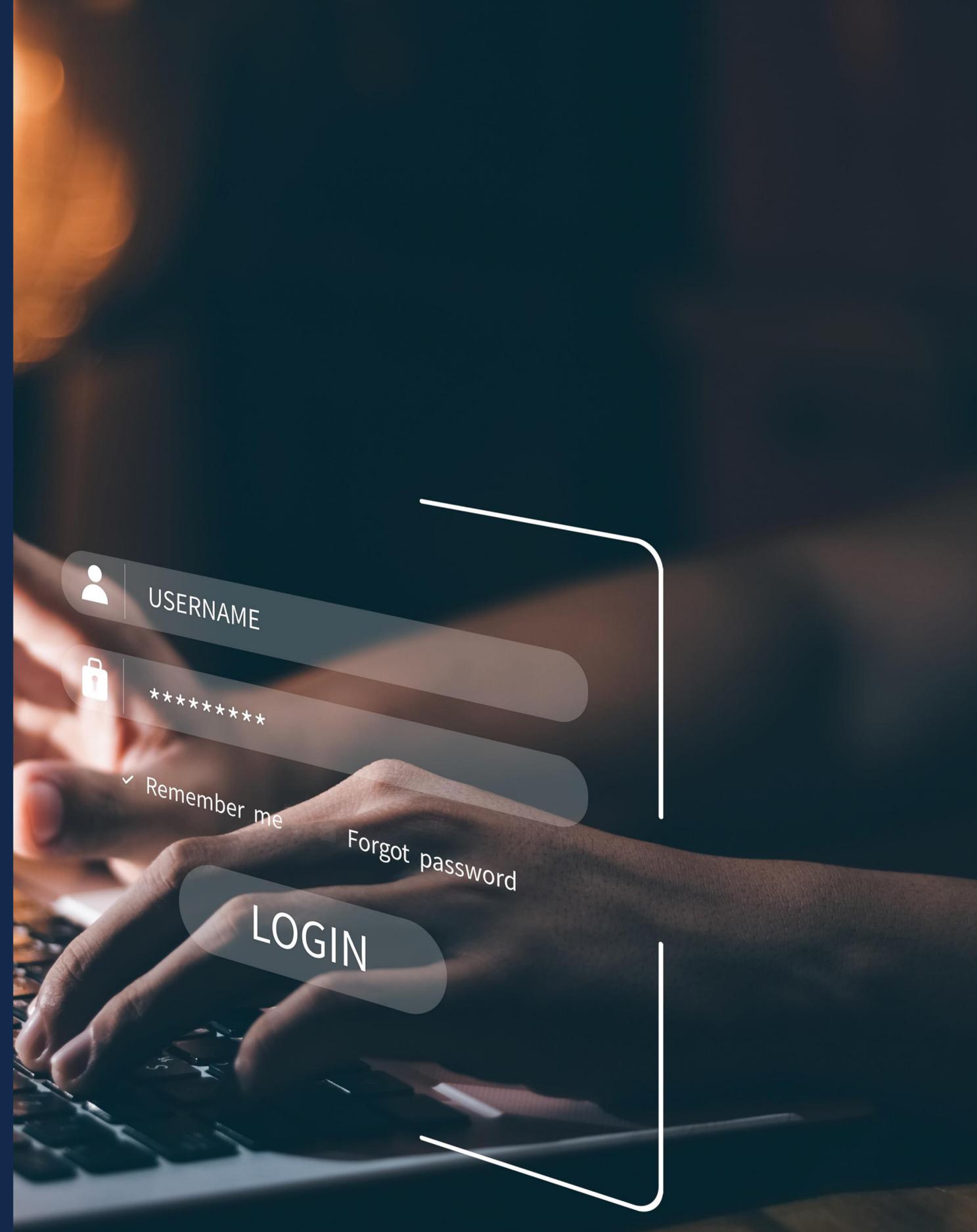


HIGHLIGHTS OF “THE GOOD PRACTICE  
GUIDE FOR BANKING SECTOR”  
RELATING TO THE PROCESSING OF  
PERSONAL DATA IN THE BANKING  
SECTOR



