GENERAL
PRIVACY NOTICE

INTRODUCTION, THE DATA CONTROLLER'S DATA AND CONTACT DETAILS

The purpose of this privacy notice (hereinafter: "**Notice**") is to provide natural persons doing business with MKB Bank Nyrt. ("**Data Subjects**") with transparent and easy to understand information on the circumstances of the processings of their personal data carried out by the Bank, including the purpose(s), legal basis and duration of data processings, those authorised to consult their data and the Recipients to which they may be transferred, as well as the rights Data Subjects can exercise in regard to their personal data and what possible legal remedies are available for them, in accordance with the General Data Protection Regulation EU No 2016/679 ("**GDPR**").

Please read the Notice carefully and if you have any further question, please do not hesitate to contact the Bank's Data Protection Officer at the contact data to be found below. For the most important terms and concepts relating to data protection see Annex 1.

DETAILS OF DATA CONTROLLER

Name of Data Controller	**MKB Bank Nyrt.**
	('**Bank**' or '**Controller**')
Registered office	H-1056 Budapest, Váci u. 38., Hungary
	E-mail: ugyfelszolgalat@mkb.hu
Central contact details	Telephone: +36 (80) 350-350
	(MKB TeleBANKár)
Website	www.mkb.hu
Company registration number	01-10-040952

CONTACT DETAILS OF DATA PROTECTION OFFICER

Postal address	H-1134 Budapest, Kassák Lajos u. 16-18.
E-mail address	adatvedelem@mkb.hu

If you have any question to ask or any request or complaint to make regarding the protection of personal data or any request concerning the exercise of the right relating to the processing of personal data, feel free to contact MKB Bank Nyrt's Data Protection Officer.

1. BASIC PRINCIPLES

Personal data may only be collected, stored, processed and transferred, and any other operation involving the data may only be performed ('**Data Processing**') if the purpose of data processing is adequately specified and lawful, the required legal basis is available and if the lawfulness of data processing is guaranteed throughout the whole period of data processing. The Bank – in its

capacity as controller – is responsible for ensuring that the following basic principles are observed in regard to processings:

- it must make sure that in every single data processing it performs, the personal data are processed in accordance with the principles of lawfulness, integrity and transparency.
- personal data may only be processed for a clear-cut and specific purpose and personal data cannot be used for any other purpose in any way not compatible with the original purpose; the purpose, means and the necessity of data processing must be proportional to one another, which must be adequately documented.
- the processing of personal data must be limited to the necessary scope in accordance with its purpose.
- personal data must be up to date and accurate; throughout the proceedings all reasonable efforts must be made to ensure that any inaccurate or outdated data are rectified or deleted.
- personal data may only be stored for the period of time as required for the accomplishment of the purpose of processing; the processing of personal data after the period of data processing is prohibited.
- personal data must be processed in a way guaranteeing the rights of the data subjects, the availability, integrity and confidentiality of the data.
- in its capacity as controller the Bank is responsible for ensuring compliance with the GDPR and for proving it (accountability).

2. CATEGORIES OF DATA SUBJECTS

In its capacity as such, the Controller processes personal data of persons of the following categories:

2.1. Natural persons entering into cooperation with the Controller for the purpose of using products and/or services:

- A contractual relationship is established between the Bank and the Data Subject (e.g. borrower, account holder, bank card holder).
- No contractual relationship is established between the Bank and the Data Subject (e.g. loan applicant, person requesting the opening of accounts).

2.2. Data Subjects not wishing to use the Bank's products and/or services but establishing a contractual relationship with the Bank or being involved in a transaction

- Natural persons not qualifying as customers under contracts pertaining to the use of services (e.g. guarantors, pledgors), including, in the case of legal entities, natural persons entering into contracts concerning covenants securing the contract concerned, as well as occasional customers.

2.3. Data Subjects not in a contractual relationship with the Bank

- Third persons facilitating the use of services or the conclusion of the relevant contracts (e.g. authorised representatives, witnesses, lawful representatives, guardians, persons signing for illiterate persons, interpreters).
- Natural persons transacting or communicating with the Bank for purposes other than the use of its services (e.g. occasional customer, representative as specified in the AML Act, external supervisory board members, shareholders, natural persons specified in requests received from authorities or courts etc. based on relevant legal regulations, sellers, usufructuaries, lessees and tenants, Data Subjects appearing in camera footage, representatives, contact persons, third party providers of contractual partners not involved in a customer relationship and in the case of subsidised loans minors living in the same household as the loan applicant.)

Such data subjects have the rights granted to data subjects specified in the Notice in the same way, including the right to information, which data subjects can familiarise themselves with in the individual notice regarding data content, furnished for them at the beginning of processing.

3. SOURCE OF PERSONAL DATA

The Controller processes the personal data of the Data Subjects primarily on the basis of their communication (by using the service, in the context of the conclusion of the contract, communication during the term of the contract etc.). In some cases – during certain transactions – the Controller may obtain personal data from third parties as well (in particular, from courts or other authorities).

In addition to the data supplied by the Data Subjects, the Controller collects further data from public registry systems containing data concerning the Data Subjects or – in the case of the certification of its right or legitimate interest – from registry systems accessible for anybody or lawfully generated from them.

