PRIVACY POLICY AND CLARIFICATION TEXT
REGARDING THE PROCESSING OF PERSONAL DATA
WITHIN THE SCOPE OF THE NUROL YATIRIM BANKASI A.Ş. MOBILE APP

This clarification text has been prepared by Nurol Yatırım Bankası A.Ş. ("**Bank**"), the data controller within the scope of the Personal Data Protection Law No. 6698 and the relevant secondary regulations, to provide information about the personal data processing activities carried out during the use of the Bank's mobile application ("**Mobile App**").

This clarification text covers only the personal data processing activities carried out through the features specific to the Mobile App. Clarification texts about the personal data processing activities related to the banking products and services accessed through the Mobile App can be found at Nurolbank Kişisel Verilerin Korunması.

E-mail : nurolbank@nurolbank.com.tr
Phone : +90 (212)286 81 00
Registered Electronic Mail : nurolbank.muhaberat@ nurolbank.hs03.kep.tr
Address : Büyükdere Cad. No:255 Nurol Plaza B Blok Kat:15 34485 Maslak/İstanbul
Website : https://www.nurolbank.com.tr

1. Personal Data Processed Specific to Use of the Mobile App

Data Category	Processed Data
Identity	Name-surname; if remote customer acquisition or authentication is used: one's Turkish ID/Foreign National ID/passport number, date and place of birth, marital status, mother's name, father's name, sex, ID card serial number, nationality, signature.
Communication	Phone number, e-mail address, and communication preferences for notifications made via the Mobile App.
Customer Procedures	Customer number, digital channel user identifiers, identification, activation and use authorization records for the Mobile App, records of applications, requests, support and operational processing transmitted via the Mobile App using representative/authorization details.
Location	Approximate or precise location details when a location-based feature is used in the Mobile App.
Financial Transaction	Financial instructions and orders and the transaction and results records relating to their execution.
Customer Recognition and Compliance	Occupation, employer, source of income, actual beneficiary, politically exposed person (PEP), sanctions/screening and customer risk profile information related to KYC/MASAK controls if remote customer acquisition or authentication is used.
Transaction Security and Device Information	IP address, device ID and model, operating system and app version, user ID, login-logout, access and transaction logs, OTP generation and verification records, password verification result, failed login attempt and other authentication transaction records, mobile notification tokens

Data Category	Processed Data
	and delivery records, device pairing records and signals and records created for the purpose of detecting unauthorized access, fraud, and security risks.
Visual and Audiovisual Records	When used for remote authentication or video/audio communication via the Mobile App: photo, video/call image and audio recording to the extent necessary.
Liveness Check and Biometric/Verification Data	When remote authentication is used: **Biometric Data** Data on facial image, facial features, and biometric comparison of face and ID photo processed by special technical methods to uniquely authenticate the person. **Liveness and Authentication Data** Facial movement and position, depth data processed only instantly on the device if supported by the device, liveness result, verification result, security score, and fraud risk indicators.
User Selected Device Contents	Photos, documents, receipts, and files uploaded by the user via the respective Mobile App feature and the necessary information about the directory person selected by the user in a money transfer or similar transaction.
Technical Usage, Error and Performance Data	Error and crash records, error codes, screen and process response times, connection and network performance, technical event records and performance records related to the continuity and functionality of the service during the operation and monitoring of the technical performance of the Mobile App.
Request, Complaint, and Legal Action	Request, complaint, objection, security notification, and support records transmitted via the Mobile App and records created for the purpose of concluding them and proof in possible disputes.

Special Information on Camera, Face Detection/Depth Sensors, and Video Recording

The Mobile App uses the camera of the device and face detection/depth sensors if supported by the device to confirm that the person performing the transaction is a real and live person, if remote authentication and liveness checks are used. Facial movement, facial position, depth data, facial map, and biometric template detected by these sensors are processed only on the device in real time and temporarily; they are not transferred to Bank servers, permanently recorded on the device or Bank systems, stored, shared with third parties, and used for advertising, marketing, user profiling, data mining, or general-purpose artificial intelligence model training.