---

## Which Topics Does the Guideline Cover?

---

- Evaluations regarding the Data Controller – Data Processor
- Evaluations regarding the Conditions for Processing Personal Data and Explicit Consent
- Evaluations regarding the Special Categories of Personal Data
- Evaluations regarding the Transfer of Personal Data in the Country
- Evaluations regarding the Transfer of Personal Data Abroad
- Evaluations regarding the General Principles in the Law on The Protection of Personal Data No: 6698 (“PDP Law”)
- Evaluations regarding the Liabilities of the Data Controllers (Obligation to Inform)

---

## Conclusion

---

# Which Topics Does the Guideline Cover?

Banks have been processing personal data intensively through various channels within the scope of banking activities. Personal data is mostly processed for specific purposes under the regulations. However, there was a need of a guidance for the protection of personal data so that banks could stay in accordance with the PDP Law and related regulations. Therefore, the Banking Sector Good Practices Guide (“Guide”) was published by the Personal Data Protection Authority (“Authority”) in July 2022 to help navigate banks by presenting good practices related to processing personal data.

You may access the relevant Guide [here](#).

# 1

## Evaluations Regarding the Data Controller – Data Processor

The “Data controller” is a natural or legal person who determines the purposes and means of processing personal data in compliance with the PDP Law. Banks could be a data controller or a data processor within the scope of the data processing activities they conduct. For instance, Banks could be a data controller within the scope of banking activities related to Article 4 of the Banking Law No: 5411 (“**Banking Law**”).

### a. Data Processing Agreement (DPA) Between the Data Controller – Data Processor

Bankacılık ekosisteminde veri sorumlusu ile veri işleyen arasında akdedilecek sözleşmelerin de KVKK’ya uygun bir şekilde düzenlenmesi gerekiyor. Bu kapsamda, bankaların; destek hizmetleri, iştirakleri ve bağlı ortaklıkları ile açık bankacılık ve bankanın acente sıfatıyla hareket ettiği sözleşmelerde, sözleşmenin taraflarının veri işleyen ya da veri sorumlusu olarak hareket edip etmediklerinin dikkate alınması gerekiyor. Sözleşmelerin bu ayrım göz önünde bulundurularak kurgulanması gerekiyor

### b. Support Services

The Guide defines support services as cargo and courier companies that provide services to the banks as data processors within the scope of PDP Law. Support services could be considered as data controllers in cases where they use personal data transferred from banks for their own interest.

### **c. Affiliates and Subsidiaries**

If banks provide services to their subsidiaries based on Banking Regulation and Supervision Agency (“**BRSA**”) permission, an evaluation should be made by considering each service provided and the data controller-data processor titles of the parties should be determined.

### **d. Open Banking**

The Guide also focuses on banks’ open banking activities. Open banking is defined as “an e-distribution channel where customers or parties acting on behalf of customers can perform banking transactions or give instructions to the bank to perform their banking transactions by remotely processing financial services offered by the bank by means of APIs, web services, file transfer protocols, etc.”. With these channels, customers could remotely access the financial services offered by the bank and perform banking transactions or they can give instructions to the bank for realization. Within the scope of open banking, personal data could be processed by providing banking services to the data subjects processed by the bank for the purposes of providing banking services to the data subjects and by a third-party provider in order for them to benefit from banking products and services. Certain categories of personal data can be processed by the Bank through the transfer of personal data to the third-party provider and simultaneously with the third-party provider's recording of these data in its own system.

### **e. Agent**

In cases where banks act as agents, banks are authorized to perform insurance agency and private pension intermediary services. In cases where insurance contracts are mediated on behalf of insurance companies as agents, banks can only have the title of data processor since they are the ones who carry out the contract preparation work before the contract is signed and assists in the implementation of the contract and the payment of compensation. In addition to being a data processor, banks are also responsible to take technical and organizational measures to ensure personal data security. In cases where banks act as an agency, banks that process data can only perform these activities if the data controller is assigned by the insurance company, within the scope of fulfilling the obligation of disclosure and obtaining explicit consent.