Where the Controller collects personal data concerning Data Subjects not from the Data Subjects themselves, it provides the Data Subjects with the information prescribed in Article 14 of the GDPR; in particular, it provides information on the source of the personal data and whether the data originate from a publicly accessible source, as the case may be.

4. PURPOSES AND LEGAL BASES OF DATA PROCESSING IN GENERAL

The Bank processes data for the purposes of performing its services, fulfilling its legal obligations and providing data as prescribed by law, and, in some cases, in the Bank's or third persons' legitimate interests. Personal data are processed by the Bank on the following legal bases for the most part:

- based on the Data Subject's voluntary, specific and clear-cut **consent** to processing, based on prior information and expressed by the Data Subject's action (e.g. processing for the purpose of direct marketing);
- for **performing contracts** on the use of the various services provided by the Bank (e.g. concluding bank account contracts);

- for the purposes of **fulfilling obligations imposed on the bank by law** (e.g. the 8-year retention time as per the AML Act), and
- in certain cases on the basis of the **Bank's or third parties' legitimate interests** (e.g. the operation of a security CCTV system).

Detailed information on specific individual data processings pertaining to the Bank's services is provided in separate (special) privacy notices in a breakdown by products, services and activities (www.mkb.hu/adatvedelmi-tajekoztatas).

Concerning data processings for which no special notice is available additional details are available in Annex 2 hereto.

If the special notice specifies the period of limitation for the enforceability of a claim as the final date for the duration of the processing, this must be construed in such a way that the legal act interrupting limitation extends the deadline for the duration of processing the personal data until the new date of limitation.

4.1. Processing of sensitive data

The Bank processes special personal data categories with particular care. The special categories of personal data are as follows:

a) Data on racial or ethnic origin:
b) Data on political opinion, religion or beliefs;
c) Data on trade union membership;
d) Biometric; and
e) Genetic data used for the individual identification of the Data Subject;
f) Health data; and
g) Data on sex life or sexual orientation.

The Bank does not process personal data falling into above special categories a), b) e) and g), and the processing of data of categories c), d) and f) is permitted only if the Data Subject has given their specific consent to processing or any of the following criteria regarding the processing of those data, as specified in 9 of the GDPR, is met.

a) carrying out obligations and exercising rights in the field of employment and social security and social protection law;
b) protection of vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
c) in relation to the activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, where processing relates solely to the members or to former members of the organisation or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
d) the data have been manifestly made public by the data subject;
e) establishment, exercise or defence of legal claims;
f) substantial public interest;
g) preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
h) public interest in the area of public health; or

i) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5. THE DURATION OF DATA PROCESSING

As a general rule, the Bank processes adequate and relevant personal data, collected regarding the Data Subjects for a legitimate purpose, which data are strictly necessary for the purpose concerned, not longer than is necessary for the accomplishment of the purpose of processing.

The Bank is obliged to erase and it erases all personal data pertaining to the Data Subject regarding which the purpose of processing no longer exists and for the processing of which no other legal basis has arisen.

The general rules on the retention times based on the applicable statutory regulations and the Bank's legitimate interest are detailed below.

The various specific retention times relating to the various data processing purposes are identified in the Bank's privacy notices.

5.1. Retention based on legal obligations

- The documents specified in Act C of 2000 on Accounting (**Accounting Act**), including, in particular, accounting documents underlying the accounting records directly or indirectly and the records required by law must be retained in a legible form and in a retrievable way for at least 8 years (Sections 165, 166 and 169 of the Accounting Act). Pursuant to Section 166 (1) of the Accounting Act accounting documents include invoices, contracts, agreements, statements, credit institution certificates and bank statements, the retention of which is regulated by the prevailing provisions of the Accounting Act.

- Section 57 (1)-(3) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (**AML Act**) provides that personal data, documents, copies, including documents obtained by the controller as part of the electronic identification process, must be retained by the Bank for a period of 8 years.

- In the cases[1] specified in Section 58 of the AML Act the retention time is 10 years.

- Pursuant to Section 9 (1) and Section 18 (1) of ***MNB Decree 26/2020. (VIII. 25)*** *on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests,* the entire communication between the service provider and the Data Subject during the use of the service via an electronic

[1] At the request of the supervisory authority (MNB), the financial intelligence unit (NTCA), the investigating authority, the prosecution service or the court.

communications device and during the associated direct and/or indirect customer due diligence process, the detailed information provided for the Data Subject in regard the indirect or direct electronic due diligence process and the Data Subject's express consent to this are recorded by the Bank in the form of video and audio recordings. For the retention of the video and audio recording the Bank observes, and complies with, the 8-year retention period prescribed in the AML Act, if customer due diligence takes place and the 8-year retention period prescribed in the Accounting Act, if a contract qualifying as an accounting document is signed.

5.2. Retention based legitimate interest

- As regards contracts that failed to be executed, the financial institution may, pursuant to Section 166/A of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (**Credit Institutions Act**) process data on the Data Subject constituting banking secrets and personal data relating to the service contract that failed to be executed as long as any claim can be enforced in relation to the contract's failure to be executed. Unless otherwise provided by law the general period of limitation specified in the Civil Code applies regarding the enforcement of claims; currently 5 years (Section 6:22 of the Civil Code).

