GENERAL

PRIVACY NOTICE

INTRODUCTION, DATA AND CONTACT DETAILS OF THE CONTROLLER

MBH Bank Nyrt. (hereinafter the **Bank** or the **Controller**) considers the protection of personal data a high priority area, and therefore, taking into account the nature, scope, context and purposes of the Bank's activities involving data processing, as well as the rights and freedoms of Data Subjects in relation to the protection of their personal data, the Bank has established an internal Privacy Policy in accordance with Article 24(2) of the GDPR, the purpose of which is to ensure that the Controller complies with the laws and recommendations on the processing of personal data throughout the entire data processing process.

The Bank's internal data protection rules apply to all processes involving the processing of personal data, whether performed electronically or manually, by all its organisational units and accordingly all internal rules of the Bank are drawn up and applied in accordance with its Privacy Policy. The Bank informs the Data Subjects of its data processing practices, designed and implemented in accordance with its internal regulations, by means of privacy notices.

The purpose of this privacy notice (hereinafter: "**Notice**") is to provide transparent and comprehensible information to natural persons ("**Data Subjects**") who come into contact with MBH Bank Nyrt. in accordance with the General Data Protection Regulation 2016/679/EU ("**GDPR**") on the circumstances of the personal data processing performed by the Bank, such as the purpose, legal ground and duration of the processing, the persons entitled to access the data, the Recipients to whom the data may be transferred, and the rights and remedies available to the Data Subjects in connection with the processing of their personal data.

Please read the Notice carefully and if you have any further questions, please contact the Bank's Data Protection Officer at the contact details below. Important concepts relating to data protection are listed in Annex 1.

DATA OF THE CONTROLLER

Name of the Controller	**MBH Bank Nyrt.**
Registered office	(**Bank** or **Controller**) 1056 Budapest, Váci u. 38.
Central contact details	E-mail: ugyfelszolgalat@mbhbank.hu Phone number: +36 80 350 350 (**Telebank**)
Website	mbhbank.hu
Company registration number	01-10-040952

CONTACT DETAILS OF THE DATA PROTECTION OFFICER

Postal address	5600 Békéscsaba, Andrássy út 37-43
E-mail address	adatvedelem@mbhbank.hu

Given that the nature, scope and/or purposes of the Bank's activities require regular and systematic processing of Personal Data of Data Subjects on a large scale, the Bank has appointed a Data Protection Officer in accordance with Article 37 of the GDPR. The Data Protection Officer monitors the Controller's compliance with the law and internal privacy rules relating to the processing of personal data, primarily taking into account the interests of the Data Subjects of the processing. The Bank ensures that the Data Protection Officer is involved in matters involving data processing in due time. The Data Protection Officer reports to the Bank's senior management.

If you have any requests, questions, complaints or applications to exercise your rights regarding the protection of your personal data, you the Data Subjects may contact the data protection officer, using the above contact details.

1. BASIC PRINCIPLES

Personal data may be collected, stored, processed and transferred or any other operation performed on the data (**Processing**) only if the purpose of the processing is sufficiently specific and legitimate, the legal ground for the processing is available and the lawfulness of the processing is ensured for the entire duration of the processing. The Bank, as controller, is responsible for ensuring that the following principles are complied with in relation to the processing:

- ensure that, in all its processing, personal data are processed in accordance with the principles of lawfulness, fairness and transparency.
- any processing of personal data must be performed only for a clear and specific purpose and must not be used for other purposes incompatible with the original purpose; the purposes and means of the processing and the necessity of the processing must be proportionate and adequately documented.
- the processing of personal data must be limited to what is necessary for the purposes for which the data are processed.
- personal data must be up to date and accurate, and all reasonable efforts must be made in the procedures to correct or erase inaccurate or outdated personal data.
- personal data should be stored only for a period of time adequate for the purposes for which the data are processed; the processing of personal data is prohibited after the expiry of the period of processing.
- personal data must be processed in a way that ensures the rights of data subjects, data availability, integrity and confidentiality.
- the Bank, as data controller, is responsible for compliance with the requirements of the GDPR and for demonstrating compliance (accountability).

2. DATA SUBJECT CATEGORIES

In this capacity, the Data Controller processes personal data of the following categories of Data Subjects:

2.1. Natural persons who have contacted the Data Controller in order to obtain a product or service:

- The contractual relationship is established between the Bank and the Data Subject (e.g.: debtor; account holder; bank cardholder).
- A contractual relationship is not established between the Bank and the Data Subject (e.g. credit applicants; account openers).

2.2. Data Subjects who do not require the Bank's products or services but who enter into a contractual relationship or transaction with the Bank

- Natural persons who are not customers (e.g. guarantors, pledgers) in respect of a contract for the use of services, including, in the case of legal persons, natural persons who have entered into a contract for ancillary obligations, and casual customers.

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

- Third parties involved in the use of the services and in the conclusion of the related contract (e.g.: proxy, witness, legal representative, guardian, custodian, name writer, interpreter).
- Natural persons who come into contact with the Bank for purposes other than the use of the Bank's services (e.g.: casual customers, representatives under the AML Act, external members of the Supervisory Board, shareholders, persons subject to statutory authority, court proceedings, etc. natural persons included in requests for information, sellers, beneficial owners and lessee, Data Subjects in the view of a camera, representatives. contact persons, persons assisting in the performance of the loan of contractual partners not involved in a customer relationship, minor children living in the same household as the loan applicant in the case of subsidised loans).