## 2 Evaluations Regarding the Conditions for Processing Personal Data and Explicit Consent

The Guide contains evaluations regarding the need to obtain explicit consent in cases where at least one of the conditions, which are considered as personal data processing conditions and legal compliance, cannot be met. In addition to this explanation, it is discussed that the scope and limits of banking activities are strictly determined by legislation and many personal data processing activities will already be carried out within the scope of personal data processing conditions.

The guide presents examples of good practice within the scope of obtaining explicit consent by banks. Explicit consent in the banking ecosystem can be obtained by physical and electronic means through channels such as branches, ATMs, internet/mobile banking, call centers, SMS, and e-mail. Also, in the Guide it is pointed out that convenient tools and methods, which are accepted as permanent data storage, can be used to provide proof, considering that there is no requirement for express consent to be in written form and that the proof of explicit consent belongs to the data responsible bank.

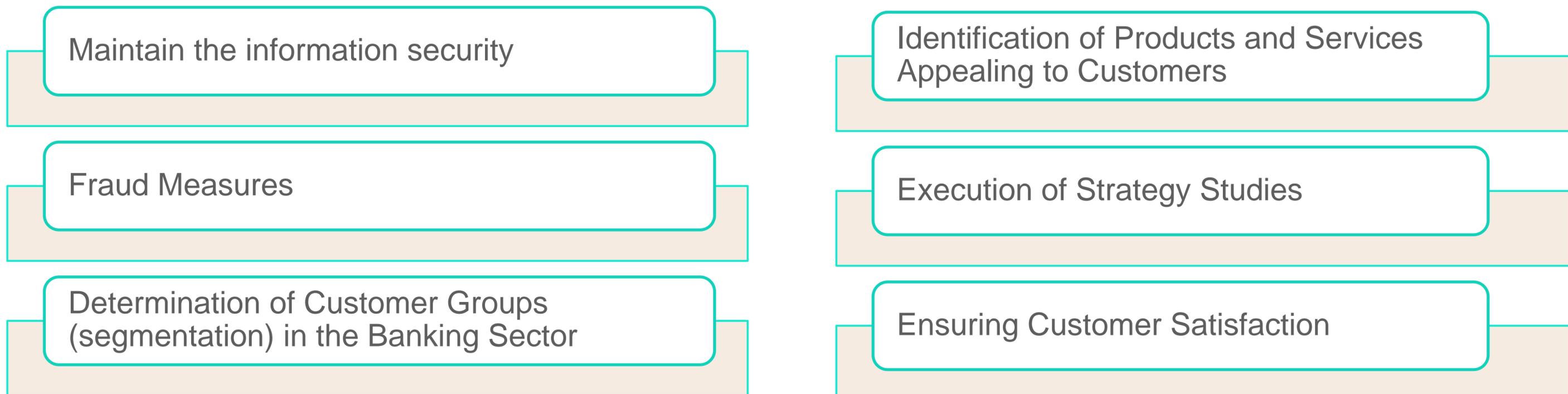
The Guide discusses data processing conditions that are provided by laws and compliance with a legal obligation to which the data controller is subject to. If one of these two personal data processing conditions is present, explicit consent is not required for the personal data processing activity. The Banks risk assessments after loan applications, sharing information in some audits specific to the banking sector, check prohibition query, identification, etc. are shown could be examples in this context. The Guide also points out to two legislations related to expressly stipulated laws which are the Banking Law and the Regulation on the Sharing of Confidential Information as an example of the conditions of being clearly stipulated in the laws and legal obligations.