- In lieu of any legal regulation stipulating a longer or a shorter retention time for the retention of personal data, the Bank considers the general period of limitation (5 years) set out in the Civil Code to be primarily applicable in other cases as well.

- The purpose of retaining personal data for the period of limitation (5 years) under the civil law based on legitimate interest is to make it possible to prove that the controller proceeded lawfully in processing and in its activity involving processing as well, also in view of the fact that the controller is under obligation to prove that processing is in accordance with the applicable legal regulations.

- Information on cases in which, in accordance with the principle of purpose limitation a shorter than 5-year retention period is prescribed for specific data processings, is contained in the relevant specific privacy notice.

6. WHO CAN ACCESS, WITH WHOM DO WE SHARE THE PERSONAL DATA OF THE DATA SUBJECTS

The personal data can be accessed by the Bank's employees for purposes required for the performance of their tasks who participate in the work aimed achieving and checking the purposes of processing or those acting in relation to representation; to the extent strictly necessary for their work (on a "need-to-know" basis).

In addition to the above, the personal data processed by the Bank may be transferred to other natural persons or legal entities ("**Recipients**"). The recipients may include public authorities, other authorities or other bodies performing public duties as well as courts to which personal data have to be disclosed in order to fulfil legal obligations, along with third party Processors

(e.g. GIRO Zrt. in the case of a GIRINFO query), persons performing outsourced activities, intermediaries).

The data processed by the Bank also qualify at the same time as banking, securities and payment secrets. The transfer of banking secrets is regulated by the relevant provisions of the Credit Institutions Act, that of securities secrets is regulated by Act CXXXVII of 2007 on Investment Firms and Commodity Brokers and on the Rules of their Activities (**Investment Firms Act**), while the transfer of payment secrets is regulated by the relevant provisions of Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (**Business Payments Act**).

The Bank transfers to third parties data qualifying as banking, securities or payment secrets only in cases prescribed by the relevant legal regulations.

Such data transfers may take place primarily in the performance of data supplies prescribed by law (to the Supervisory Authority, the Magyar Nemzeti Bank, competent authorities etc.) and in the context of responding to requests from authorities and others (court, notary public etc.) as well as in exercising controlling rights (when for instance the use of housing subsidies are checked by the Hungarian State Treasury, checks or audits by the tax authority etc.).

Personal data may also be transferred in the context of the fulfilment of legal obligations (e.g. supply of data to the Magyar Nemzeti Bank, the Hungarian State Treasury etc.).

In performing credit institutions' activities in relation to cross-border payment transactions and other international financial transactions, the Credit Institution uses the services of the SWIFT system – in accordance with the sectoral practices –, when in relation to the said operations and the performance of service contracts the data subjects' personal data relating to the given financial transaction can be transferred abroad. Further information on the processing activities of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system is available on the company's web page. (https://www.swift.com/about-us/legal/compliance-0/data-protection-policies).

7. DATA PROCESSING

In providing certain services or performing certain activities, the Bank uses the services of third parties (e.g. IT services, performance of operation-related tasks), during which the partner in contractual relationship with the Bank performs data processing at the instructions of the Bank and, therefore, qualifies as the Data Processor of the Bank. In performing its activities, the Data Processor may, in certain cases, have access to and is entitled to become familiar with the Data Subject's personal data.

Data Processors process personal data under contracts concluded with the Bank, for and on behalf of the Bank, for specific purposes specified by the Bank. The Bank engages only Data Processors who or which provide adequate guarantees for the protection of personal data in the contract concluded with them.

The Data Subject's personal data are transmitted typically to the following recipients:

- entities providing IT system support services;
- service providers performing data storage, archiving, filing and destruction activities;
- legal representatives, lawyers;
- entities providing mail, delivery and document management services;
- entities providing printing house services, which make customer certificates and information brochures;
- companies personalising and producing bank cards;
- companies providing payment services;
- debt collectors and bailiffs.

8. OUTSOURCED ACTIVITIES

With the authorisation under Section 68 of the Credit Institutions Act (Hpt.), the Bank may outsource activities during which data processing is carried out and which are associated with its own activities subject to compliance with the data protection regulations. Additional information on the data processors performing outsourced activities for the Bank is to be found in subsection 4.6 of MKB Bank Nyrt's General Business Rules.

Data transmission as required for the performance of outsourced activities, to entities performing outsourced activities and to data processors retained by such entities, is not – according to Section 164 (j) of the Credit Institutions Act – regarded as violation of banking secrets.

9. INTRA-GROUP DATA SHARING

Intra-group data processings between MKB Bank and the members of the MKB Bank Financial Group:

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Acceptance of the results of customer due diligence assessments carried out by other service providers.	Data Subject's consent (Article 6 (1) (a) of the GDPR)	Data involved in customer due diligence as well as other data required for the establishment of customer relationship, provided by the Data Subject.	Until consent is withdrawn. Before the withdrawal of consent the eight years specified in the AML Act (or 10 years in cases specified in the same) following the discontinuation of the business relationship.
Sharing bank secrets with partners in the Bank's sphere of proprietary interests, not operating under controlling influence and strategic partners to enable them to know all details required for the establishment of the	Data Subject's consent (Article 6 (1) (a) of the GDPR)	The data content contained in the declaration of consent.	Until consent is withdrawn.

