

THE

Gökçe

Fine PRINT

August 2022

105

SUMMARIES OF PERSONAL DATA PROTECTION BOARD'S RECENT DECISIONS



**Guideline on Data Protection
in the Banking Sector**

**Developments in Remote
Healthcare Information System**

**A New Era for Domain
Names with ".tr"
Extension: TRABIS to be
Launched Soon**

Summaries Of Personal Data Protection Board's Recent Decisions

We compiled below some of Personal Data Protection Board's (**Board**) recent decisions within the scope of Personal Data Protection Law (**Law**) and secondary legislation.

Decision on processing of the data subject's "hand geometry" information by the data controller without obtaining explicit consent for entrances to the service building of an enterprise

Data subject has filed a complaint with the Board, alleging that palm and fingerprint information was scanned by the company authorities to enter the service area while registering to the enterprise, and that it was against the Law to scan the palm and fingerprint without his/her explicit consent.

Within the scope of the investigation initiated on the subject of the complaint, the data controller stated that a device called "hand geometry terminal" is used at the enterprise entrance to recognize the identity of registered subscribers, and that this device records the "hand geometries" of the people in the system, unlike fingerprint or palm prints. It has been argued that with this device, only the upper part of the hand is scanned, the hand geometry does not have a personal characteristic and the system is not infallible so that the data processed cannot be considered biometric data.

Emphasizing the name of the device used by the data controller, which is "biometric hand terminal", Board decided that biometric data is processed based on the fact that **(i)** the device 3D scans the hand and fingers from 31.000 points and analyses all the characteristics of the hand, **(ii)** the margin of error is less than 1 in a hundred trillion, and **(iii)** in a decision of the Council of State hand geometry has been accepted as biometric data. Accordingly, it has been decided to impose an administrative fine of 100,000 TRY on the data controller who processes biometric data of the data subject without any processing conditions.

You can reach the full text of the decision [here](#) (*Only available in Turkish*).

Decision on processing of the data subject's personal data by data controller operating in the health sector for the purpose of sending commercial electronic message without the explicit consent of the data subject

In the event subject to the decision, data processing has been carried out by sending a commercial message to the e-mail address of the data subject by the data controller operating in the health sector. Upon the complaint of data subject, an investigation was initiated against the data controller.

The data controller argued that the data processing activity in question was carried out for purpose of performance of the contract between the data subject and the hospital. Also, provisions of the Private Hospitals Law and the Fundamental Law on Healthcare Services are referred as the legal reason for data processing. Regarding the related commercial e-mail content, it was stated that it was sent without the consent of the data subject due temporary lack of coordination between the units.

Since the personal data subject to the decision was obtained from the data subject while the patient was registered, Board has determined that the data processing conditions have been met at this stage. However, Board stipulated that the contact information regarding the commercial electronic message has been used for marketing purposes, not for medical purposes, and that personal data has been processed by sending a notification for advertising and marketing purposes by the data controller without any existent data processing conditions. As a result, it was decided to impose an administrative fine of 100,000 TRY against the data controller who processed data unlawfully.

You can reach the full text of the decision [here](#) *(Only available in Turkish)*.

Decision on processing of the data subject's data and establishment of a blacklist program that ensures the sharing of this data between car rental companies by car rental software producer and vendor companies

Board has received notices about car rental software producer and vendor companies, which stated that the car rental companies record all the data they have obtained about their customers through the software offered by software companies, and other companies using the same software were able to see the relevant customers' personal data from the blacklist pool in without the customers' consent.

The Board initiated an ex officio investigation regarding the aforementioned notice. In this context, Board determined the customers of car rental companies to be the target group whose personal data has been collected, and car rental companies and software companies as "joint data controllers". It has been determined that software companies deciding which car rental company will receive the personal data of the target audience exceeds their authority as data processor and thus, they can be defined as data controller.

In addition, it has been determined that the software companies are providing their services via cloud computing in the form of a SaaS (Software as a Service) over the online network. In this context, supporting the joint data controller status of software companies, it has been underlined that the management of the database and software is in the control of software companies. Also, the fact that car rental companies' software management authorities are limited to the content and it is not possible for them to make changes in the software is highlighted.