These categories of data subjects are equally entitled to the data subjects' rights set out in the Notice, including the right to information, which the Data Subject may obtain from the specific information notice on the processing given at the start of the processing.

3. SOURCE OF PERSONAL DATA

The Data Controller processes the personal data of Data Subjects primarily on the basis of the communication by the Data Subjects (when using a service, in the course of entering into a contract, in the course of maintaining contact, etc.). It is possible that, in the course of certain transactions,

personal data may also be obtained in part from third parties (in particular from a court or other authority).

In addition to the data provided by the Data Subjects, the Data Controller collects additional data from public registers containing data about the Data Subjects or, where it can demonstrate a right or legitimate interest, from records accessible to any person or lawfully established from such registers.

Where the Controller collects personal data relating to the Data Subject from a source other than the Data Subject, the Controller shall provide the Data Subject with the information required under Article 14 of the GDPR, in particular information on the source of the personal data and, where applicable, whether the data originate from a publicly accessible source.

4. THE PURPOSES AND LEGAL GROUNDS OF THE PROCESSING IN GENERAL

The processing carried out by the Bank is performed for the purposes of the provision of services by the Bank, the fulfilment of legal obligations and data reporting and, in certain cases, for the legitimate interests of the Bank or third parties. Processing by the Bank is generally performed on the following legal grounds:

- on the basis of the Data Subject's prior, informed, voluntary, specific, unambiguous **consent** to the processing, expressed by an active act of the Data Subject (e.g. processing for direct marketing purposes);
- for the **performance of a contract** for the use of certain services provided by the Bank (e.g.: conclusion of a bank account agreement);
- to **comply with any legal obligations** applicable to the Bank (e.g. 8-year retention period required by the AML Act); and
- in certain cases, on the basis of a **legitimate interest of the Bank or a third party** (e.g. operation of a security CCTV system).

Detailed information on specific data processing in connection with the Bank's services, broken down by products, services and activities, is provided in separate (special) privacy notices (www.mbhbank.hu/adatvedelem).

For data processing for which no specific information is available, further details can be found in Annex 2 of the Notice.

If the limitation period of the validity of the request in the special notice is indicated as the final date of the duration of the Data Processing, this shall be interpreted as that the act interrupting the limitation period extends the period of the duration of the processing of personal data until the new date on which the limitation period ends.

4.1. Processing of special data

Special categories of personal data are processed with increased care by the Bank. Special categories of personal data:

a) Data concerning racial or ethnic origin;
b) Political, religious or philosophical beliefs;
c) data relating to trade union membership;
d) Biometric data for the purpose of uniquely identifying data subjects; and
e) genetic data;
f) Health data; and
g) Data concerning sexual life or sexual orientation.

The Bank does not process personal data falling under the special categories of data referred to in points a), b) e) and g) above, and the processing of data referred to in points c) and d) and f) is only permitted if the data subject has given their explicit consent to the processing or if one of the following conditions for the processing set out in Article 9 of the GDPR is met:

a) complying with obligations and exercise of rights arising from legal provisions governing employment, social security and social protection;
b) the protection of the vital interests of the data subject or of another natural person if the data subject is physically or legally incapacitated and is unable to give their consent;
c) in the context of the activities of a foundation, association or any other non-profit organisation with political, philosophical, religious or trade union aims, to its current or former members or to persons who have a regular contact with the organisation in relation to the purposes of the organisation and that the personal data will not be disclosed to persons outside the organisation without the consent of the data subjects;
d) the data have been explicitly disclosed by the data subject;
e) presentation, enforcement or defence of legal claims;
f) significant public interest;
g) for preventive health or occupational health purposes, to assess an employee's ability to work, to make a medical diagnosis, to provide health or social care or treatment, or to administer health or social care systems and services;
h) public interest that relates to public health; and
i) archiving in the public interest, scientific and historical research or statistical purposes

5. THE DURATION OF DATA PROCESSING

As a general rule, the Bank shall process adequate and relevant personal data collected from Data Subjects for a legitimate purpose and which are strictly necessary for that purpose for the time necessary to achieve the purpose of the processing.

The Bank is obliged to delete and erase all personal data relating to the Data Subject which processing has ceased to serve a purpose and for which no other legal ground for processing arises.

The general rules on retention periods based on law and the Bank's legitimate interest are described below.

The specific retention periods for each processing purpose are set out in the information notices on processing

5.1. Data retention on the basis of legal obligations

- Documents pursuant to Act C of 2000 on Accounting (**Accounting Act**), in particular accounting documents directly and indirectly supporting the accounting statements and records required by law, shall be kept by the Bank in a readable and retrievable form for at least 8 years (Sections 165, 166 and 169 of the Accounting Act). Pursuant to the provisions of the Accounting Act (Section 166 (1)), invoices, contracts, agreements, statements, credit institution document and bank statements shall be considered accounting documents, the retention of which is subject to the current provisions of the Accounting Act.

- Pursuant to the provisions of Section 57 (1)-(3) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (**AML Act**), the Bank shall keep personal data, documents and copies processed in connection with the business relationship, including documents obtained by the data controller during electronic identification, for a period of 8 years.

- In the cases specified in Section 58 of the AML Act, the[1] retention period shall be 10 years.