business relationship.			
Sharing of banking secret with institutions under controlling influence of the Bank to enable them to know all details required for the establishment of the business relationship.	The legitimate interest of the Bank and the institutions operating under its controlling influence relating to contacting each other's customers as specified in Section 164/B (1)-(3) of the Credit Institutions Act. (Article 6 (1) (f) of the GDPR)	Data required for contacting customers	During the term of the customer relationship, not beyond the date on which the declaration of prohibition as specified in Section 164/B (4) is made
Consolidated supervisory compliance	The binding legitimate interest relating to the ensuring of consolidated supervisory compliance and, in the case of an audit, proving such compliance (Article 6 (1) (f) of the GDPR)	The data required for consolidated supervision according to Sections 172-176 of the Credit Institutions Act	8 years

Pursuant to Section 164/B of the Credit Institutions Act, the Bank and financial institutions, payment institutions, electronic money institutions, investment enterprises, insurers, AIFM and UCITS fund managers operating under its controlling influence, may mutually access the Data Subjects' personal data, their data regarded as bank, securities, payment and insurance secrets, as well as those regarded as business secrets, in connection with the performance of their business activities, to the extent required for the performance of their services, and the controllers participating in joint processing may transfer such data to each other in accordance with their respective general contractual terms and conditions in order to provide access to specific individual services, and process the data so received, during the period of the establishment and maintenance of the customer relationships concerned, in which case both MKB Bank Zrt. and the above enterprises in its sphere of interests must equally be regarded a controllers.

The prevailing list of the legal entities operating under the Bank's controlling influence, regarded as financial institutions, payment institutions, electronic money institutions, investment enterprises, insurers, AIFM or UCITS is presented in a separate notice on the web page www.mkb.hu.

Based on the Customer's prior specific authorisation, the Bank also has the right to transfer data to further companies in its sphere of interests not operating under its controlling influence and to other companies engaged in strategic cooperation with the Bank. The list of such entities is contained in a separate notice at the web page www.mkb.hu.

The Data Subjects have the right to restrict or prohibit the above data transfers by their express declarations at any time. Declarations restricting or prohibiting data transfer can be submitted by e-mail addressed to ugyfelszolgalat@mkb.hu or be made by phone on workdays between 8:00 and 17:00 at the toll-free number +36 (80) 350-350, or by mail, addressed to MKB Bank Nyrt., H-1134 Budapest, Kassák Lajos u. 16-18. .

10. JOINT DATA PROCESSING

In case the Bank performs data processing together with another controller, it specifically notifies this to the Data Subject in a special notice; such notification shall specify the key elements of the agreement between the Bank and the other controller.

In the case of joint data processing the Data Subject can exercise their rights specified in Section 11 with regard to each controller, regardless of the above-mentioned agreement.

11. RIGHTS OF THE DATA SUBJECT

In accordance with the GDPR the Data Subjects are – if specific conditions are met – have the right to:

- receive information about the processing of their personal data;
- request access to their personal data;
- request rectification of their personal data;
- request erasure of their personal data;
- request restriction on the processing of their personal data;
- request data portability;
- object to the processing of their personal data (including objection to profiling, and other rights relating to automated decision making).

The Controller informs the Data Subject without undue delay, but not later than within one month of receipt of the request for exercising the rights set out in this section, about the measures taken in response to the request. If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by an additional two months. The Controller informs the Data Subject about the extension of the deadline, with an indication of the reasons for the delay, within one month of receipt of the request. If you submitted your request electronically, the Controller provides the information electronically wherever possible unless you request otherwise.

If the Controller does not take measures after the submitted request, it informs you about the reasons for not taking any measures and where you can lodge your complaint and what other right to legal remedy you are entitled to without delay, but not later that within one month of receipt of the request.

The Controller provides the information to be provided on the basis of requests relating to the rights set out in this section as well as the fulfilment of the request free of charge. The Controller may charge a reasonable administrative fee for fulfilling the request if it is clearly unfounded or, especially due to its repetitive nature, excessive, or may refuse to act on the request. A request submitted on the same subject within 3 (three) months must be considered repetitive.

If the Controller has reasonable doubts about the identity of a natural person submitting a request for exercising the rights set out in this section, it may request the provision of additional information necessary to confirm the identity of the Data Subject.

The Controller informs all Recipients to whom or which the Data Subject's personal data have been disclosed, about any rectification, erasure or data processing restriction as per the rights specified in this section, unless this is not possible or would take disproportionately great efforts. At your request you will be notified of the Recipients.

11.1. Rights of information

- If the Controller has collected the personal data from the Data Subject, it provides detailed information – in addition to the Notice – on the circumstances of processing with content specified in Article 13 of the GDPR (detailed in subsection 11.2 below) at the time of obtaining the personal data in the privacy notices relating to the activity/service involving data processing.

- If the personal data processed by the Controller are obtained not directly from the Data Subject
  In such cases the following is added to the content of the notice:

  - source of personal data;
  - categories of personal data.

  The Controller provides information – of the above content – for the data subjects within a reasonable time limit after obtaining the personal data concerned.

  - If the Controller uses the personal data for communication with the Data Subject, it provides the information at least when it first contacts the Data Subject.
  - If the data are expected to be communicated to other recipients as well, the Controller provides the information upon the first such communication.

