Balcıoğlu Selçuk Ardıyok Keki

Turkish Data Protection Authority published the Guideline on Best Practices for Personal Data Protection in Banking Sector

August 2022

Turkish Data Protection Authority ("**DPA**") published the Guideline on Best Practices for Personal Data Protection in Banking Sector ("**Guideline**") on August 5, 2022. The Guide includes general explanations on the procedures and principles that banks should comply within the scope of personal data protection, as well as other obligations of the banks. Please see the essential principles described within the Guideline below.

1. Scenarios where banks can qualify as Data Controllers and Data Processors

Guideline assesses the legal status of banks and thirds parties by addressing various scenarios on personal data processing:

Scenario	Legal Status
Transfer of personal data to banks by the customer within the scope of payment of employee salaries	**Data Controller:** Customers that concluded "payment of employee salary" agreement with banks
Data processing activities carried out by carrier/cargo companies as Support Services Provider	**Data Controller:** Both banks and cargo companies (with respect to the data processing activities for delivery)
A bank located in Turkey provides support services to its subsidiary abroad on its contract processes	**Data Processor:** Bank
Data processing activities performed within the scope of open banking	1. If bank processes personal data of the customer for the purpose of providing banking services; • **Data Controller:** Bank 2. If a third party provider processes personal data of the customer in order for the customer to benefit from open banking products and services; • **Data Controller:** Bank, Third Party Provider 3. If customer's special categories of personal data is transferred by bank to a third party provider and if the third party provider simultaneously records such data within its data recording system; • **Data Controller:** Third Party Provider that transfers and registers the personal data in their system
Cases where a bank acts as an insurance agency	**Data Controller:** Insurance Company **Data Processor:** Bank

2. Legal basis for processing of personal data

The Guideline mentions that since the scope of banking operations are determined in the applicable regulations, most of the data processing activities of the banks are performed by relying on legal basis other than the explicit consent. Guideline sets forth applicable legal basis for processing activities for different cases as below:

Scenario	Legal Basis
Recording customers' disability status	Explicit consent ** A request that clearly shows a customer's intention to benefit from the accessibility opportunities for disabled persons can be evaluated as the declaration of explicit consent.*
Processing health data of customers	Explicit consent ** If a data subjects shares her health data through the "requests and complaints" section of a bank's website, this action may be evaluated as the declaration of explicit consent.*
Processing personal data of persons listed in the "Risk Group" within the scope of risk assessments	Fulfillment of Legal Obligation
Processing personal data of data subjects listed within the "Risk Group" for bank's use and for transferring such data to the Risk Center	Fulfillment of Legal Obligation
Processing personal data as required by the other legal obligations (e.g: Obligations arising from Bill of Exchange Law, Capital Markets Law, Tax Procedure Law and Law of Obligations)	Explicitly Foreseen by the Laws
Data processing activities regarding establishment of contractual relationships between the bank and data subjects	Execution and Performance of the Contract
Processing contact information of individuals in order to get informed by creditor bank	Execution and Performance of the Contract
Operations carried out by banks in order to provide the transaction security of the data subjects and to take the necessary measures against suspicious activities	Legitimate Interest ** Guideline refers to decisions of DPA and highlights the necessity of applying the legitimate interest balance test for determining whether legitimate interest is a legal basis that can be relied for the data processing activities of the banks.*
Evaluation of customer data in order to determine the service level to be provided to customer, to understand the relationship of the customer with the banks and her use of product and channel (Segmentation)	Legitimate Interest
Activities for identifying products and services that might be the interest of customers in order to ensure customer satisfaction and the efficient use of the bank's financial resources, and to accurately address customer needs	Legitimate Interest
Activities carried out for management of customer complaints and customer relations	Legitimate Interest ** Use of the customer analysis for marketing and profiling purposes requires explicit consent.*
Strategical studies made by using artificial intelligence	Legitimate Interest ** Apart from the determination of the strategies, during the application of such strategies to real persons, the legal basis of processing should be re-considered.*
Contacting with customer who is a loan debtor by bank for the purposes of commercial interests and collection of debt	Establishment and Protection of a Right

3. Special categories of Personal Data processed by banks

Sensitive Personal Data	Legal Basis & Good Practices
Religion and blood type information placed on ID cards	Special categories of personal data included ID cards should not be processed without explicit consent. It is necessary to mask the special categories of personal data within ID cards and only the front side of ID cards should be processed, if possible.
Customers' health data	As banks do not meet the conditions stipulated under Article 6/3 of the DPL, they will be able to process the related data (e.g. disability) by obtaining the explicit consent of the customers.
Criminal records, criminal convictions, and security measures	• **Retention of customers' criminal records for the bill of exchange ban assessment under the Bill of Exchange Law:** Explicitly Foreseen by the Laws • **Requesting criminal conviction data (criminal record) from candidates:** Guideline states that it may be preferable not to collect these data of candidates. However, banks that prefer to collect such data should obtain explicit consent of the candidates.
Employees' health data	For companies where there is a workplace doctor, health data can be processed by workplace doctors without obtaining employees' explicit consent. In such case, health data should not be accessible (or should be restricted) by anyone other than the workplace doctor. For companies where there is no workplace doctor, explicit consent of employees should be obtained for processing their health data.
Biometric data used for authentication	Biometric data should be processed in accordance with the Regulation on Remote Identification Methods and the Establishment of a Contractual Relationship in Electronic Means by obtaining data subjects' explicit consent.