- The Bank shall record all communications between the service provider and the Data Subject during the use of the service to be used via electronic communication means, the related customer due diligence pursuant to Section 9 (1) and Section 18 (1) of ***MNB Decree 26/2020 (25 August)*** *on the Detailed Rules on the Implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing applicable to service providers supervised by the MNB and on the minimum requirements applicable to the development and operation of the screening system stipulated in the Act on the Implementation of Financial and Asset Restrictions Ordered by the European Union and the UN Security Council*, and the detailed information of the Data Subject in connection with the direct or indirect electronic customer due diligence and the Data Subject's express consent thereto in a retrievable manner in the form of video and audio recordings. The Bank shall consider the retention period of 8 years in accordance with the AML Act to be decisive for the retention of the image and audio recording in the case of customer due diligence, and 8 years in accordance with the Accounting Act in the case of the conclusion of a contract that constitutes an accounting document.

[1] In the case of a request by a supervisory authority (MNB), the Financial Intelligence Unit (NAV - National Tax and Customs Administration), the investigating authority, the public prosecutor's office and the court.

5.2. Data retention on the basis of legitimate interest

- Pursuant to Section 166/A of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (**CIFE Act**), the financial institution may process the Data Subject's data and personal data that constitute banking secret in connection with the non-executed service contract for as long as the claim is enforced in connection with the failure to execute the contract. Unless otherwise provided by law, the general limitation period set out in the Civil Code, which is currently 5 years (6:22 of the Civil Code), shall apply for the purpose of claim enforcement.

- In the absence of a statutory provision specifying a longer or shorter retention period for the retention of personal data, the Bank shall regard the general limitation period (5 years) laid down in the Civil Code as the primary applicable period in other cases.

- The purpose of the retention of personal data for a civil law limitation period (5 years) based on legitimate interest is to enable the controller to prove that it has acted lawfully with regard to the processing or its activities entailing the processing, subject to the burden of proof that the processing is lawful.

- Where a retention period of less than 5 years has been specified for certain processing operations on the basis of the purpose limitation principle, information on this is provided in the relevant specific privacy notice.

6. WHO HAS ACCESS TO THE DATA SUBJECTS' PERSONAL DATA AND WITH WHOM IS IT SHARED?

The data may be known for the purposes necessary for the performance of their duties by those employees of the Bank who are involved in the implementation and monitoring of the processing purposes and who act in connection with representation to the extent strictly necessary for the performance of their work ("need-to-know").

Personal data processed by the Bank may be transferred to natural or non-natural persons other than the above ("**Recipients**"). Recipients may be public authorities, regulatory bodies, other organisations performing public tasks or courts to whom the transfer of personal data is necessary for the fulfilment of a legal obligation, as well as third party Data Processors (e.g. GIRO Zrt. in the case of GIRINFO queries) outsourcing their activities, the intermediaries.

The data processed by the Bank are also banking, securities and payment secrets. The transfer of banking secrets is governed by the CIFE Act, the transfer of securities secrets is governed by Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers and on the Regulations Governing their Activities (**Investment Services Act**), and the transfer of payment secrets is governed by the relevant provisions of Act LXXXV of 2009 on the Provision of Payment Services (**Payment Services Act**.

Data that classified banking, securities or payment secrets will only be transferred to third parties in the cases specified in the applicable legislation.

These data transfers may take place in the course of providing data required by law (Supervisory Authority, National Bank of Hungary, authorities, etc.), in connection with responding to requests from authorities or other requests (court, notary, etc.), or in the exercise of the right of control (e.g. control of housing state subsidies by the Hungarian State Treasury, tax authority control, etc.).

Personal data may also be transferred in the context of the performance of a legal obligation (e.g. providing data to the National Bank of Hungary, the Hungarian State Treasury, etc.).

In connection with cross-border payment transactions and other international financial transactions, the Credit Institution, in accordance with the industry practice, uses the services of SWIFT in the performance of the activities of credit institutions, in connection with which the personal data of the data subjects related to the financial transaction may be transferred abroad. For more information about SWIFT (Society for Worldwide Interbank Financial Telecommunication) data processing, please visit the company's website (https://www.swift.com/about-us/legal/compliance-0/data-protection-policies)

7. DATA PROCESSING

The Bank uses the services of third parties in the provision of certain services or activities (e.g., IT services, performance of operational tasks), during which the partner with a contractual relationship with the Bank performs data processing according to the bank's instructions, therefore it qualifies as a Data Processor of the Bank. In certain cases, the Data Processor may have access to and have the right to know the Data Subject’s personal data in the course of its activities.

The Processors process personal data on behalf of the Bank and for a specific purpose as defined by the Bank, on the basis of a contract with the Bank. The Bank uses only Data Processors who and which offer adequate contractual guarantees regarding the protection of personal data.

The Bank's internal privacy policy also covers the activities of Processors. The Processors provide the above-mentioned guarantees in the Data Processing Agreement in accordance with Article 28 of the GDPR, including in particular the obligation of cooperation of Processors in connection with the processing and the right of the Bank to audit the adequacy of the Processor's activities performed for the Bank at any time.

Personal data of Data Subjects is typically transferred to the following recipients:

- to IT system support service providers;
- to service providers engaged in data storage, archiving, filing and shredding activities;
- to legal representatives, lawyers;

- to providers of mailing, delivery and document management services;
- to printing service providers producing customer receipts and information leaflets;
- to companies personalising and manufacturing bank cards;
- to payment service provider companies;
- to debt managers and execution officers.