In the Guide, the Board states that the processing of personal data of persons included in the “Risk Group” within the framework of the provisions of the Banking Law and other relevant legislation, only for the purpose of being used within the scope of banking activities within its own bank and transferred to the Risk Center, is within the scope of fulfilling the legal obligations of the banks. It is regulated that the processing of personal data for the making and operation of systemic arrangements can be carried out without the explicit consent of the person concerned. Banks could conduct certain activities such as obtaining the necessary information and documents to perform risk analysis and risk assessment for real persons and legal entities to whom loans are granted and other persons in the same risk group, taking all necessary steps to confirm the information and documents provided in the examples of good practice explained in the Guide, it is stated that excessive personal data should not be shared, provided that the conditions are clearly stipulated in the laws and that the legal obligation is fulfilled. The information and documents shared should be limited to the data requested, if information and documents cannot be limited, other data in the documents should be masked/deleted/anonymized.

The Guide also addresses the personal data processing condition which is the processing of personal data of contracting parties. It is stated that banks may process personal data for some services they offer to data subjects, whether they have customers or not (the processes of receiving, evaluating, and responding to requests such as loan requests via SMS). When concluding a contract, it is not necessary to obtain the express consent of the person concerned, as it is included in the exceptions within the scope of the PDP Law.

“Legitimate interest” is another condition of the personal data processing listed in the PDP Law, which is closely related to banks. Personal data may be processed without the explicit consent of the data subject if it is necessary for the legitimate interests of the data controller provided that fundamental rights and freedoms of the data subject are not harmed. If data processing activity is necessary the Banks’s legitimate interest, banks could process the personal data of the data subject without obtaining explicit consent within the scope of legitimate interest. To determine legitimate interest within the framework of the "principle of proportionality", data controller should carry out an evaluation. This evaluation covers following three points: Data controllers should have legitimate interest to realize the purpose (Purpose). Not to harm the fundamental rights and freedoms of the data subject (Proportionality) and Personal data processing is mandatory/necessary to achieve the purpose (Necessity). Following the passing of this triple balance test, banks will be able to process data without obtaining explicit consent, provided that they fulfill their obligation to inform within the scope of legitimate interests and not use them for any other purpose.

The Guidelines provide examples of data processing within the scope of legitimate interest for the following purposes.



In addition to these personal data processing conditions specified above, banks could process personal data based on the condition that it is "obligatory for the establishment or protection of a right". For the collection of receivables, banks can use some platforms such as official information sharing platforms (Risk Center, etc.) or ICTA-licensed inquiries and institutions providing guidance services to obtain personal data by querying the Turkish ID Number.

This situation also serves to prevent the person from being followed up by institutions like enforcement offices by paying their overdue debts for the data subjects. With the Guide, it is recommended that banks operate identity verification mechanisms when accessing the data subject with this information obtained from authorized institutions and organizations and prevent third parties from obtaining customer information.

# 3 Evaluation Regarding the Special Categories of Personal Data

The Guide and the related legislations recommend that banks should pay maximum precision to comply with the general principles of PDP Law during the processing of sensitive personal data. The Guide provides more detailed explanations regarding the special categories of personal data that are processed intensively within the scope of banking activities.

## a. Copy of Identity Card

Among all documents containing special categories of personal data in the banking sector, the identity card comes first. The copy of the identity card is used for identification purposes which is a legal obligation of the bank. Especially old identity cards give information regarding blood type and religion. Also, old driving licenses give information related to blood type, disabilities, and prosthetics. All kinds of information as mentioned above are considered as special category personal data. The Guide recommends that if explicit consent cannot be obtained the Banks should process the copy of the ID by masking the special category personal data.

In addition, it is stated that the same sensitivity should be shown for power of attorneys and signature circulars from which copies of identity documents are obtained.

## **b. Medical Reports**

Another document including special category personal data is medical reports. Medical data can only be used for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of medical services and financing. Medical data can only be processed without the explicit consent of the person concerned by persons or authorized institutions and organizations that are under the obligation to keep secrets. Since banks cannot meet the above-mentioned conditions, they will only be able to carry out the process with the explicit consent of the data subjects.

In the recommendations presented in the Guide, it is mentioned that the processes should be revised, if necessary, in cases where medical data is processed by banks; In this context, it is stated that it is necessary to control whether the explicit consent of the data subject is obtained or not, and that the medical data should not be processed in the absence of the explicit consent of the persons concerned.