In addition, standard video/call recording can be made with the device camera to complete the remote authentication and liveness verification process. This record is transmitted to the Bank's systems through encrypted communication channels and is examined by artificial intelligence supported systems and, if necessary, authorized Bank personnel for the purpose of fulfilling the Bank's legal obligations and can be kept for periods in accordance with the legislation within the scope of banking processes.

Camera, microphone, location, photo/file, directory or notification permissions shown by the operating system provide only technical access to the respective device feature and do not replace explicit consent under the PDPL. When processing activity that requires explicit consent, the clarification and explicit consent processes are carried out separately.

2. Purpose of and Legal Basis for Mobile App-Specific Processing

Processed Data Categories	**Process / Purpose of Processing**	**Legal Basis**
Identity Communication Customer Procedures Customer Recognition and Compliance	Receiving the remote customer acquisition application via the Mobile App, carrying out identification and customer recognition/compliance checks, and carrying out customer and digital channel identification/activation processes.	PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations.
Customer Procedures Financial Transaction	Managing the Mobile App account and digital channel authorizations; Viewing the accounts via the Mobile App and performing the payment, transfer, card, credit, investment, treasury, and other banking transactions initiated by the user.	PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, **In terms of the transactions required by the relevant legislation:** PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations.
Transaction Security and Device Information Technical Usage, Error, and Performance Data	Secure login and session management, OTP and mobile notification processes, device pairing, keeping access and transaction logs, cyber security, prevention of unauthorized access and fraud attempts, anomaly and risk analysis, and fulfillment of information systems obligations.	PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-e: Data processing is necessary for the establishment, exercise or protection of a right. PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject.
Identity Customer Recognition and Compliance Visual and Audiovisual Records Liveness Check and Biometric/Verification	Remote identification, matching the identity document with the person, liveness check, video/call recording, biometric comparison, fraud checks, approval and review processes, and providing authentication security.	**In terms of general data:** PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations.

Processed Data Categories	Process / Purpose of Processing	Legal Basis
Data Transaction Security and Device Information		PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject. **In terms of processing biometric data** PDPL Art.6/3-a: is processed when the data subject has given his/her explicit consent.
Location Visual and Audiovisual Records User Selected Device Contents Transaction Security and Device Information	When the user prefers the relevant Mobile App feature, obtaining an identity document/document image or scanning a QR/barcode with the camera; establishing video/audio communication with the microphone; providing location-based branch/ATM or security service; using the photo, file or directory person selected by the user in the relevant transaction, and sending service/security notifications.	Depending on the nature of the feature: PDPL Art.5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations.
Transaction Security and Device Information Technical Usage, Error, and Performance Data	Running the Mobile App, ensuring that it is compatible with the device and operating system, error and performance management, technical support, detection of security vulnerabilities, and ensuring service continuity.	Depending on the nature of the feature: PDPL Art.5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject.
Request, Complaint, and Legal Action Transaction Security and Device Information	Concluding requests, complaints, objections and security notifications transmitted via the Mobile App; responding to the applications of the data subject; Establishing, exercising, or protecting rights in disputes and security incidents related to the Mobile App.	PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-e: Data processing is necessary for the establishment, exercise or protection of a right.

3. Transfer of Personal Data within the Scope of the Mobile App

Personal data processed within the scope of the Mobile App may only be transferred to domestic recipients for the purposes specified below and limited to the necessary data sets. Personal data processed within the scope of the Mobile App are not transferred abroad.