8. OUTSOURCED ACTIVITIES

With the authorisation pursuant to Section 68 of the CIFE Act, the Bank may outsource activities related to its activities, in the course of which data management or data processing is performed, in compliance with data protection regulations. The list of service providers that perform outsourced activities for the Bank is available **in the General Business Rules of MBH Bank Nyrt.**

Pursuant to Section 164 j) of the CIFE Act, the transfer of data necessary for the performance of the outsourced activity to the party pursuing the outsourced activity and to the data processor used by it does not constitute a breach of bank secrecy.

9. INTRA-GROUP DATA SHARING

Data processing within the group between MBH Bank and the members of the MBH Bank Financial Group:

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
The sharing of bank secrets with strategic partners within the Bank's sphere of interest, operating under non-controlling influence, or strategic partners in order to fully understand the information needed to establish a business relationship.	Consent of the data subject (Article 6 (1) a) of the GDPR).	Data content listed in the consent form.	Until consent is withdrawn.
Sharing of banking secrets between entities under the Bank's control in order to obtain full information necessary to establish a business relationship	The legitimate interest of the Bank and the institutions under its control to communicate with each other's customers pursuant	Data required for contacting customers	For the duration of the customer relationship, at the latest until the declaration of prohibition pursuant to Section 164/B (4) of the CIFE Act.

	to Section 164/B (1)-(3) of the CIFE Act. (Article 6 (1) f) of the GDPR).		
Supervisory compliance on a consolidated basis	Compelling legitimate interest to ensure compliance with supervision on a consolidated basis or to prove compliance in the event of an inspection (Article 6 (1) f) of the GDPR).	Data required for compliance on a consolidated basis pursuant to Sections 172-176 of the CIFE Act	8 years

Pursuant to Section 164/B of the CIFE Act, the Bank may have mutual access to the personal data, bank, securities, payment and insurance confidential data and business confidential data of the Data Subjects of financial institutions, payment institutions, electronic money institutions, investment firms, insurance undertakings, AIFMs and UCITS fund managers operating under its control, to the extent necessary for the provision of their services in the context of the performance of their activities, and may, in accordance with the general contractual conditions of the controllers participating in the joint processing, transfer the data to each other for the purpose of providing access to specific services and process the data thus received for the duration of the establishment and maintenance of the customer relationship, in which case both MBH Bank and the undertakings within the sphere of its interest shall be considered as controllers.

The list of legal entities under the control of MBH Bank and which qualify as financial institutions, payment institutions, electronic money institutions, investment firms, insurance companies, AIFMs or UCITS is set out in a separate notice available on the mbhbank.hu website.

On the basis of the Customer's prior and express authorisation, the Bank is also entitled to transfer data to other companies not under its control, which are part of its sphere of interest or which have a strategic cooperation with the Bank. The list of such companies is listed in a separate announcement on the following website: www.mbhbank.hu

The Data Subjects are entitled, at any time, to restrict or prohibit the transfer of data as described above by means of an explicit declaration. A statement on the restriction or prohibition of data

transfer can be sent to the e-mail address ugyfelszolgalat@mbhbank.hu or by calling the green number +36 80 350-350 free of charge on working days between 8 am and 5 pm, or by post, a mail sent to MBH Bank Nyrt., 5600 Békéscsaba, Andrássy út 37-43.

10. JOINT DATA PROCESSING

If the Bank performs the processing jointly with another controller, the Data Subject shall be informed separately in the special notice, which shall include the essence of the agreement between the Bank and the other controller.

In the case of joint data processing, it may exercise the rights set out in Section 11, independently of the aforementioned agreement, against each controller.

11. THE DATA SUBJECT'S RIGHTS

In accordance with the GDPR, Data Subjects are entitled to the following, subject to certain conditions:

- be **informed** about the processing of their personal data;
- request **access** to their personal data;
- request the **rectification** of their personal data;
- request the **erasure** of their personal data;
- request the **restriction** of processing of their personal data;
- request **data portability**;
- **object** to the processing of their personal data (including objection to profiling and other rights related to automated decision-making).

The Controller will inform the Data Subject of the measures taken following the request without undue delay, but no later than within one month from the receipt of the request to exercise the rights set out in this section. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Controller shall notify the Data Subject of any such extension within one month of receiving the request; such a notification shall include the reason of the extension. If you submit your request via an electronic channel, the Data Controller preferably sends the notification in electronic format unless you request a different format.

If the Data Controller fails to act upon the submitted request you will be informed without delay, but no later than within one month from the receipt of the request, of the reasons for not taking action and of where to turn to complain and what other legal remedies are available.

The Data Controller supplies the information to be provided on the basis of the requests related to the rights included in this section, as well as the fulfilment of the request free of charge. The Data Controller may charge a fair administrative fee in connection with the fulfilment of the contents of

the request, if it is clearly unfounded or - especially due to its repetitive nature - excessive, or it may refuse to take action on the basis of the request. A request submitted within three (3) months on the same subject shall be deemed to be repetitive.

In the event that the Data Controller has reasonable doubts regarding the identity of the natural person submitting the request for the exercise of 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 Data Controller shall communicate any rectification or erasure of personal data or restriction of processing performed to each Recipient under the rights specified in this Section, to whom the personal data of the Data Subject have been disclosed, unless this proves impossible or involves disproportionate effort. Upon request, you will be informed separately about these Recipients.