## **c. Criminal Records and Criminal Conviction and Security Measures**

Other documents including special categories of personal data are criminal records, criminal convictions, and security measures. Unless expressly stipulated in the laws, banks will only be able to process personal data related to criminal records, criminal convictions, and security measures with explicit consent. According to good practices in the Guide, Banks shouldn't collect personal data while they conduct the hiring process because there is no legislation expressly stipulated in the laws. Banks could prefer not to collect this personal data related to this matter. If there is a necessity to collect this kind of information, banks should collect these kinds of personal data by obtaining explicit consent. For instance, in terms of cheque prohibition, since this issue is clearly stipulated in the law the customer's criminal record can be processed without explicit consent by the banks.

#### d. Medical Data of Employees

Medical data of employees is considered a special category of personal data. Since banks with an occupational physician fulfil the special quality personal data processing required in the PDP Law, explicit consent is not required. If the Bank doesn't have any occupational physician on its own, explicit consent should be obtained from the data subject because there are no data processing conditions.

According to good practices examples from the Guide, medical data of employees should only be processed by the occupational physician. Also, if departments need access to employee medical data, access to this data authorization/restriction should be applied, and personal data should be accessed only by certain persons and departments within the bank, by stating the legal reason.

In the current situation, it is also emphasized that since the medical data of the employees need to be processed, banks should in any case obtain explicit consent from the employees.

#### **e. Medical Data Received as an Insurance Agent**

According to the Guide, banks are obliged to implement necessary technical and administrative measures to ensure the data security of special categories of personal data in terms of medical data is processed in accordance with their 'agency' title (as data processors).

#### **f. Biometric Data Used for Authentication**

Another special category of personal data used within the scope of banking activities is biometric data. During the remote identification process, banks can make a biometric comparison of the person's face and the photo on the identity document only with the explicit consent of the data subject. Outside this scope, biometric data should only be processed with the explicit consent of the data subject and by evaluating whether such processing is related to the purpose, limited and proportionate in accordance with the general principles of the PDP Law, unless there is an issue clearly stipulated in the laws. The Guide states that if the Banks could achieve their purposes without processing biometric data, they should prefer alternative methods other than collecting and processing biometric data.

# 4 Evaluations Regarding the Transfer of Personal Data in Türkiye

The transfer of personal data is of great importance for banks. The Guide emphasizes that Banks must comply with personal data transferring conditions from PDP Law to transfer personal data in Türkiye. The transfer of personal data is handled under two titles as transfer in Türkiye and transfer abroad in the Guide.

## Transfer of Personal Data in Türkiye

The Guide states that it is necessary to comply with the procedures and principles in the PDP Law for the transfer of personal data within the country. Also, the provisions in other laws are reserved. Therefore, data controllers must act by considering both PDP Law and other relevant laws. For instance, while data controllers transfer personal data which are considered as a customer secret in the relevant laws related to transfers within the country, data controller, the banks should consider the “Banking Law” and the “Regulation on Sharing of Secret Information”.

The PDP Law identifies the main rules about the transferring of personal data within the country. However, the Guide also states there are other relevant laws about the transferring of personal data. Thus, banks could transfer personal data without obtaining explicit consent within the scope expressly provided by the laws.

## Personal Data Transfers from Banks to Institutions which Authorized to Request Information

Banks can transfer personal data that they collect to the authorities authorized to request information and documents from banks within the scope of the laws. These authorities are listed below and are not limited to them:

Courts, Prosecution Offices, Banking Regulation and Supervision Agency, Court of Accounts, Capital Markets Board, Central Bank of the Republic of Türkiye, Savings Deposit Insurance Fund, Revenue Administration, Social Security Institution, Financial Crimes Investigation Agency, Execution and Bankruptcy Directorates, etc.

## Personal Data Transfers Made within the Scope of Suspicious Transaction Reporting Obligation

If there is any information and suspicion that the person's assets are illegally obtained or used for illegal purposes within the scope of the Law on the Prevention of Laundering Proceeds of Crime, this should be reported to Financial Crimes Investigation Board (MASAK).

