

MOKA UNITED ODEME HIZMETLERI VE ELEKTRONIK PARA KURULUSU A.S.

Clarification Text

Moka United Odeme Hizmetleri ve Elektronik Para Kurulusu A.S. (“**Moka United**” or “**Company**”) demonstrates the utmost care and attention to ensure the confidentiality and security of the personal data it collects and processes.

For this reason, personal information processed by our Company in the capacity of Data Controller or Data Receiver is processed and stored in accordance with the Personal Data Protection Law No. 6698 (“PDPL”). For this purpose, Moka United takes all necessary administrative and technical measures to protect your personal data in all your transactions and processes your personal data under the conditions explained below and within the limits prescribed by the Law and other applicable legislation.

1. Legal Nature and Scope

Article 10 of the Law No. 6698 on the Personal Data Protection Law titled the Obligation to Inform stipulates that the persons whose personal data are processed should be informed by the data controllers. According to the provisions of the PDPL, Moka United is the “Data Controller” in terms of personal data in its field of disposal.

This Clarification Text informs data subjects about: the identity of the data controller; the purposes for which personal data are processed; the recipients of personal data and the purposes of such transfers; the legal grounds for collecting personal data; to whom and by what means personal data may be transferred; and the rights listed in Article 11 of the Law—such as requesting updates, deletion, or anonymisation of their data from the data controller.

2. Identity of the Data Controller

In subparagraph (1) of Article 3/1 of the PDPL, the Data Controller is defined as “Natural or legal persons who determine the purposes and means of processing personal data and are responsible for the establishment and management of the data recording system”. Within this framework, our Company is the data controller in respect of some data.

The contact details of our Company as the Data Controller are as follows. Levent Mah. Meltem Sok. İşbankası Kuleleri Blok No: 10 İç Kapı No:4 Beşiktaş/İstanbul – Türkiye, info@mokaunited.com www.mokaunited.com

3. Your Processed Personal Data

The following information you shared with the company,

- 1) Identity Information: Name and surname, Turkish ID Number/Tax ID Number, date of birth, nationality, copy of ID/Passport/Driving Licence (if necessary)
- 2) Contact Information: Mobile phone number, e-mail address, office and/or residential address (if necessary)
- 3) Customer Transaction Information: IBAN, customer card number, customer account balance, transaction limit, risk information, transaction history, payment methods and invoice information
- 4) Process Security Information: IP Address, internet login and logout information, password and passcode information, device and browser information, user session information
- 5) Audio and Visual Information: Selfie or biometric photograph for identity verification purposes (where necessary), voice recordings of calls made to the call centre
- 6) Location information: Device location (IP-based or GPS data)

- 7) Online Help and Customer Service Records: Written or verbal communications with our Company via online support, call centre, e-mail and similar media, live support chat records,
- 8) Electronic Mail Communications: The content and attached documents in the e-mails you have sent to our company,
- 9) Web Interaction and Analytics Data: Device model and operating system, browser information, visited pages and session duration, IP address, page and advertisement interaction data, user behaviour analytics data (most used buttons, browsing habits, etc.),

are processed in accordance with the relevant legislation within the scope of PDPL. Within the framework of the data processing conditions specified in Articles 5 and 6 of the PDPL; it is processed by fulfilling contractual obligations, complying with legal obligations, protecting legitimate interests and obtaining explicit consent when necessary. The purposes and categories of processing your data are detailed in the table below.

4. Purposes and Legal Grounds for Processing Your Personal Data

Data Processing Purposes	Personal Data Category	Legal Grounds for Processing
Effective conclusion of the agreement and provision of services	Identity information Contact details	It is directly related to the establishment or performance of the agreement, it is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law
Creating your user account and carrying out authentication processes	Identity information Contact details Visual and auditory information	It is directly related to the establishment or performance of the agreement, it is compulsory for the Company to fulfil its legal obligation,
Performing top-up, payment transactions and money transfers	Identity information Contact details Customer transaction information Transaction Security Information Location Information	It is directly related to the establishment or performance of the agreement, it is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law
Creating your virtual card and providing payment and cash withdrawal transactions with the card and providing wallet services	Identity information Contact details Customer transaction information Transaction Security Information	It is directly related to the establishment or performance of the agreement, it is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law