11.1. Right to information

- If the personal data have been collected by the Data Controller from the Data Subject, the Data Controller shall, in addition to the information contained in this Notice, provide detailed information in the privacy notices relating to the activity or service involving the processing, on the circumstances of the processing at the time of obtaining the personal data, with the content detailed in Article 13 of the GDPR (in Section 11.2 below).

- If the source of the personal data processed by the Controller is not directly the Data Subject In such cases, the information shall be supplemented by the following:

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

    The Controller shall provide the data subject with the above information within a reasonable period of time after obtaining the personal data.

    - If the Controller uses the personal data for the purpose of contacting the Data Subject, the information shall be provided at least at the time of the first contact with the Data Subject.
    - If the data are likely to be communicated to other recipients, the Data Controller will provide the information at the latest when the personal data are communicated for the first time.

    The information shall be provided to the data subjects within one month of the date of obtaining the data at the latest, and the above time limits shall therefore be understood to be within that one month.

11.2. Access rights

The Data Subject may request that the Controller provides information regarding the processing of your Personal Data. If the Controller processes your Personal Data, the following information is provided to you:

- the purpose(s) of the Data Processing activity;
- categories of Personal Data processed;
- Categories of Recipients;
- if interpretative (e.g., data storage takes place), the planned period of storage of the Personal Data, or if the planned period cannot be determined at the time of the information given regarding the exercise of the right of access, the criteria for determining this period;
- the rights to rectification, erasure, restriction and objection;
- the 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;
- whether or not automated decision-making has taken place, and in the case of automated decision-making, clear information on the logic used and the importance of automated decision-making and what the expected consequences are.

If the Controller transfers your Personal Data to a third country or international organisation, the Data Subject has the right to be informed about the guarantees of the transfer. Upon request, a copy of the Personal Data we process will be provided with you. The Data Controller may charge a reasonable fee based on administrative costs for additional copies.

11.3. Right to rectification

The Data Subject may request the Controller to rectify their inaccurate Personal Data without delay or to supplement their Personal Data that is incomplete for the purpose of Data Processing.

11.4. Right to erasure

You can request the erasure of your Personal Data in the following cases:

- the Personal Data is no longer required for the purpose for which it was originally processed;
- in the case of processing under consent, if you have withdrawn your consent and the Data Processing has no other legal ground;
- in accordance with Section 11.7 of the Notice, you successfully object against the processing of your Personal Data and there are no overriding legitimate grounds for Data Processing, or successfully object against the processing of your Personal Data for the purpose of direct marketing;
- the Personal Data was processed unlawfully;

- the Personal Data must be erased in order to fulfil a legal obligation under Union or Member State law applicable to the MBH Bank;
- we have processed Personal Data in relation to information society services offered directly to children.

11.5. Right to restriction of processing

The Data Subject has the right to have the Data Controller restrict the Processing if any of the following criteria apply:

- they contest the accuracy of the Personal Data, in which cases the restriction shall only apply to the time period necessary for the Controller to verify the correctness of the Personal Data;
- the Processing is unlawful and the Data Subject oppose the erasure of the Personal Data and request the restriction of their use instead;
- the Controller no longer needs the Personal Data for Data Processing purposes, but the Data Subject requests the data for the establishment, exercise or defence of legal claims; or
- the Data Subject objects to Processing; in this case the restriction applies to the period while it is verified whether the legitimate interest of the Controller override those of the Data Subject.

In the event of a successful objection, the Controller will process the Personal Data affected by the restriction, with the exception of storage, only with the Data Subject's consent or for the purpose of the establishment, exercise or defence of legal claims or protecting the rights of another person or in the important public interest of the European Union or a Member State.

If the processing of Personal Data is subject to a restriction, we will inform you in advance of the lifting of the restriction on Data Processing

11.6. Right to data portability

In the following cases, the Data Subject has the right to receive the personal data concerning them, which the Data Subject has provided to a Controller, in a structured, commonly used and machine-readable format and shall have the right to transfer those Personal Data to another controller.

- Processing is based on the Data Subject's consent or is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; and
- the Processing is an automated process.

11.7. Right to objection

The Data Subject has the right to object, on grounds relating to their situation, at any time to processing of their Personal Data, that is in the public interest or necessary to enforce the legitimate interests of the Controller or a third party, including profiling based on the above provisions. In this case, the Controller shall abandon the processing of the Personal Data unless the Data Processing is justified by overriding compelling legitimate grounds, which override the Data Subject's interests, rights and freedoms, or are necessary for the establishment, exercise or defence of legal claims.

Where Personal Data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of Personal Data for such marketing, which includes profiling to the extent that it is related to such direct marketing.

11.8. The right to automated decision-making

The Data Subject has the right to excuse themselves from the force of resolutions which are based exclusively on automated data processing (including profiling) and would have legal effect on them or would affect them in any other way to a similar extent, unless such a decision:

- is necessary for entering into, or performance of, a contract between the Data Subject and a Controller;
- authorised by Union 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
- based on the Data Subject's explicit consent.

In the event that the Data Subject may not exercise the right referred to in this subsection due to automated decision-making based on the contract or consent, they have the right to request human intervention on behalf of the Controller to express their position and to object to the decision.

During the credit rating process, the Controller is entitled to make a decision in an automated manner by assessing the various personal circumstances of its customers (such as location of residence, age, educational qualifications, marital status, previous credit history, employment history, financial habits), which affects the outcome of the credit assessment and the conclusion of the transaction. The purpose of the scoring performed by the Controller during the credit rating process is to assess the circumstances of the customers' solvency, payment habits and willingness and to make a business decision taking into account the circumstances of the customer.