Recipient Group	**Purpose of Data Transfer**	**Legal Basis**
Regulatory and Legally Authorized Bodies	Transferring information and documents related to remote customer acquisition, authentication, user login, device pairing, banking transactions and security processes carried out through the Mobile App to meet the regulatory information and document requests made by legally authorized public institutions and legally authorized private persons, to fulfill legal notification and reporting obligations, and to carry out audit, investigation, and surveillance activities.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-e: Data processing is necessary for the establishment, exercise or protection of a right.
Judicial and Dispute Authorities	Conducting litigation, enforcement, investigation, mediation, expert review, and other dispute processes related to transactions carried out via the Mobile App, user instructions, authentication processes, and security incidents; Protecting the rights and interests of the Bank, performing defense and proof activities, and submitting the necessary information and documents to the competent authorities.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-e: Data processing is necessary for the establishment, exercise or protection of a right.
Mobile App, IT, Information Security, Software, Infrastructure, and Technical Support Service Providers	Developing, installing, hosting, operating, maintaining and updating the Mobile App; transferring user and access management, backup, logging, technical support, cyber security, vulnerability and event management, error and performance analysis, prevention of unauthorized access and fraud attempts, and ensuring service continuity.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject. **Access to personal data by service providers acting in their capacity as data processors is limited by the**

Recipient Group	Purpose of Data Transfer	Legal Basis
		Bank's instructions, privacy obligations, and data security measures.
Providers of Remote Authentication, Video Call, Liveness Check and AI-Assisted Review Service	Performing identity document control in the remote customer acquisition and authentication, taking video calls or video recordings, matching the person with the photo on the identity document, performing liveness and biometric comparison, conducting fraud checks, creating the verification result, examining failed or suspicious transactions and transferring them for the purpose of providing authentication security.	Pursuant to PDPL Art.8/2-a **in terms of general personal data**: PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. **Biometric Data and Liveness and Authentication Data processed instantly on the device are not transferred to third parties.**
Payment, Card, Investment and Financial Infrastructure Institutions, and Other Banks Party to the Transaction	Transmitting the payment, money transfer, card, credit, investment, treasury, clearing, custody, and other banking instructions given by the user via the Mobile App to the relevant financial infrastructures and transaction parties; authorizing, performing, reconciling, and exchanging the transactions, storing, finalizing, and transferring the transaction results to the user.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, **In terms of the transfers and transactions required by the relevant legislation** PDPL Art. 5/2-a: It is expressly provided for by the laws. PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations.
SMS, OTP, Mobile Notification, and Communication Service Providers	Transmitting one-time verification codes, transaction confirmations, security alerts, device pairing notifications, service messages related to account and transaction movements, and other operational notifications requested by the user for the purpose of login to the Mobile App and transaction confirmation, and keeping transmission and delivery records.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-c: It is directly related to the establishment or performance of a contract, PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject.

Recipient Group	Purpose of Data Transfer	Legal Basis
Law Offices, Independent Auditors, and Expert Advisors	In the event of a security incident, personal data breach, audit, regulatory review, legal dispute or application of the data subject related to the Mobile App, examining the incident, conducting technical and legal evaluation, obtaining legal opinion and audit service, conducting defense and proof activities, and protecting the rights of the Bank.	Pursuant to PDPL Art. 8/2-a: PDPL Art. 5/2-e: Data processing is necessary for the establishment, exercise or protection of a right. PDPL Art. 5/2-ç: It is necessary for the data controller to fulfill their legal obligations. PDPL Art. 5/2-f: Data processing is necessary for the legitimate interests of the data controller provided this does not harm the fundamental rights and freedoms of the data subject.

4. Methods of Collecting Personal Data within the Scope of the Mobile App

- Membership, authentication, login, transaction, request and notification screens in the Mobile App, and information entered by the user.
- The camera, microphone, location, photo/file, directory and notification permissions of your device; these permissions are only activated if the respective Mobile App feature is used.
- Remote authentication, liveness check, video/call recording, identity document image, and artificial intelligence-assisted authentication, and fraud prevention systems.
- IP, device, operating system, application version, session, access, transaction, error, and performance records automatically generated by the Mobile App and the Bank's security infrastructures.
- Requests, complaints, notifications, documents, and files transmitted by the user via the Mobile App.
- Information obtained in accordance with the law from authorized institutions, financial infrastructure organizations, and other banking systems within the scope of banking transactions initiated via remote authentication or Mobile App.

