the data subject, who was not a party to the distant sales contract, without establishing a confirmation mechanism for the recipient groups to which the invoice will be sent, and indirectly disclosed the information of the sender and recipient in the invoice to the data subject, and evaluated that the data controller did not fulfill its security obligations arising from the KVKK. Accordingly, it was ruled that the said processing activity was not based on any processing conditions in Art. 6 of the KVKK and that an administrative fine should be imposed.

In the decision, it was also emphasized by the Board that the KVKK has priority over the General Data Protection Regulation of the European Union in terms of the aforementioned event and it is necessary to comply with the KVKK first.

You may find the summary of the relevant decision here (in Turkish).

The Board's Decision on Disclosure of the Telephone Number of Data Subject to Third Parties by a Bank's Call Center

In the complaint submitted before the Authority, it was stated that the card of a third party was found by the data subject in the ATM of the bank, then the call center of the data controller bank was contacted; during the call, the call center official suggested to collect the card from the data subject by sharing the phone number with the third-party cardholder. The data subject did not consent to this solution proposal. However, in the following hours, it was understood that the cardholder sent a message to the data subject via his/her personal phone number and that the processed data was transmitted to the cardholder without the explicit consent of the data subject.

The Board decided that when the bank communicated with the caller through the call center, the KVKK disclosure text was presented to the caller, and at the same time it is seen that the data subject checked the box *"I have read and understood the Information made within the scope of the Law on the Protection of Personal Data"* while making an application on the website of the data controller.

On the other hand, the disclosure of the data subject's data to a third party is in violation of the KVKK; the Board subjected the data controller bank to administrative fines.

You may find the summary of the relevant decision here (in Turkish).

The Board's Decision on the Usage of Personal Data, Obtained for Patient Registration Purposes, by the Data Controller for Another Purpose Such as Sending Commercial Electronic Messages Without Obtaining Explicit Consent

In the petition submitted before the Authority, it was stated that (i) a message with commercial content was sent to the e-mail address by the data controller operating in the health sector, and this situation constitutes a violation of Art. 6/1 of the Law on the Regulation of Electronic Commerce No. 6563 which provides that *"Commercial electronic messages can only be sent to recipients with their prior consent..."*, (ii) explicit consent was not obtained for the processing of personal data and special conditions were not met. The Board evaluated that the obtaining of the contact information of the data subject or his/her companions during the opening of a patient record is not in violation of the KVKK, but the use of medical information for commercial purposes constitutes a violation.

You may find the summary of the relevant decision here (in Turkish).

The Board's Decision on the Establishment of a Blacklist Program by Software Developers and Sellers of Car Rental Programs

In the complaint received by the Board, it was stated that car rental companies using car rental software keep all the data they obtain about their customers on this software, and that other car rental companies using the same software can view the personal data of the relevant customers from the blacklist pool contained in the application without their consent.

With the said decision, the Board first evaluated the data controller characteristics of car rental software companies and car rental companies in detail and determined some criteria for the determination of the data controller. When the case at hand is considered, although there is a nonliability clause in the contracts, the software companies were deemed as the data controller in case they decide how to transfer the data, which is recorded by the car rental companies through the usage of the software, from one organization to another (which car rental companies can view the black list) within the scope of their commercial activities. As a result, it was decided that the companies that produce and sell car rental software act as joint data controllers with the car rental com-

panies and that the parties are instructed to destroy the processed personal data. Since the concept of joint data controller is not included in the KVKK, the Decision in question is considered important.

In addition, the Board stated that the fact that the evaluations and comments, which were made by car rental companies about their customers in the database, constitutes disclosure of customer secret (trade secret) and personal data.

You may find the summary of the relevant decision here (in Turkish).

The Board's Decision on the Processing Personal Data of Employees by the Liaison Office in Turkey of a Data Controller Resident Abroad

The complaint petition submitted before the Board relates to the liaison office in Turkey of the data controller residing abroad. The main allegations in the complaint petition are as follows; (i) the liaison office requested criminal record, health report, chest X-ray report, blood type certificate, copy of driver's license, copy of marriage certificate and copy of identity cards of family members and these documents were submitted by the data subject, (ii) requesting the identity card information of family members contradicts with the general principles of the law, (iii) since the data controller is resident abroad, the personal data of the data subject may also have been transferred abroad.

The Board stated that the office in Turkey is a liaison office that does not carry out commercial activities, does not have a legal personality, and only engages in "Communication and Information Transfer" activities. Thus, it is concluded that the employer of the data subject is not the liaison office but the data controller which is the company that is resident abroad.

Since it is understood that the personal data of the data subject is obtained by the data controller residing abroad in accordance with the law of the resident country within the scope of the employment contract, that the personal data of the data subject must be processed abroad for the performance of the employment contract and the explicit consent of the data subject is obtained, it has been determined that the explicit consent obtained from the data subject is lawful.