Receiving and following up your requests and complaints, providing you with the services of the Company in order for you to benefit from the call centre service and to resolve the problems experienced	Identity information Contact details Customer transaction information Online Help and Customer Service Records, Audio and Visual Information	It is directly related to the establishment or performance of the agreement, it is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law
Effective implementation of customer identification processes (KYC - Know Your Customer), anti-money laundering (AML - Anti-Money Laundering) and anti-fraud mechanisms to ensure financial security; implementation, supervision and continuous improvement of the compliance programme within the scope of the relevant legislation; management of legal processes to prevent laundering of proceeds of crime and unlawful transactions	Identity information Contact details Customer transaction information Transaction Security Information Location Information, Audio and Visual Information	It is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law
Managing risk management and internal control processes, ensuring the highest level of financial and commercial data security, establishing appropriate IT infrastructure and databases, and taking administrative technical measures, particularly for electronic services	Identity information Contact details Customer transaction information Transaction Security Information	It is compulsory for the Company to fulfil its legal obligation, it is clearly stipulated in the law
Improvement of user experience, marketing, advertising and personalised campaign activities	Identity information Contact details User preferences Web Interaction and Analytics Data	It is processed on the condition that explicit consent is obtained. The User may withdraw his/her consent at any time.

In line with the specified methods and purposes, your personal data is processed in accordance with the Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, Law No. 5549 on Prevention of Laundering Proceeds of Crime, Regulation on Payment Services and Electronic Money Issuance and Payment Institutions and Electronic Money Institutions, Decree Law No. 660 on the Organisation and Duties of the Public Oversight, Accounting and Auditing Standards Authority and other relevant legislation, Articles 4, 5 and 6 of the PDPL and the provisions of the Attorneyship Law No. 1136. In this context, your data is obtained and processed in order for our Company to fulfil its obligations arising from the agreement and the legal regulations in force in a complete and accurate way, to ensure the security of the financial system, to fulfil its obligations to prevent laundering of proceeds of crime and to comply with legal audit processes.

5. Our Principles on Processing Personal Data

As Moka United, we undertake to act in accordance with all relevant legislation, especially the Personal Data Protection Law No. 6698 (“PDPL”), when processing your personal data. In this context, we execute our data processing processes in line with the following basic principles:

- a. Processing in accordance with the law and good faith: Your personal data is processed in accordance with legal obligations and within the framework of the principle of transparency.
- b. Keeping it accurate and up to date: We take the necessary measures to ensure the accuracy and up-to-dateness of your personal data.
- c. Processing for specific, explicit and legitimate purposes: Your data will only be used for clearly specified and legally applicable processing purposes.
- d. Being purpose-related, limited and proportionate (data minimisation): Your personal data are processed as much as necessary and appropriate with respect to the purpose of processing, and unnecessary data collection or processing activities are avoided.
- e. Compliance with the storage period: Your personal data is stored only for the period stipulated in the relevant legislation or necessary for the purpose of processing and expired data is securely destroyed.

6. Methods of Processing Personal Data

Your personal data are processed in accordance with the processing conditions specified in Article 5 of the PDPL. In this context, your data is processed based on the following;

- a. Explicitly stipulated in the law,
- b. Being necessary for the conclusion or performance of a contract,
- c. It is compulsory for the data controller to fulfil its legal obligations,
- d. Processing in accordance with the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject,

Your sensitive personal data is processed only in accordance with the conditions stipulated by the PDPL and relevant legislation. Accordingly, your biometric data (such as selfies or facial recognition data used in identity verification processes) is processed in cases where it is necessary for our company to fulfil its legal obligations, required for the establishment, exercise, or protection of a right, explicitly prescribed by the legislation, or where your explicit consent has been obtained. Our company demonstrates utmost care in the processing and protection of special categories of personal data and processes them only when necessary, in the most limited extent possible and by taking secure technical/administrative measures.

7. Recipients and Purpose of Personal Data Transfers

Your personal data collected and processed in our company in accordance with the PDPL may be transferred to;

- Legally authorised public or private institutions/organisations such as Banking Regulation and Supervision Agency (BDDK), Financial Crimes Investigation Board Directorate (MASAK), Central Bank of the Republic of Türkiye, independent audit institutions in order to fulfil the obligations such as risk management, notification, accounting, internal control and audit, compliance, etc. stipulated in Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, Law No. 5549 on Prevention of Laundering Proceeds of Crime, Decree Law No. 660 on the Organisation and Duties of the Public Oversight, Accounting and Auditing Standards Authority for Moka United,
- Domestic goods and service providers, business and solution partners and consultants for the purpose of supplying administrative, financial, legal and technical materials and services required by the Company and accompanied by confidentiality agreements,
- Authorised public legal entities or judicial authorities due to the lawsuits and proceedings addressed in order to establish, protect and exercise a right.