5. Retention and Disposal and Managing Mobile Device Permissions

Personal data processed within the scope of the Mobile App are kept for the period required by the relevant processing purpose and taking into account the retention obligations and statute of limitations arising from banking, information systems, prevention of laundering of crime revenues, and other applicable legislation to which the Bank is subject. Personal data whose retention period has expired or the purpose of processing no longer exists is deleted, destroyed, or anonymized in accordance with the PDPL and the relevant legislation.

Facial movement, facial position, and depth data processed instantly on the device for liveness control are not stored in Bank systems as they are not transferred to Bank servers. Video/call records, verification results, and transaction security records taken within the scope of authentication are kept only for the periods required for authentication, compliance with the legislation, audit, transaction security, and proof purposes in case of dispute.

Camera, microphone, location, photo, file, directory, and notification permissions can be managed or withdrawn in the settings section of your device. Withdrawal of a consent may only result in the inability to use the Mobile App feature that needs this consent and does not affect the personal data processing activities carried out in accordance with the law before the withdrawal date.

- Camera permission can be used for remote authentication and liveness check, displaying the identity document or the document selected by the user, and scanning the QR/barcode if presented in the Mobile App.

- Microphone permission can be used to the extent necessary during remote authentication or video/audio communication initiated by the user via the Mobile App. The microphone is not used for continuous listening or recording in the background of the Mobile App.

- Location permission can be used to show the nearest branch/ATM to the user if offered in the Mobile App, to provide services based on the location requested by the user, and to ensure transaction security to the extent applicable. Continuous location tracking is not performed.

- Photo and file access is used only for the purpose of uploading the photo, receipt, document, or file selected by the user to the Mobile App; no mass access is provided to content that the user does not select.

- If directory permission is used, only the necessary information of the person selected by the user for the relevant transaction in the Mobile App is processed; the entire directory is not transferred to the Bank's systems.

- Notification permission can be used to send service messages such as verification codes, transaction notifications, security alerts, and account activity. Advertising, marketing, or promotional notifications are also subject to the consent/approval and rejection processes performed.

6. Your Rights Concerning the Protection of Your Personal Data

Pursuant to Article 11 of the Law, you have the following rights by applying to our Bank:

- to learn whether your personal data have been processed,
- if they have been processed, to request information in relation to such processing,
- to learn the purpose of processing and whether they have been used in accordance with this purpose,
- to know the 3rd parties to whom they have been transferred domestically/ abroad,
- to request correction if they have been processed incompletely/incorrectly,
- to request their deletion/destruction,
- to request that the operations performed pursuant to the requests for correction, deletion, or destruction are reported to the 3rd parties to whom your data were transferred,
- to object to any unfavorable outcome due to your processed personal data being analyzed solely by automatic systems,
- to claim compensation for losses arising from the unlawful processing of your personal

data.

Requests within the scope of Article 11 of the Law No. 6698, which regulates the rights of the data subject, can be submitted to the address of our Bank at Maslak Mahallesi, Büyükdere Caddesi, No:255, Kat:15 İç Kapı No: 1502, 34485 Maslak-Sarıyer/İstanbul in person or via a notary public; to the Registered Electronic Mail address of our Bank, nurolbank.kvkk@nurolbank.hs03.kep.tr; to the e-mail address of nurolbank@nurolbank.com.tr by using the e-mail address previously notified by the data subject and registered in our system, or by using an e-mail address not registered in our system using a secure electronic signature / mobile signature. Our bank shall conclude the requests in the application within 30 (thirty) days depending on the nature of the request.

Effective Date: 08/04/2026
Date of Last Update: 08/04/2026