  The information must be provided for the data subject not later than within one month of obtaining the data; i.e. the above time limits shall be within such one-month period.

11.2. Right of access

The Data Subject may ask the Controller to provide information on the processing of their Personal Data. If the Controller processes your Personal Data, it makes the following information available to you:

- the purpose(s) of the processing;
- categories of the processed Personal Data;
- categories of Recipients;
- if applicable (e.g. data storage is involved), the planned duration of the storage of Personal Data or if the planned duration cannot be determined yet at the moment

when information is provided on exercising the right of access, the criteria used to determine that period;
- your rights to rectification, to erasure, to restriction and to object;
- your right to lodge a complaint with the supervisory authority;
- if the source of the Personal Data is not the Data Subject, all available information about the source of the Personal Data;
- information whether automated decision-making is carried out or not carried out and, in the case of automated decision-making, non-technical information about the logic used and the significance and expected consequences of the automated decision-making.

In case the Personal Data of the Data Subject are transmitted by the Controller to a third country or to an international organisation, the Data Subject is entitled to being informed about the guarantees securing such data transmission. At their request the Data Subject is provided with a copy of their Personal Data processed by the Bank. For additional copies, the Controller may charge a reasonable fee based on its administrative costs.

11.3. Right to rectification

The Data Subject may request the Controller to rectify their incorrect Personal Data without delay or to supplement their Personal Data incomplete for the purposes of Data Processing.

11.4. Right to erasure

You may request that your Personal Data be erased in the following cases:

- the Personal Data are no longer needed for the purpose of which they have been originally processed;
- in the event of consent-based Processing, if you have withdrawn your consent and Processing has no other legal basis;
- you successfully object to the processing of your Personal Data in accordance with Section 11.7 of the Privacy Notice and there is no legitimate priority reason for Processing or you successfully object to the processing of your Personal Data for direct marketing;
- the processing of Personal Data was unlawful;
- the Personal Data have to be erased for fulfilling a legal obligation prescribed by EU or Member State law applicable to MKB Bank;
- we processed the Personal Data in respect of services relating to information society and offered directly to children.

11.5. Right to restriction of processing

The Data Subject has the right to obtain from the Controller restriction of Processing where one of the following applies:

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;

- the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
- the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; or
- the Data Subject has objected to Processing pending the verification whether the legitimate interests of the Controller override those of the Data Subject.

In the case of a successful objection, the Controller processes the Personal Data subject to the restriction, except for storage, only with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of another person's right or for reasons of important public interest of the EU or of a Member State.

If the processing of Personal Data is subject to restriction, we inform you in advance about the lifting of such restriction.

11.6. Right to data portability

In the following cases, the Data Subject is entitled to receive the Personal Data concerning them which they have provided to the Controller in a structured, commonly used and machine-readable format and is entitled to transmit it to another Controller:

- Processing is based on the Data Subject's consent or is required for performing an agreement to which the Data Subject is one of the parties or which is required for taking steps at the Data Subject's request before concluding the agreement; and
- the Processing is carried out by automated means.

11.7. Right to object

The Data Subject is entitled to object, on grounds relating to their particular situation, at any time to processing of their Personal Data, where such processing is for the public interest or is required for the purposes of the legitimate interests pursued by the Controller or by a third party, including profiling based on the above-mentioned provisions. In this case, the Controller may not continue to process the Personal Data unless Processing is warranted by compelling legitimate reasons, which take priority over the interests, rights and freedoms of the Data Subject or which are related to the establishment, exercise or defence of legal claims.

If the Personal Data are processed for the purposes of direct marketing, the Data Subject is entitled to object to the processing of Personal Data for this purpose, including profiling, at any time if it is related to direct marketing.

11.8. Right to automated decision-making

The Data Subject is entitled to opt out from any decision made exclusively on the basis of automated data processing – including, among other techniques, profiling – which would have a legal impact on, or otherwise significantly affect, the data subject, unless such decision:

- is necessary for entering into, or performance of, a contract between the Data Subject and the Controller;
- is permitted to be taken by EU or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or
- it is based on the Data Subject's explicit consent.

In case the Data Subject cannot exercise their right referred to above in this subsection, on account of automated decision making based on a contract or a consent, the Data Subject has the right to request human intervention on the part of the Controller to express their point of view and to contest the decision.

In the course of the credit rating procedure the Controller has the right to make automated decisions through assessing the customer's personal circumstances (including location of the place of residence, age, educational attainment, marital status, credit history, employment history, financial habits), such decisions having an impact on the outcome of the loan appraisal and the conclusion of the transaction. The purpose of the evaluation carried out by the Controller as part of the credit rating procedure (scoring) is to assess the circumstances relating to the customer's payment capability, payment habits and willingness and make its business decision in view of the customer's circumstances.

11.9. Right to withdraw consent

In the case of consent-based Processing, the Data Subject is entitled to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of Processing based on consent before its withdrawal.

11.10. The means of the exercising the rights relating to the protection of personal data

You can exercise your rights specified in Section 11 hereof in regard to the processing of personal data, in person or via an authorised representative at the branches of MKB Bank, via letters addressed to the Data Protection Officer, by telephone at the toll-free green number +36 (80) 350-350 between 8:00 and 17:00 on working days or by e-mail, at adatvedelem@mkb.hu. For submission at a branch you are kindly asked to use the form we have introduced for this purpose, which you can download from: www.mkb.hu/adatvedelmi-tajekoztatas.