4. Data transfer

Pursuant to Art. 73 of Banking Law, Guideline evaluates that customer secrets which are specifically regulated in banking law constitutes *lex specialis* over the provisions of the DPL and special provisions of Banking Law would be priorly applicable for the disclosure of customer secrets.

As mentioned above, the DPA considers that DPL's provisions on domestic and foreign data transfer are not applicable to the transfer of customer secrets, pursuant to Art. 73 of Banking Law which states that customer secrets may not be disclosed or shared with domestic or foreign third parties without a demand or instruction received from the customer, even if the customer's explicit consent is obtained. DPA's evaluation is limited with the applicability of the DPL's provisions on data transfer and banks are obliged to comply with the other provisions of DPL (e.g. complying with the general principles and taking administrative and technical measures) while carrying out such data transfers.

Considering that Art.8/3 of DPL reserves the provisions of other applicable regulations related to domestic transfer, Guideline mentions the data transfers that can be performed by banks within the framework of such special regulations, and listed such transfers as follows:

1. Transfers to authorities authorized to request information from banks,
2. Transfers within the scope of reporting obligation of suspicious transaction,
3. Transfers to the parent companies/subsidiaries,
4. Transfers to potential buyers,
5. Transfers to banks and financial institutions,
6. Transfers to the risk center, interbank card center and Credit Bureau,
7. Transfers to affiliates,
8. Transfers to assessment, rating and support services providers,
9. Transfers to business partners of banks.

5. Obligation to inform

Considering that the data processing activities of banks can differ depending on the services they provide, information notices should be prepared specifically for the banking activities that concerns the provision of services requested by the data subject. Accordingly, a general information notice that covers all services should not be used.

A layered information notice can be provided in cases where it is not convenient for the customer to read the entire information notice. The Guideline emphasizes that layered information notices can be provided in platforms such as internet or mobile banking interfaces, ATMs and online forms.

Guideline stipulates various situations that banks can encounter in practice and determines the relevant party who should fulfill the obligation to inform in such scenarios. The evaluations are listed in the table below:

Scenario	The Party Who Should Fulfill the Obligation to Inform
Transfer of personal data included within the documents pertaining to the authorization of a legal entity's authorized signatories with the banks	Legal person who appoints the authorized signatory
Processing the personal data of the individuals listed in the Risk Group within the scope of the credit application	Bank ** It is possible to inform data subjects with a general information notice specific to "Risk Group's" activities rather than informing each member of the Risk Group separately.*
Transfer of personal data of individuals other than the owners of assets for security to banks concerning the security transactions	Bank ** In cases where the data isn't categorized to be analyzed by banks, banks do not have an obligation to inform any individual other than asset owners.*
Institutions' data transfer to banks for making salary payments	Institutions that are parties to the agreement for salary payments
Banks' efforts for establishing customer relations with data subjects through group accounts that are opened for salary payment	Bank
Bank customers' use of cards in different banking devices and pos machines	Customer's Bank ** In these cases, the bank that owns the device and pos machine is not obliged to inform the data subjects for a second time.*

6. Deletion requests

Cease of the Purposes of Processing

Under the banks' obligations arising from the legislations and banks' area of activity, Guideline provides examples for cases where the data processing purposes are ceases to exist. For instance, it is considered that the processing of a customer's personal data is no longer needed in cases where the following situations occur collectively:

- Request of the customer regarding to termination of the regular business relationship and closure of the accounts
- Expiration date of retention period of the customer's documents arising from legal regulations.
- Absence of any ongoing legal disputes between the customer and the bank
- Absence of registration such as any confiscation, pledge etc. that will prevent the closure of accounts on the customer's accounts

The Guideline (p. 115-117) also includes a table for the deletion, destruction, and anonymization of personal data where it examines the techniques for deletion, destruction, and anonymization of personal data as well as their advantages and disadvantages.

Pursuant to the Guideline, DPA accepts that individual pieces of data (of a data subject) located within a data set (e.g. the revenue transaction of a person's loan on a certain date) can be processed for the purposes such as "protection of data integrity" and "providing the consistency of the customer information" by taking into account the structure of information systems in the banking sector. Also, it is accepted that banks can rely on fulfilment of the legal obligations and their legitimate interests for processing such data.

7. Data security

Banks are subject to obligations concerning data security, which are derived from being a data controller and being subject to banking regulations. Guideline provides assessments regarding data security by referring both to the banking legislation and Personal Data Security Guide (Technical and Administrative Measures) prepared by the DPA. In addition, the obligation to comply with the secondary legislation published by the Banking Regulation and Supervision Agency is reminded within the Guideline.

8. Audits and data subject requests

While examining the banking regulations and auditing obligations foreseen under DPL, it is concluded that the internal audit departments fulfill the audit obligations foreseen under the DPL while complying with applicable banking regulations that regulate the auditing obligation.

In the Guide, it is stipulated that the data subject requests should be made in accordance with the Communiqué on the Procedures and Principles of Application to the Data Controller. Also, it is considered that banks may reject requests if the authentication of data subject is not possible, on the grounds that the request does not contain the legal requirements.

Contacts

Kağan Dora
Partner
D +90 212 329 30 35
kdora@baseak.com

Neslihan Kasap
Senior Associate
D +90 212 708 93 42
nkasap@baseak.com

Hazal Durak
Associate
D +90 212 708 93 96
hdurak@baseak.com

Emirhan Başol
Associate
D +90 212 708 93 65
ebasol@baseak.com

Yaren Alparslan
Associate
D +90 212 708 93 66
yalparslan@baseak.com

CSBrand-96564-PDF-client-alert — 15/08/2022