11.9. Right to withdraw consent

In the case of processing under consent, the Data Subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

11.10. Methods of exercising rights relating to the protection of personal data

You may exercise your rights in relation to the processing of personal data, as listed in Section 11 of the Notice, at the branches of MBH Bank, in person or by proxy, by sending a letter to the Data Protection Officer, by calling the free green number +36 80 350-350, available on working days between 8 a.m. and 5 p.m., or by sending an e-mail to adatvedelem@mbhbank.hu.

12. DATA SECURITY MEASURES

The Bank is obliged to ensure the secure operation of its IT system and the appropriate protection of data in accordance with the GDPR and certain provisions of Government Decree 42/2015 (12 March) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers.

In order to ensure the protection and security of personal data, the Bank shall ensure the security of data processing through internal regulatory (data and confidentiality protection, information security, access rights, etc.), technical, organisational, technical and educational measures. These include in particular the technologies that form the IT security infrastructure, security access controls, access management systems that limit access rights for individual employees to the extent necessary for the performance of their work, certain segregations (e.g. separate processing of data held in the financial services and investment services areas), data leakage protection, computer identifiers, passwords, screen protection, logging, etc.

Filtering software is used to protect against certain risks (e.g. phishing emails, viruses, spyware, etc.). These applications may sometimes have the consequence of, for example, stopping private mail from outside by the filtering software.

12.1. Personal data breach handling

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the data processed.

The Bank shall notify the National Authority for Data Protection and Freedom of Information of any occurred personal data breach if it involves a risk, no later than 72 hours after becoming aware of it. The Bank may not submit a notification if, based on the circumstances of the case, the data breach is unlikely to pose a risk to the Data Subject. If the data breach is likely to involve a high risk based on the circumstances, in addition to the notification, the Bank will inform the Data Subject of the nature of the data breach, the likely consequences thereof and the measures taken or planned to remedy the data breach.

Irrespective of the risk classification of the data breaches, the Bank records all personal data breaches and takes the necessary technical and organisational measures.

Data Subjects who believe that a data breach has occurred during the processing of their personal data may contact the Bank's Data Protection Officer directly by email at adatvedelem@mbhbank.hu or report the incident by phone to the Bank's Customer Service at 06 80 350 350.

13. LEGAL REMEDY OPTIONS

13.1. Complaints to the bank

If the Data Subject feels that the Bank has acted inappropriately in relation to the processing of their personal data or otherwise considers the Bank's processing of their personal data to be prejudicial, they have the right to lodge a data protection complaint with the Bank. The complaint may be made at any of the Bank's branches or at the contact details indicated in the introduction to the Bank's Notice.

The Bank's Data Protection Officer shall investigate the Data Subjects' complaints and shall endeavour to propose a satisfactory solution. If the Data Subject is dissatisfied with the Bank's handling of their data protection complaint, they may have further remedies in accordance with Sections 13.2 to 13.3.

For more information on the Bank's complaints handling procedure, please visit www.mbhbank.hu/kapcsolat/panaszkezeles .

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

The Data Subject may lodge a complaint about the processing of his/her personal data with the National Authority for Data Protection and Freedom of Information (**NAIH** - 1055 Budapest, Falk Miksa utca 9-11.; postal address: 1363 Budapest, PO Box: 9.; e-mail: ugyfelszolgalat@naih.hu; phone: +36 (30) 683-5969, +36 (30) 549-6838; +36 (1) 391 1400; Fax: +36 (1) 391-1410)).

13.3. Judicial remedy

If the competent supervisory authority does not deal with the Data Subject’s complaint, or does not provide information within three months of the progress of the complaint or its outcome, or if the Data Subject considers that the processing of Personal Data concerning them by the Controller infringes their rights to the protection of personal data, they are entitled to turn to the court.

In this case, legal proceedings against NAIH must be initiated before the Budapest-Capital Regional Court or the court of the regular place of residence.

In the event of violation of the Data Subject’s rights, legal proceedings against MBH Bank must also be initialled before the Budapest-Capital Regional Court or the court of the regular place of residence.

14. OTHER CIRCUMSTANCES

MBH Bank may amend the Notice at any time by informing the Data Subjects simultaneously. We will notify our customers of any changes to the Notice by posting information on the www.mbhbank.hu website and in our branches.

1. Annex 1.

Definitions relating to data protection

Controller: the organisation defined in the Introduction of the Notice.

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.

Casual customer: a person making a cash payment at a bank branch, who does not have a contractual relationship with the Bank and is not included in a banking transaction.

Recipient: a person, public authority or another body, to which the Personal Data are disclosed by the Controller, regardless of whether the Recipient is a third party other than the Controller or the Data Subject. Public authorities that may have access to personal data in the framework of an individual investigation in accordance with EU or Member State law (e.g., in the course of an investigation by the Magyar Nemzeti Bank (National Bank of Hungary) in the exercise of its supervisory powers) shall not be considered as recipients.

Data Subject: identified or identifiable natural persons in relation to whom the Data Controller processes any information that constitutes Personal Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, date of birth, online identifier (e.g., IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

Consent: a freely given, specific, informed and unambiguous indication of wishes, by which the data subject clearly indicates their consent to the processing of personal data concerning them.

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

MBH Bank Financial Group: MBH Bank Nyrt., MBH Befektetési Bank Zrt., MBH Jelzálog Bank Nyrt. and legal entities subject to the laws of the financial sector in which the aforementioned hold a controlling interest.