12. DATA SECURITY MEASURES

The Bank must guarantee the safe and secure operation of its information system and the adequate protection of the data in accordance with the GDPR and Government Decree 42/2015. (III. 12.) on the protection of the information systems of financial institutions, insurance and reinsurance companies, as well as investment companies and commodity exchange service providers.

To protect and secure personal data the Bank provides for secure data processing through its internal regulations (on data and secret protection, information security, access authorisations etc.) along with technological, organisational, technical and training actions and measures.

These include, in particular, technologies constituting the IT security infrastructure, security access regulations, authorisation management systems limiting access authorisations to the extent required for work in the case of individual employees, certain segregations (e.g. separate processing of data obtained in the context of financial services and those obtained in the context of investment services), data leakage protection, the use of computer IDs, passwords, screen protection, logging etc.

For protection against certain risks (e.g. data phishing letters, viruses, spy programs etc.) the Controller uses screening programs. The use of such applications may in some cases result in the blocking of, for instance, private mails from the outside.

13. POSSIBILITIES OF LEGAL REMEDY

13.1. Lodging a complaint with the Bank

If the Data Subject considers that the Bank has not acted properly in relation to the processing of their data or is otherwise dissatisfied with the way the Bank processes their data, they have the right to submit to the Bank a complaint regarding data protection. Such complaint may be submitted at any branch or at any of the Bank's contact details listed in the introduction section of the Notice.

The Bank's Data Protection Officer investigates the Data Subjects' complaints regarding data protection and makes proposals for their reassuring resolution. If not satisfied with the Bank's management of their complaint, the Data Subject has other possibilities for legal remedy as detailed in subsections 13.2-13.3.

For more information on the Bank's complaint management procedure please visit www.mkb.hu/elerhetosegek/panaszkezeles.

13.2. Hungarian National Authority for Data Protection and Freedom of Information (NAIH)

Data Subjects may submit complaints in relation to the processing of their personal data to the National Authority for Data Protection and Freedom of Information (Hungarian acronym **NAIH** - H-1055 Budapest, Falk Miksa utca 9-11.; postal address: H-1363 Budapest, Pf.: 9.; e-mail: ugyfelszolgalat@naih.hu; telephone: +36 (30) 683-5969, +36 (30) 549-6838; +36 (1) 391 1400; fax: +36 (1) 391-1410).

13.3. Judicial remedies

If the competent supervisory authority does not consider the Data Subject's complaint or does not provide information on the procedural developments relating to or the result of the submitted complaint within three months, or the Data Subject believes that the processing of Personal Data relating to them by the Controller infringes their rights to the protection of personal data, they are entitled to initiate court proceedings.

In this case, the court proceedings against NAIH have to be initiated before the Metropolitan Court of Budapest or the county court with jurisdiction at your habitual residence.

If your rights are infringed, court proceedings against MKB Bank have to be initiated also before the Metropolitan Court of Budapest or the county court with jurisdiction at your habitual residence.

14. OTHER CIRCUMSTANCES

This privacy notice is effective from 1 April 2022 until withdrawal. MKB Bank may modify this Notice at any time, simultaneously with informing the Data Subjects. Information on any modification of the Notice will be notified to our customers at www.mkb.hu and in the branches.

Annex 1

Terms relating to data protection

Data Controller: the organisation specified in the Introduction section of the Notice

Data Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

Occasional customer: any person depositing cash amount at any branch, who does not have a contract with the Bank and is not involved in any banking transaction with the Bank either.

Recipient: the person, public authority or another body to whom or which the Personal Data are disclosed by the Data Controller, whether or not the Recipient is a third party other than the Data Controller or the Data Subject. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. Magyar Nemzeti Bank during its investigations carried out within its supervisory powers) do not qualify as Recipients.

Data Subject: identified or identifiable natural persons regarding whom the Controller processes any information qualifying as Personal Data. An identifiable natural person is one whose identity can be established directly or indirectly, particularly with the help of some identifier such as name, date of birth, online ID (e.g. IP address) or one or more factors pertaining to their bodily, physiological, genetic, intellectual, economic, cultural or social identity.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

Consent: a voluntary, specific, unambiguous declaration of intent based on adequate information whereby the data subject unequivocally states that they consent to the processing of personal data relating to them.

Hpt.: Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises.

MKB Bank Financial Group: MKB Bank Nyrt., MTB Magyar Takarékszövetkezeti Bank Zrt., Takarékbank Zrt. and Takarék Jelzálogbank Nyrt., together with the legal entities covered by financial sectoral legal regulations in which the aforementioned have direct or indirect qualifying holdings.

Personal Data: any information relating to the Data Subject, on the basis of which the Data Subject is directly or indirectly identifiable.

Notice: this Privacy Notice.

Terms not specifically defined and not capitalised in the Notice have the meanings ascribed to them in the GDPR.

Annex 2

INFORMATION ON DATA PROCESSINGS FOR WHICH NO SPECIFIC NOTICES ARE AVAILABLE

1. Querying of contact data (home address) available in public databases and sending letter calling for reconciliation of contact data

If the Data Subject has failed to fulfil their obligation to notify changes in their contact data, as a consequence of which the Bank, which has a contract in place with them, has no contact data at which it could contact them in the context of the cooperation obligation relating to performance of the contract, the Controller has the right to carry out the following query (data processing operation).