You can find the summary of the relevant decision here (in Turkish).

Recent Developments from the World

A Record Fine by Irish Data Protection Authority for Instagram

On 15.09.2022, the Irish Data Protection Authority **("DPA")** decided to issue 405 million Euro of fine to Instagram (Meta Platforms Ireland Limited) following the European Data Protection Board's **("EDPB")** decision dated 28.07.2022. The decision is related to Instagram's public disclosure of email addresses and/or phone numbers of children that use Instagram's business account feature and a public-by-default setting for personal Instagram accounts of children. This fine is important since it is the second highest fine since the entry into application of the General Data Protection Regulation **("GDPR")**, and the first EU-wide decision on children's data protection rights.

You may find the announcement on the EDPB's official site here.

Italian Data Protection Authority Fines Unicredit S.p.A.

Italian Data Protection Authority **("DPA")** imposed 70,000 Euro administrative fine on the controller and ordered to grant the access request by the data subject. The DPA concluded that the reply by Unicredit S.p.A. regarding the request for access lacks substance as the filling out of a form is a prerequisite for any reply. Moreover, it was established that Unicredit S.p.A. discarded access requests that were submitted without using the given form. The DPA concluded that the right of access to one's personal data and right to be informed are mutually related.

You may find the announcement on the EDPB's official site here.

South Korea Data Protection Authority Fines Google and Meta

On 14.09.2022, South Korea Data Protection Authority **("DPA")** imposed a fine of approximately 50 million Euro on Google LLC and a fine of approximately 22 million Euro on Meta Platforms, Inc. clearly for not informing their users and not obtaining their prior consent when collecting and analyzing behavioral information.

You may find the relevant news here.

The Law Commission Published Consultation Paper on Digital Assets

Upon the UK Government's request to make recommendations for reform to ensure that the law is capable of accommodating both crypto-tokens and other digital assets in a way which allows the possibilities of this type of technology to flourish, the Law Commission published a consultation paper on 18.07.2022. The proposals presented in the paper aim to support transactions that involve digital asset technology by protecting the competition and the dynamics of the law.

You may find the announcement here.

Volkswagen Fined 1.1 Million Euros for GDPR Violations:

On 26.07.2022, the Lower Saxony data protection authority **("DPA")** announced that it has decided to impose 1.1 million Euro of fine on Volkswagen due to the GDPR violations. The DPA stated that Volkswagen has connected cameras to the test vehicle in 2019 to record the surrounding traffic situation for error analysis while testing the driving assistance system; however, it is concluded that Volkswagen violated data protection regulations on the grounds that other drivers who could be recorded were not informed, that an impact assessment was not made prior to the test drive, and that a processing agreement was not signed with the company that made the test drive.

You may find the relevant announcement here (in German) and the news here.

The Dutch Council of State Discusses Whether Commercial Interest Constitutes A Legitimate Interest:

On 27.07.2022, the Dutch Council of State **("Council")** confirmed that the Dutch Data Protection Authority **("DPA")** gave a wrong interpretation of the concept of legitimate interest and wrongly imposed a 575,000 Euro fine on VoetbalTV; however, did not answer clearly whether purely commercial interest may be considered as a legitimate interest within the GDPR. On the other hand, the EU Commission also stands distant to the DPA's strict legitimate interest interpretation and suggests that purely commercial purposes, such as maximization of profits, would not be considered a "legitimate interest". It seems

that the Council embraces a similar approach and shares similar concerns.

You may find the new regarding the decision here.

Data Protection Reforms by Russia

In July 2022, the Russian Parliament and the President of the Russian Federation adopted the law that includes amendments to the existing law on personal data in terms of its scope of application, cross-border data transfers, breach notifications, additional guarantees for data subjects.

You may find the news regarding the law here.

The Final Version of the Measures for Security Assessment of Data Exports by CAC

Cyberspace Administration of China **("CAC")**, published the final version of the Measures for Security Assessment of Data Exports on 07.07.2022. Pertaining to Art. 40 of the China's Personal Information Protection Law **("PIPL")**, the personal information handlers and critical information infrastructure operators to export personal information abroad must first pass a security assessment organized by the State Cybersecurity and Informatization Department. Those measures entered into force on 01.09.2022.

You may find the relevant news here.

The Statement of the European Data Protection Board Regarding Data Transfers to the Russian Federation:

The EDPB states that Russia is no longer a contracting party to the conventions and protocols concluded within the framework of the Council of Europe, therefore Russia will not benefit from an adequacy decision by the European Commission as per Art. 45 of the GDPR, and consequentially, data transfers to Russia must be carried out by using one of the mechanisms under Chapter V of the GDPR. Following the Schrems II ruling of the European Court of Justice, and the EDPB Recommendations on supplementary measures, data exporters should assess if there is anything in the law and/or practices in

force in Russia that may have a negative impact on the effectiveness of the appropriate safeguards.

You may find the press release here.