Personal Data: any relevant information about the Data Subject on the basis of which the Data Subject can be identified directly or indirectly.

Notice: this Privacy Notice.

Definitions not specifically defined in the Notice and not capitalised have the meanings set out in the GDPR.

2. Annex 2.

INFORMATION ON DATA PROCESSING FOR WHICH NO SPECIFIC INFORMATION IS AVAILABLE

1. Retrieve contact details (address) from a public database and sending a letter requesting contact details for data reconciliation

If the Data Subject has failed to notify the Bank of a change in their contact details and, as a result, the Bank, which has a contractual relationship with them, does not have any contact details at which they can be contacted in the context of the obligation to cooperate in the performance of the contract, the Data Controller is entitled to perform the following query (data processing operation).

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	SOURCE OF DATA	DATA RETENTION PERIOD
Recording of address details for contacting the Customer	Performing a contract with the Data Subject (First indent of Article 6(1)b) of the GDPR)	Address	GIRinfO Data Processing Service application GIRO Zrt., company registration number 01-10-041159, registered office: 1054 Budapest, Vadász u. 31.)	Unless otherwise provided by law, the processing of personal data generated during the customer relationship shall be limited to 5 years from the termination of the customer relationship (6:22 of the Civil Code)

Taking into account that the data are not provided to the Bank by the Data Subject, therefore, the Bank provides detailed information regarding processing to the Data Subject with the content and time according to Article 14 of the GDPR. In the present case, the information is provided to the data subject in the letter requesting them to the data reconciliation (at the time of the first contact), but no later than 1 month after the address has been retrieved from the public database.

2. Processing of personal data in a test environment

The Bank performs testing and debugging procedures in a test environment separate from the live environment in order to continuously maintain and improve its IT systems.

If the procedures in the test environment also require the use of personal data taken from the live system, the processing of such live data (e.g. customer data) in the test environment shall be considered as a separate and legitimate processing purpose from the purpose for which the data were originally processed (e.g. performance of a contract).

As a general rule, the Bank shall process such personal data in the separate test environment only after full anonymisation.

In the case of anonymised data, it is not identifiable to which natural person the data relates, the link between the data and the data subject is irreversibly broken and they do not pose any data protection risk to the rights and freedoms of the data subject. Such anonymous data are outside the scope of the GDPR.

If the given testing or development process would not lead to a result with anonymous data (i.e. without data processing) the Bank will process personal data taken from the live environment in the segregated test environment as follows.

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Correction of errors in the live IT system.	The Data Controller's legitimate interest in the operation of its IT systems (in this context, the full provision of its services). (Article 6 (1) f) of the GDPR)	Customer data, employee data (e.g. identification data, financial data) taken from the live system and essential for the correction of an error.	Once the error is corrected, the data is deleted from the test environment.
Development of a live IT system.	The Data Controller's legitimate interest in the operation of its IT systems (in this context, the full provision of its services). (Article 6 (1) f) of the GDPR)	Customer data, employee data (e.g., identification data, financial data) taken from the live system and essential for improvement.	Once the development is completed, the data will be erased from the test environment.

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

- The testing will be performed in an environment separate from the live environment, the Bank will ensure the separation of the test environment at database and network level.
- The controls for the test environment are the same as, and sometimes more stringent than, those for the live systems.

- The Bank also ensures an adequate level of protection of personal data by restricting access, ensuring appropriate allocation of rights and encryption when processing data for this purpose.

3. Complaints handling

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Compliance with the legal obligation to handle complaints	Fulfilment of the legal obligation pursuant to Article 6 (1) c) of the GDPR in accordance with the provisions of Section 288 (1) of the CIFE Act and Section 121 (1) of the Investment Services Act.	The data specified in Annex 1, Point III of the MNB Regulation 46/2018 (17 December) on the detailed rules on the form and method of handling complaints by certain financial organisations issued on the basis of the authorisation of the CIFE Act and the Investment Services Act.	5 years from the date of the complaint

4. Processing of personal data of casual customers

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Preventing and combating money laundering and terrorist financing. (Section 14 (1) of the AML Act)	Fulfilment of legal obligation pursuant to Article 6 (1) c) of the GDPR Section 14 (1) of the AML Act	The data specified in Article 14 (1) of the AML Act (first and family name, date and place of birth, subject and amount of the order)	8 years pursuant to Section 57 (3) of the AML Act

In addition, the credit institution may request the presentation of the documents specified in Article 7(3) of the AML Act, i.e. in the case of natural persons:

- in the case of a Hungarian citizen, official document suitable for identification purposes and official address card, the latter in the case of a Hungarian citizen whose address or place of residence is in Hungary,
- in the case of foreign nationals, passport or personal identification document, if it embodies an authorization to reside in Hungary, document evidencing the right of residence or a valid

residence permit, official address card in Hungary, if their address or place of residence is in Hungary.

5. Internet cookies

MBH Bank uses cookies on its websites and sub-sites to ensure the correct functioning of the site and to improve our services. Cookies placed on the user's computer are considered as personal data of the user.

When the user visits the MBH Bank's websites, the Data Controller places a small data package, known as a cookie, on their device. If the user visits the site again later, the browser returns the previously saved cookie, so that the cookie management service provider can link the user's current visit to previous visits, but only in relation to its own content.

There are several types of cookies.