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	SOURCE OF DATA	DATA RETENTION PERIOD
Recording the Customer's home address data for the purpose of contacting them	Performance of the contract concluded with the Data Subject (first part of Article 6 (1) b) of the GDPR)	Home address	Use of the GIRinfO Data Processing Service (GIRO Zrt., company registration number: 01-10-041159, registered office: H-1054 Budapest, Vadász u. 31.)	In lieu of any other statutory provision concerning the processing of personal data generated during the existence of the customer relationship, 5 years from the end of the customer relationship (Section 6:22 of the Civil Code)

Since this data is not provided for the Bank by the Data Subject, the Bank provides the Data Subject with detailed information on processing at the time and with the content specified in Article 14 of the GDPR. In this case the data subject is informed in the letter calling them to reconcile data (when the first contact is made), but not later than within 1 month of the query of the home address from the public database.

2. Processing of personal data in a test environment

For the continuous maintenance and development of its information systems the Bank performs testing and fault-finding procedures in a test environment separated from the live environment.

In case personal data from the live system also need to be used for the procedures taking place in the test environment, the processing of such live data (e.g. customer data) in the test environment qualifies as a legitimate purpose of processing on its own, which is separate from the original purpose of processing of the same (e.g. the performance of the contract).

As a general rule, the Bank processes such personal data in the separated test environment only after complete depersonalisation.

The natural person to whom the depersonalised data relates cannot be identified; the connection between the data and the data subject is irrecoverably terminated, i.e. they constitute no data protection risk whatsoever regarding the rights and freedoms of the data subject concerned. The GDPR does not apply to such depersonalised data.

In case the given testing or development procedure fails with depersonalised data – i.e. without processing – the Bank processes personal data taken from the live environment in the following way in the separated test environment.

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Repair of defects of the live information system.	The Controller's legitimate interest relating to the operation of its information systems (and, in relation to this, the comprehensive provision of its services). (Article 6 (1) (f) of the GDPR)	Customer data, employee data (e.g. ID data, financial data) taken from the live system, indispensable for the rectification of the error.	After the rectification of the error the data are erased from the test environment.
Development of the live information system.	The Controller's legitimate interest relating to the operation of its information systems (and, in relation to this, the comprehensive provision of its services). (Article 6 (1) (f) of the GDPR)	Customer data, employee data (e.g. ID data, financial data) taken from the live system, indispensable for the development.	After the implementation of the development the data are erased from the test environment.

Data security measures applied by the Bank for the above data processing purposes:

- Testing takes place in an environment separated from the live operating environment; the Bank provides for the separation of the testing environment at database and network level as well.
- The control mechanisms covering the test environment are the same as – in some cases stricter than – those applying to the live systems.
- Moreover, in the case of such processing operations the Bank guarantees adequate protection of the personal data by restricting access, by allocating adequate access authorisations and encryption.

3. Complaints Management

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Compliance with the statutory obligations relating to complaint management	Fulfilment of the legal obligation as per Article 6 (1) c) of the GDPR as specified in Section 288 (1) of the Credit Institutions Act and Section 121 (1) of the Investment Firms Act.	The data specified in Section III of Annex 1 to MNB Decree 46/2018. (XII. 17.) on the form and way of complaint management by certain financial organisations issued on the basis of the authorisation granted by the Credit Institutions Act and the Investment Firms Act, along with other data supplied by the complainant.	5 years of submission of the complaint

4. Processing of the data of occasional customers

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Prevention and combating money laundering and terrorist financing (Section 14 (1) of the AML Act)	Fulfilment of the legal obligation as per Article 6 (1) c) of the GDPR Section 14 (1) of the AML Act	Data specified in Section 14 (1) of the AML Act (family name, surname, place and date of birth, subject and amount of the order)	The 8 years prescribed in Section 57 (3) of the AML Act

Moreover, the credit institution may ask presentation of the documents specified in Section 7 (3) of the AML Act, such as in the case of natural persons who are

- Hungarian citizens, their official card suitable for identification and official address card, the latter if their domicile or residence is in Hungary;
- foreign citizens, their travel document or identity card, provided that it authorises its holder to reside in Hungary, and their document certifying the holder's residence right or document authorising the holder to reside in Hungary, or their official address card proving their residence in Hungary if their domicile or residence is in Hungary.

5. Cookies

MKB Bank uses cookies on its web pages to enable proper functioning of the pages and facilitate the development of its services. Cookies deployed on the user's computer qualify as their personal data.

When a user visits an MKB Bank web page, the Controller deploys a small data package, a so-called cookie on the user's device. When the user returns to the page later, on the browser returns the cookie saved previously, so the service provider managing the cookie can connect the user's current visit with the previous ones, but only in relation to its own content.

There are various kinds of cookies.

- Some cookies are indispensable for the operation of the web page.
- Others collect information on the use of the page to make the use of the page even more convenient and user-friendly, and to be able to provide even more relevant services for the data subjects.
- Temporary cookies are automatically erased when the browser is closed.
- Permanent cookies may remain on the user's device for a longer period of time.