French Data Protection Authority Imposed 60 Million Euro Fine to the French Company Criteo for Non-Compliance:

As a result of multi-year investigation, the French Data Protection Authority **("CNIL")** imposed 60 million Euros to Criteo. The fine stems from the investigation of a 2018 complaint into Criteo's data processing practices related to targeted advertising and user profiling.

You may find Criteo's press release here.

CNIL's Checklist for Data Controllers Creating Health Data Warehouses:

Health data warehouses are databases intended to be used in particular for the purposes of research, studies or evaluations in the field of health. On 28.09.2022, a checklist for personal data processing activities carried out within the scope of establishing health data warehouses was published for those responsible for these sensitive databases. The checklist helps data controllers determine whether they comply with the standard that was approved in October 2021 which simplifies the procedures and provides a strict legal and technical framework. If one of the answers within the scope of the checklist is negative, the data controllers must request a special authorization from the CNIL.

You may find the press release here (in French), and the news here.

UBEEQO International Has Been Fined By CNIL

CNIL imposed a 175,000 Euro fine on Ubeeqo International on the date of 07.07.2022. Ubeqoo, which operates as a car rental service provider was found to be collecting customers' geolocation data constantly storing that data for an excessive period, and thus violated GDPR. CNIL highlighted that geological data is sensitive data and it can

only be collected where it is absolutely necessary for.

You may find the press release regarding the decision here.

35 Million Euro Fine regarding Amazon Was Uphold

French Council of State, uphold the decision of the CNIL, which imposed 35 million Euro fine against Amazon for the use of cookies without consent, that constitute a cookie violation under the GDPR.

Amazon's violations from regarding using cookies without consent and not informing users of the application.

You may find the press release regarding the decision here (in French), and the news here.

Belgium Data Protection Authority's Decision on Personal Health Information Disclosed:

In the decision, the Belgium Data Protection Authority **("DPA")** concluded that the public authority violated GDPR. The decision is related to the sharing of an employee's health data in an HR meeting while the employee is absent, recording this data to the minutes and storing this minute on a server that other employees can view. The DPA, stated that communicating an employee's sensitive health data to employees when it is not required and recording them to the minutes cannot be considered as a "lawful processing".

You may find the news regarding the decision here.

US and UK's Joint Statement on the "Data Access Agreement":

With an intention to bring into force a data access agreement to prevent and combat with serious crimes on 03.10.2022, the US and the UK have published joint statement on 21.07.2022. The Agreement will empower investigators of each country regarding the access to data while combatting with serious crimes.

You may find the press release regarding the agreement here.

Digital Markets Act and Digital Services Act Have Been Adopted

The Digital Markets Act **("DMA")** and Digital Services Act **("DSA")** have been adopted on 05.07.2022. DMA and DSA are the first comprehensive rulebook related to online platforms that have become an integral part of our daily lives. The mentioned rules will be applicable within the EU market and they aim to make the digital area safer and more open where the fundamental rights should be respected.

You may find the press release and further information regarding the issue here.

The Decision by the Baden-Württemberg For Data Transfers Outside of the EU:

The Baden-Württemberg Procurement Chamber issued a controversial decision (decision dated 13.07.2022 - Ref. 1 VK 23/22). It is of the opinion that the mere possibility of accessing data should be regarded as an actual data transmission and there was an unlawful transfer of data to a third country. The relevant decision, which the term "Transfer" was interpreted broadly by The Procurement Chamber, is not binding since it was reversed by Karlsruhe Higher Regional Court.

You may find the relevant news here.

The UK's National Cyber Security Centre Published Machine Learning Security Principles:

The National Cyber Security Centre, the UK's cyber security agency has recently released a new set of machine learning security principles to support the public sector and large organizations. They aim to help those developing, deploying, and operating a system with a machine learning ("ML") component and to address potential vulnerabilities in the ML systems.

These principles are not a comprehensive assurance framework to grade a system or workflow, and do not provide a checklist. Instead, they provide context and structure to

help scientists, engineers, decision makers and risk owners make educated decisions about system design and development processes, helping to assess the specific threats to a system.

You may find the announcement of the agency here.

Swiss' New Data Protection Law Is Adopted:

Swiss Federal Council adopted Data Protection Ordinance as well as the Ordinance on Data Protection Certifications and confirmed that the Ordinances together with the revised Data Protection Act. They will enter into force on 01.09.2023.

You may find the relevant code here.

Key Contacts

Mert Karamustafaoğlu
Partner, Competition and Compliance Leader

mertkaramustafaoglu@erdem-erdem.av.tr

Sevgi Ünsal Özden
Managing Associate

sevgiunsal@erdem-erdem.com

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

IZMIR

1476 Sokak, No. 2, D. 27, Aksoy Plaza,
Alsancak, İzmir

+90 232 464 66 76
+90 232 466 01 21

izmir@erdem-erdem.com

www.erdem-erdem.av.tr