In the light of this, Board concluded that with the blacklist program software companies, which are the joint data controllers, process data and this activity has no legal basis. Also, it has been evaluated that the inability to predict which car rental company gets or able to get the data constitutes a violation of the general principles of data processing and data transfer. Thus, Board decided to instruct the data controllers examined on the destruction of the relevant personal data processed in accordance with the relevant legislation.

You can reach the full text of the decision [here](#) *(Only available in Turkish)*.

For further information please contact us at info@gokce.av.tr

Decision on unlawful processing of the personal data of the data subject by the data controller company whose employment contract has ended

In a complaint filed to Board, it has been alleged that the data subject's personal data was unlawfully processed by the data controller company with which employment agreement was terminated. Data subject requested the Board to take necessary actions by alleging that the company did not fulfill its obligation of disclosure, that sensitive personal data was processed without his explicit consent and adequate security measures were not taken.

In the examination, Board determined that the privacy policies and explicit consent texts in the employment contract lacked minimum requirements and that these texts were not signed by the data subject. For this reason, it was stated that the informing obligation of data controller was not fulfilled properly.

As for the process of sensitive data with a fingerprint and face scanning system, Board has stated that is not based on free will since explicit consent text is presented with employment contract and there is no option to start to work without signing employment contract. Furthermore, stating that the principle of proportionality is not met, Board has emphasized that the security aimed by the data controller using this system can also be ensured with applications such as magnetic card reader and checklist. In this context, the Board decided to impose an administrative fine of 125,000 TRY on the employer company that does not fulfill its obligations as a data controller.

You can reach the full text of the decision [here](#) (Only available in Turkish).

Guideline on Data Protection in the Banking Sector Has Been Published

"Guideline on Good Practices regarding the Protection of Personal Data in the Banking Sector" (**Guideline**) has been published by Turkish Data Protection Authority (**Authority**) on 5 August 2022.

As part of the preparation process for the Guideline, working groups were formed within the Banks Association of Turkey with the aim to shed light on questions and uncertainties by cooperating with the actors within the sector. Considering the fact that intense personal data was being obtained by banks during this preparation process, the need to share good practice examples enabling the banks to comprehend their liabilities became evident.

Guideline includes detailed explanations on the protection of personal data in the banking sector and sector-based examples of good practices.

Significant aspects outlined in Guideline are as follows:

- The distinction between the data controller and the data processor, which has been frequently mentioned in the legislation, decisions and Authority's other guides, has been discussed in further detail in Guideline. Scenarios

For further information please contact us at info@gokce.av.tr

where banks could be data controllers or data processors were shared. In regard to support services processes, which comprise a large part of banking applications, different examples were given, such as the title of the service provider and the bank, and how to determine the data controller in terms of open banking services which will be newly implemented.