## Personal Data Transfers to the Parent/Subsidiaries

In accordance with the Banking Law, information and document requests of a bank's parent company in Türkiye must be carried out with a non-disclosure agreement. These kinds of data transfers are limited to consolidated financial statements, risk management and internal audit practices. According to the Guide, the parent company in question may be a financial institution or another undertaking.

## Personal Data Transfers to Prospective Purchaser

Within the Banking Law, banks can meet the information and document requests of prospective buyers for the valuation studies of potential receivables, provided that a confidentiality agreement is concluded, and the conditions specified in the agreement are limited.

## Personal Data Transfers to Banks and Financial Institutions

According to the Banking Law, banks and financial institutions will be able to directly exchange all kinds of information and documents among themselves, if they have concluded confidentiality agreement and are limited to the purposes specified in the agreement.

## Personal Data Transfers to Risk Center, Interbank Card Center, and Credit Registration Office

In accordance with the Banking Law, Banks could transfer personal data to Risk Center, Interbank Card Center, and Credit Registration Office, if they have concluded a confidentiality agreement and are limited to the purposes specified in the agreement.

## Personal Data Transfers to Affiliates

In accordance with the Banking Law, any exchange of information and documents could be made by banks and financial institutions through risk centers or companies to be established by at least five banks or financial institutions, provided that a confidentiality agreement is concluded and limited only to the stated purposes. Such exchanges of information and documents are excluded from the scope of confidentiality obligation.

## Personal Data Transfers to Valuation, Rating and Support Service Organizations

Following the Banking Law, personal data could be transferred within the scope of establishing confidentiality agreements between banks and valuation, rating, and support services institutions and provided that it is limited to the stated purposes only. This information and documents could be used for getting services related to valuation, rating, and support. Such exchanges of information and documents are out of the scope of confidentiality obligation.

## Personal Data Transfers to Business Partners

In accordance with the Banking Law, Banks could transfer personal data to business partners.

# 5 Evaluations Regarding the Transfer of Personal Data Abroad

For personal data to be transferred abroad in accordance with the law, the conditions in the provisions of the PDP Law regarding foreign data transfer must be fulfilled. It is stated that in accordance with the provisions of the PDP Law on transfers to be made abroad and the relevant Board decisions in case there are special provisions regarding data transfer abroad in other laws, these provisions should be applied with priority. In terms of personal data regarding customer secrets, since the Banking Law is a special norm compared to the PDP Law, personal data with the nature of customer secret can be transferred abroad in cases where customer secret sharing is regulated by the Banking Law and the Regulation on Sharing of Secret Information.

In the Guide, any information showing that a real or legal person is a customer of the bank is a customer secret. It is stated that even if a customer relationship has not been established pursuant to the relevant provision in the Regulation, if the customer secret information held by another bank is obtained and learned by another bank, this data will also have the quality of customer secret for the other bank. Regarding the Amendment of the Banking Law No. 7222 and dated 20/02/2020 and Some Laws in the Guide Pursuant to the justification of the relevant article of the law, which is not a customer secret and the bank's customer and customer Information that exists before the relationship is established is considered personal data. It is stated that personal data of this nature gains the title of customer secret when processed alone or together with the data formed after the establishment of the customer relationship, in a way to show that the real person concerned is a bank customer.

# 6 Evaluations Regarding the General Principles in the PDP Law

Personal data could be processed under the procedures and principles stipulated in the PDP Law and other laws. There are general principles in the PDP Law related to processing personal data as followed and all data controllers must follow general principles;

- Lawfulness and fairness
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed.

It should be noted that it is a legal obligation to comply with the above-mentioned general principles in all circumstances and conditions in the processing of personal data.