- Some cookies are essential for the website to function.
- Others collect information about the use of the site to make it more convenient and user-friendly and to offer more relevant services to the users.
- Temporary cookies are automatically deleted when you close your browser.
- Permanent cookies may remain on the user's device for a longer period of time.

Further details on the cookies used by MBH Bank can be found in the Cookie Notice: mbhbank.hu/cookies

6. Fraud detection

According to Section 107 (1) of the CIFE Act, credit institutions must have an effective and sound corporate governance system and internal control function in order to, among others, promote the smooth and effective operation of the institution, maintain confidence in the institution, protect the economic interests and social objectives of the owners and customers relating to the institution.

MBH Bank, by its nature as a credit institution, is exposed to increased risks of fraud and other forms of abuse, the success of which could undermine confidence in the institution and could also significantly harm the economic interests of its customers and ultimately its owners.

In view of the above, MBH Bank keeps a record of certain attempts of abuse, which necessarily includes personal data. The list is used by the data controller to avoid entering into business relationships that would be likely to result in (further) losses for them. The details of the processing are summarised in the table below:

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD

Identification of fraud and other attempted fraud, loss avoidance	Legitimate interest in the protection of (public) confidence in the institution and the protection of customers' and owners' investments, pursuant to Article 6(1)f) of the GDPR.	Identification of the perpetrators, date, nature of the abuse, IP address	Consistent with the retention of negative information in the CCIS (10 years)

The data protection guarantees applied by the Bank, for the purposes of data processing under this section:

- The number of persons having access to the database is extremely limited, restricted to a few persons involved in fraud prevention activities;
- Inclusion in the database does not result in an automatic rejection of the request for customer contact, in certain cases other measures (e.g. increased verification of submitted documents) may be sufficient to manage the risk.

7. Dispute settlement

MBH Bank will endeavour to settle disputes by agreement between the parties, but if this does not lead to a settlement, the processing of data for purposes other than the original (typically contractual) purpose will necessarily be subject to legal or other official or conciliation procedures, as follows:

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Establishment, enforcement or defence of legal claims;	Legitimate interest in dispute settlement pursuant to Article 6 (1) f) of the GDPR.	Personal data recorded in documents and other evidence relevant to the dispute	5 years from the date of the final conclusion of the dispute (objective time limit for renewal).

8. Internal credits

In order to ensure the prudent operation of credit institutions, Section 106 of the CIFE Act requires credit institutions to apply special rules to the risk-taking of members of their management bodies, auditors, close relatives and business interests, and to ensure an effective procedure for the identification, recording, monitoring and reporting of risk-taking to the Supervisory Authority.

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Comply with the requirement for an effective internal	Legitimate interest in the lawful treatment of	Identification data of the members of the management body and the auditor potentially	Until the termination of the internal credit rating for the risk exposure.

credit procedure as laid down in Section 106 of the CIFE Act.	internal credits pursuant to Article 6(1)f) of the GDPR	affected by the internal credit, the data content of the risk exposure (typically proposals and loan agreement) that constitutes an internal credit, recorded during the monitoring of the transaction.	

9. Telephone voice recording

The Bank operates a telephone customer service to serve and inform customers and to deal with their complaints and requests. On certain telephone lines, the Bank uses a voice recording system, which it informs the parties concerned of at the beginning of each call. The telephone customer service is primarily a contact channel, and since it is possible to make a variety of calls for different purposes, the purpose and legal ground of the processing, the scope of the data processed, the retention period, etc. must and can be assessed primarily on the basis of the content of the call.

The retention of a complaint for 5 years is a legal obligation, the inclusion of a customer order falls within the scope of the performance of a contract, a marketing statement is based on the consent of the customer, etc.

The Bank provides information on data processing for each category of customer in this notice and in the privacy notice for each service, whether the communication is made by telephone or by other channels.

In addition to the above, the purpose of data processing is to provide evidence of the issues raised in the course of customer information and to improve the activities of our staff. Full customer information is in the interest of the customer and the Bank, and is also an expectation of the National Bank of Hungary as a supervisory body. Due to the special nature of the channel, paper-based, documented information cannot be provided to customers, so in relation to telephone numbers through which a large number of customer calls or special purpose calls are made, recording is in the legitimate interest of the data controller (Article 6 (1) f) of the GDPR), while at the same time, in the event of inadequate information, failure to record complaints or other problems, it also provides the data subject with the opportunity to enforce their rights, in view of which the retention period for these purposes is subject to the general civil law limitation period (5 years).

PURPOSE OF THE PROCESSING	LEGAL GROUND OF THE PROCESSING	CATEGORIES OF DATA PROCESSED	DATA RETENTION PERIOD
Establishment, enforcement or defence of legal claims relating to	Legitimate interest in dispute settlement pursuant to Article 6 (1) f) of the GDPR.	The audio recording relevant to the dispute and the data and legal statements made on the recording.	5 years

legal statements made in a call			
Execution of orders given by the customer in the call, contract management	Contract performance pursuant to Article 6 (1) b) of the GDPR	Customer information and voice of the customer relevant to the execution of the customer's order.	8 years
Complaints handling	Legal obligation pursuant to Section 288 of the CIFE Act and Section 121 of the Investment Services Act legal obligation pursuant to Article 6 (1) c) of the GDPR	Data specified in Annex 1, Point III of MNB Decree 66/2021 (20 December) and other data provided by the complainant, as well as the voice of the complainant.	5 years