Provided that it is directly related to the establishment or performance of an agreement, the transfer of personal data belonging to the parties to the contract is based on the legal ground that it is necessary for the fulfilment of the Companies' legal obligations, on the condition that it is explicitly stipulated by law;

- Your identity, contact and financial data in order to provide you with the services of the Company through the Wallet application,
- Your identity, contact, customer transaction information, online help and customer service records, visual and audio information in order for you to benefit from the call centre service, to resolve the problems experienced and to provide you with the services of the Company,

may be transferred by Moka United to third parties specified under Law No. 6493.

Personal data processed by our company are shared only for the above-mentioned purposes within the country and with authorised persons, institutions and organisations, and no personal data are transferred abroad.

8. Collection Methods of Your Personal Data

Your personal data are collected provided that;

- a) Transactions related to the payment account are carried out, such as depositing money into the payment account and sending money from the payment account in accordance with the payment order,

- b) The direct debit transaction related to the transfer of funds in the payment account, the payment transaction made with a payment card or a similar instrument and the money transfer including a regular payment order,
- c) Payment instrument issued or accepted,
- ç) Funds transfer,
- d) Invoice payments are mediated,
- e) The consent of the payment service user has been obtained; by automated or non-automated means in the course of the basic payment services we provide, such as the provision of consolidated information on one or more payment accounts on online platforms.

9. How Do We Protect?

Moka United takes all necessary technical and administrative measures to ensure the confidentiality and security of personal data in full compliance with the Personal Data Protection Law No. 6698 (“PDPL”) and related legislation. Advanced technical measures such as strong encryption methods, access control mechanisms, network security measures and data masking techniques are applied to prevent unauthorised access, loss, alteration, disclosure or misuse of your personal data.

In addition, as part of administrative measures, internal data security policies have been implemented, regular training is provided to employees, and personal data is processed only by authorised personnel. In cases where your personal data is shared with third parties, contractual obligations ensuring that the relevant parties comply with the same high security standards are enforced, and these processes are regularly audited.

Our data security practices are constantly updated in parallel with technological developments, and regular tests and controls are carried out against cyber security risks.

10. Protection and Storage Period of Your Data

All necessary technical and administrative measures are taken by Moka United to protect the personal data collected and to prevent unauthorized access, thereby ensuring that our customers and prospective customers do not suffer any harm. Within this scope, our internal Privacy and Information Security Policies are strictly followed, including the use of software that complies with standards, up-to-date firewalls and antivirus systems to prevent cyberattacks, careful selection of third parties, and the implementation of access and authorisation controls.

After the termination of the agreement you have concluded with our company, your personal data will be deleted, anonymised or destroyed by you or upon your request, unless otherwise required by Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, Law No. 5549 on Prevention of Laundering Proceeds of Crime, Decree Law No. 660 on the Organisation and Duties of the Public Oversight, Accounting and Auditing Standards Authority and other legislation. However, in cases where laws and regulations stipulate a certain period of storage, your data will be stored for the specified period. If this period expires, your data will be deleted ex officio or upon your request.

11. Rights of the Data Subject and Application

Within the scope of Article 11 of the PDPL, as personal data subjects, you have the following rights:

- a) To find out whether personal data is being processed,
- b) To request information if personal data has been processed,
- c) To find out the purpose of processing personal data and whether they are used in accordance with their purpose,
- d) To know the third parties to whom personal data are transferred in the country or abroad,
- e) To request correction of personal data in case of incomplete or inaccurate processing and to request notification of the transaction made within this scope to third parties to whom personal data is transferred,
- f) Although the data has been processed in accordance with the provisions of the PDPL and other relevant laws, to request the deletion or destruction of personal data if the reasons requiring its processing disappear, and to request notification of the transaction made within this scope to third parties to whom personal data is transferred,
- g) To object to the occurrence of a result to the detriment of the individual by analysing the processed data exclusively through automated systems,
- h) To demand compensation for damages in case of damage due to unlawful processing of personal data.

In order to exercise the above-mentioned rights, personal data subjects may submit their requests in accordance with Article 13 of Law No. 6698 and the Communiqué on the Procedures and Principles of Application to the Data Controller. You are required to submit your applications in writing to our company address, through a notary public or via secure electronic signature/mobile signature and registered e-mail (KEP) along with documents verifying your identity. Our company will finalise the applications free of charge within thirty (30) days at the latest depending on their nature; however, a fee may be charged according to the tariff determined by the Personal Data Protection Board for requests requiring additional costs.

In accordance with the legislation, applications must be made only by the data subject and must contain information belonging only to the applicant. Applications made on behalf of third parties (e.g. spouses, relatives, friends) may be accepted if made by a duly authorised representative of the data subject.

Last Updated: 18.04.2025