- The elements recommended to be included in the data processing agreement to be made between the persons having the title of data controller and the data processor in the banking sector were explained.
- Lawful grounds for processing personal data were evaluated and illustrated according to different scenarios that may arise in the banking sector. For example, it was illustrated that the explicit consent of the data subject is not required in case; the necessary information and documents are provided for risk analysis and assessment and follow-up of the creditors, and in cases of making criminal record inquiries to determine whether there is a check ban on the persons requesting checkbooks.
- Instances of good practices specific to various channels such as branches, ATMs, mobile banking, and SMS were included in scenarios requiring explicit consent.
- It was stipulated that explicit consent is not required for the processing of personal data, when there is an exception to the confidentiality obligation as per Article 73 of the Banking Law, which regulates confidential information, and the Regulation on Sharing Confidential Information.
- In relation to the transfer of data processed within the scope of Article 73 of the Banking Law; the distinction between the general norm and special norm was applied to the Turkish Data Protection Law (**Law**) and Article 73 of the Banking Law. It was emphasized that Law would not be applied in data transfer activities within the scope of this article since it was already governed by Article 73 of the Banking Law which prevailed as a special norm over the general norm contained in Law. Since the relevant provision of the Banking Law is frequently encountered by everyone in practice, the clarifications provided here are important.
- References were made to the previous decisions of the Authority and Constitutional Court on legitimate interest balance testing in data processing activities regarding legitimate interests of the data controller. In this context, it was emphasized that the purpose, proportionality and necessity of data processing should be evaluated and a legitimate interest balance test should be performed in each data processing activity based on the legitimate interest of the data controller.
- Sector-based examples were given for special categories of personal data processed by banks. As a matter of fact, in critical processes run by banks, such as identity confirmation, processing activities of special categories of personal data are carried out intensively. The importance of explicit consent in relevant situations and the obligation of informing the data subject under all circumstances was emphasized in Guideline.
- Information on domestic and international data transfers was explained and discussed in detail within the framework of banking practices. It was reminded that under Law the provisions of other laws regarding the transfer of personal data remained reserved. Information that is construed as customer secret as per Article 73 cannot be shared with or transferred to third parties in the country and abroad without a request or instruction from the customer, except for the cases that are exempted from the confidentiality obligation specified in the same article. In this context, it was underlined that even if the explicit consent of the data subject is available pursuant to Law, "customer's request or instruction" is required for transfers within the scope of Article 73 of the Banking Law.

Guideline sheds light on personal data processing activities in the banking sector. It is crucial for banks to take the

For further information please contact us at info@gokce.av.tr

Guideline as a basis while shaping their personal data practices.

You can reach the full text of the Guideline [here](#) (Only available in Turkish).

Developments in Remote Healthcare Information System

Regulation on Delivery of Remote Healthcare Services (**Regulation**) was published in the Official Gazette on 10 February 2022 by Ministry of Health (**Ministry**).

Regulation regulated the procedures and principles regarding the scope of remote healthcare services, licensing of the facilities to provide these services, development of remote healthcare information systems and auditing. We had already evaluated the changes brought by the Regulation in detail in our TFP February 2022 issue. You can access our article on Regulation by clicking [here](#).

One critical development introduced by the Regulation was the requirement to provide remote healthcare services only through systems either (i) generated by Ministry or (ii) generated by third parties but approved and registered by Ministry. The minimum elements required to be included in system were announced by the Ministry on its website, you can find it [here](#) (Only available in Turkish).

Registered remote healthcare information systems are also announced on Ministry's website as of 8 August 2022. You can reach the systems already announced [here](#) (Only available in Turkish).

A New Era for Domain Names with “.tr” Extension: TRABIS to be Launched Soon

ITCA, (Information Technologies and Communications Authority) has recently announced that all necessary works relating to the management and allocation of domain names with the extension “.tr” have been completed and that ".tr Network Information System" (**TRABIS**) will be activated on 14 September 2022 to oversee this management.

With the activation of TRABIS, certain provisions contained in Internet Domain Names Regulation, Internet Domain Names Communiqué and Internet Domain Names Dispute Resolution Mechanism Communiqué, which had not previously entered into force, will now enter into force. Pursuant to these regulations, domain names with the extensions “net.tr”, “org.tr” and “com.tr” will be allocated in the order of priority based on their respective application date, under the “*first come, first served*” principle, without any documents required. Another significant change is the introduction of an alternative dispute resolution mechanism to the courts for the disputes concerning domain names with “.tr” extension.

In conclusion, activation of TRABIS heralds a new era in domain names with “.tr” extension. Expanding the domain name market in Turkey, making our country code extension a global brand, and resolving domain name disputes immediately and easily are just a few of the goals targeted with TRABIS.

You can find the announcement of ITCA regarding the launch of TRABIS [here](#) (Only available in Turkish).

For further information please contact us at info@gokce.av.tr

Answers. Not theories.

Gokce Attorney Partnership

Editors:



Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr



Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr



Elif Aksöz
elif.aksoz@gokce.av.tr



Yağmur Yollu
yagmur.yollu@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33

The Fine Print is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to receive further information, please contact Gokce Attorney Partnership. No content provided in The Fine Print can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Fine Print was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.