For more information on cookies used by MKB Bank, please visit: www.mkb.hu/

6. Fraud detection

Section 107 (1) of the Credit Institutions Act stipulates that credit institutions must have effective and reliable corporate governance systems and internal controlling functions to ensure – *inter alia* – their undisturbed and effective operation, the maintenance of confidence in them and the protection of the shareholders' and customers' economic interests and social objectives relating to them.

As a credit institution, MKB Bank is specifically exposed to attempts of fraud and other violation, which, if successful, might erode confidence in the institution and materially violate the economic interests of the customers and, ultimately, the shareholders as well.

Accordingly, MKB Bank keeps records of all attempts of fraud and misuse; such records necessarily include personal data as well. The controller uses the list for avoiding the establishment of business relationships that could likely lead to (additional) losses to it. The details of data processing are summed up in the table below:

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Identification of fraud and other attempts of abuse, avoidance of losses	The legitimate interest of the protection of (public) confidence in the institution and the protection of the investments of the customers and the shareholders, as specified in Article 6 (1) f) of the GDPR.	Identification data of perpetrators, the date/time and the nature of the abuse	In accordance with the retention of negative information in the CCIS (Hungarian: KHR) (10 years)

Data protection guarantees applied by the Bank as specified in this section:

- The database can be accessed by a very few people involved in fraud prevention activities;
- Being present in the database does not entail automatic rejection of the request for the establishment of a customer relationship or, in certain cases, other actions (e.g. increased scrutiny of the documents submitted by the customer) may be sufficient for managing the risk.

7. Dispute settlement

The Bank uses its best efforts to resolve legal disputes between the parties through settlement; if however, such efforts fail, any court proceedings or any other proceedings of other competent authorities or conciliation bodies will necessarily involve data processing for purposes other than the original (typically: contractual) ones.

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Establishment, exercise or defence of legal claims	The legitimate interest associated with the settlement of disputes, as specified in Article 6 (1) f) of the GDPR.	Personal data recorded in documents and other pieces of evidence of relevance to the legal dispute	5 years from the final and binding closure of the legal dispute (objective revision renewal deadline)

8. Internal loans

To provide for the prudent operation of credit institutions Section 106 of the Credit Institutions Act stipulates that a credit institution must apply special rules on risk taking regarding members its managing body, its auditor, close relatives and business interests of such persons and apply effective procedures to ensure, *inter alia*, the identification, registration, monitoring and notification to the Supervision, of risk exposures.

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Fulfilment of the regulation laid down in Section 106 of the Credit Institutions Act regarding internal loans.	The legitimate interest relating to the management of internal loans in accordance with the applicable statutory regulations, as specified in Article 6 (1) f) of the GDPR.	The data of the members of managing bodies potentially involved in internal borrowing, and those of the auditor, the data content of risk taking qualifying as internal loans (typically those contained in proposals and loan agreements), data recorded during the monitoring of transactions.	Until the termination of the internal credit rating for the risk exposure.

9. Voice recordings

To provide its customers with services and information, the Bank operates a telephone customer service. In certain telephone lines the Bank operates voice recording system, of which the customers are notified at the beginning of the call. The telephone customer service is, primarily, a channel for communication and since calls of multiple purposes can be made through this channel, the purpose and legal basis of processing, the data being processed etc. must and can be determined primarily on the basis of the content of the call.

Recordings of complaints shall be retained for 5 years based on legal obligation, taking client orders fall within the performance of contracts, marketing related declarations are based on the client's respective consent, etc.

Regardless whether the communications is via telephone or any other channel, the notifications pertaining to certain product categories are provided in this privacy notice and in special notices provided for particular services.

In addition to the above, the purpose of the processing is to prove what information has been provided to the customer, and to improve coworkers activities, too. Providing clients with complete information and of adequate quality is the interest of both the clients and the Bank, and at the expectation of the Hungarian Central Bank – as supervisory authority – at the same time. Considering the specialties of the channel, providing hard copy notification to the client is not possible, thus in case of those telephone lines affected by a large number of calls or is used for special purposes, the purpose of the processing is the Bank's legitimate interest (Article 6 (1) f) of the GDPR) and in the event of inadequate information of the client, failure of recording a complaint or of any other error it is also an opportunity for the client to enforce his/her rights. Taking these circumstances into consideration, the retention period in case of such purposes corresponds to the general limitation period of civil claims (5 years).

PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	CATEGORIES OF PROCESSED DATA	DATA RETENTION PERIOD
Establishment, exercise or defence of legal claims referred to in the call.	The legitimate interest associated with the settlement of disputes, as specified in Article 6 (1) f) of the GDPR.	Audio recording, and the data and legal declarations of relevance to the legal dispute so recorded.	5 years
Fulfilling the orders given by the customer in the call and other administrative procedures relating to the contract	Performance of the contract specified in Article 6 (1) b) of the GDPR	The customer data given by the customer for the performance of the order and the customer's voice.	8 years
Complaints management	The legal obligation as specified in Section 288 of the Credit Institutions Act and Section 121 of the Investment Firms Act The legal obligation as per Article 6 (1) c) of the GDPR	The data specified in point III of Annex 1 to MNB Decree No. 66/2021. (XII. 20.), as well as other data provided by the complainant, and the complainant's voice.	5 years