# 7 Evaluations within the Scope of Liabilities of the Data Controllers (Obligation to Inform)

In the Guide, the obligation to inform for Data Controller is explained under a separate title. Also, the Guide clearly states that the obligation to inform must be fulfilled special for the personal data processing activity. In this context, Banks should prepare privacy statements according to banking activities as followed;

1. Customer acquisition/ account opening
2. Loan
3. Investment transactions

Within the scope of banking activities, the necessity of preparing separate privacy statements emerges. Activity-specific privacy statements should be provided by the banks for the applicant, according to the purpose of their visiting the bank; It is stated that if non-customers do not establish a permanent business relationship with the bank, it would be appropriate for the process to end with activity-specific privacy statement.



Personal data should be stated on a categorical basis by matching them with the processing purposes and legal reasons in the privacy statements prepared by the banks in a manner specific to the activity.

It is stated that as the mandatory content regarding to whom personal data can be transferred; third party groups such as support services, business partners, subsidiaries, audit institutions, authorized public institutions can be included categorically.

Products and services which are provided by the banks are diverse. Where banks cannot manage to present privacy notices to their customers because of time and place restrictions, banks can fulfill their obligation to inform by presenting layered privacy notices. Layered privacy notices should include some points as followed,

- Layered privacy notices should include main information related to processing personal data of data subjects.
- Layered Privacy notices should include limited content and it also should make pre-enlightenment.
- With the layered privacy notice, the obligation to inform should be fulfilled by referring to the main privacy notice text which is prepared in accordance with the PDP Law on the banks' website.

Data subjects could see layered privacy notices in places where data is collected by filling out an online form, places with security cameras, call centers or similar systems with voice recordings, internet or mobile banking interfaces, ATMs or SMS channels. Except for these platforms, the obligation to inform could be fulfilled through the branches, the websites, the internet branch, the mobile branch/mobile application, the call centers, the electronic mail/physical mail/ SMS/ ATM.

As for the timing of the fulfillment of the obligation to inform; the obligation to inform must be fulfilled by the data controller at the stage of obtaining personal data. However, if the personal data is not obtained from the data subject by the data controller; it can be fulfilled after the stage of obtaining personal data.

The Guide explains some special situations related to fulfilling the obligation to inform. In this context;

- Considering that the real persons authorized to represent the legal persons are already informed by the legal persons about the personal data to be transferred to the bank, there is no need to fulfill the obligation to inform additionally against these representatives. In another example, when processing personal data of data subjects in the risk group, it is deemed sufficient to provide a general privacy statement in a way that can be easily accessed and only in terms of the “Risk Group” activities, instead of informing the individuals in the risk group individually, for each credit/loan transaction,
- In cases where the personal data of persons other than the owner of the asset and persons other than the last endorser are processed in cheque and bill, an additional privacy statement is not required for these persons, and it is not possible for these persons to be masked their personal data can be presented as evidence in case of possible disputes.
- Since it is not possible to fulfill the obligation to inform at the time of opening about the mandatory information received due to the opening of bulk bank accounts by banks within the scope of salary payment agreements, banks can fulfill the disclosure obligation within a reasonable period from the acquisition of personal data,
- The banks are obliged to inform about which data will be transferred to their parties in case their cardholder clients use their cards in different national and international bank devices and POS. If the cardholders who have been enlightened on this matter, use their cards with other banks' devices and POS, there is no need to be enlightened a second time by the bank that owns the device and POS.

The Guide also explains the topics related to the data controller’s registry, obligation to prepare personal data inventory, deletion of the personal data, destruction of the personal data, anonymization, data security, rights of the data subject and complaints to the board.

# Conclusion

## In a nutshell;

Banks are among the institutions that carry out personal data processing activities most intensively. The guide explains the obligations of banks within the scope of protection of personal data in the banking sector. In addition to these obligations, the guide answers the question of when a personal data belonging to a data subject can become a customer secret and whether the PDP Law or the Banking Law or relevant legislation will be applied in terms of customer secrets. Banks should take a concrete step by considering the advice and good practices samples in this Guide within the scope of data protection.



[www.kplawtr.com](http://www.kplawtr.com)

 İş Kuleleri, Kule 3, Kat:2 Levent/Istanbul/Turkey

 +90 (212) 249 29 39

 [info@kplawtr.com](mailto:info@kplawtr.com)