KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

PRIVACY POLICY
on the Data processing of KDB Bank Europe Private Limited Company in connection with its financial services, ancillary financial services and investment services activities

Effective from: 7 May 2026

This Privacy Policy has been originally prepared in Hungarian language therefore should arise any discrepancy in connection with the interpretation of the English and the Hungarian versions of the present Privacy Policy, the Hungarian version shall prevail.

1. Introduction

KDB Bank Europe Private Limited Company (hereinafter referred to as **the "Bank"** and also referred to as **the "Data Controller")** hereby wishes to inform all Clients of natural persons and all natural persons qualifying as "Other Clients" – in compliance with its obligations set out in Articles 13 and 14 of the Regulation, of the Bank's financial services, ancillary financial services and investment services and ancillary services. (hereinafter collectively referred to as the "**service").**

II. Definitions

Data Controller: a natural or legal person, or an organisation without legal personality, who or which, independently or jointly with others, determines the purposes and means of Data processing, makes and implements decisions concerning Data Management (including the means used), or has it implemented by a data processor commissioned by it (Infotv. Section 3, Point 9; Article 4(7) of the Regulation);

Data processing: any operation or operation performed on the data, regardless of the procedure used. in particular the collection, recording, recording, structuring, organisation, storage, transformation or alteration, use, retrieval, consultation, communication, transmission, disclosure, alignment or combination, restriction, blocking, deletion and destruction of data, as well as the prevention of the further use of data, the taking of photographs, audio or video recordings, and the recording of physical characteristics suitable for the identification of a person (Infotv. Section 3, Point 10; Article 4(2) of the Regulation);

Data Processor: a natural or legal person or an organisation without legal personality, who or which processes data on the basis of a contract concluded with the Data Controller, including the conclusion of a contract based on the provisions of the law; processes Personal data on behalf of the Data Controller (Infotv. Section 3, Point 18; Article 4(8) of the Regulation)

Data transfer: making the data available to a specific third party (Infotv. Section 3, Point 11);

Data deletion: making data unrecognizable in such a way that their restoration is no longer possible (Infotv. Section 3) Point 13);

Bszt: Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers and on the Rules of the Activities They May Carry Out

CRS Act: Act XXXVII of 2013 on Certain Rules of International Administrative Cooperation in Relation to Taxes and Other Public Charges;

Data Subject (person): any natural person identified or – directly or indirectly – identifiable on the basis of Personal data (Infotv. Section 3(1)); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifiable Personal data or one or more factors of identity (Article 4(1) of the Regulation). The Data Subject in its relationship with the Bank may be the Client or the Other Client;

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

Client: Any natural or legal person, or an organisation without legal personality, who or which uses financial services, ancillary financial services or investment services from the Bank or through the Bank;

Occasional Client: A natural or legal person, or an organization without legal personality, who or which gives a transaction order to the Bank on an occasional basis (for example, the Bank considers a natural person who does not have an account but makes a direct cash deposit to the Bank's Client's payment account as such);

Prospective Client: A person who is the addressee of information, advertising or an offer related to a service or product of the Bank, as well as a person who requests or is interested in a service (but the Bank has not yet concluded a contract with him for the provision of services), or who makes a contractual offer to the Bank;

Other Client: Collective name for the Occasional Client and the Prospective Client;

FATCA Act: Act XIX of 2014 between the Government of Hungary and the Government of the United States of America on the Promotion of International Tax Compliance and the Implementation of the FATCA Regulation and on the Amendment of Certain Related Acts;

Third party: a natural or legal person, or an organisation without legal personality, or any other body that is not the same as the Data Subject, the controller, the processor or the persons authorised to process the Personal data under the direct control of the controller or processor (Article 4(10) of the Regulation);

Third country: any state that is not an EEA state (Infotv. Section 3, Point 24);

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

Infotv: Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information;

Special data: Personal data concerning racial origin, nationality, political opinion or party affiliation, religious or other philosophical beliefs, membership in an advocacy organisation, sex life, state of health, pathological addiction and criminal offences;

Pmt: Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing;

Profiling: any form of automated processing of Personal data in the course of which Personal data is used to evaluate certain personal characteristics relating to a natural person (Article 4(4) of the Regulation);

Personal data: any information relating to the Data Subject, in particular an identifier such as a name, number, location data, an online identifier provided by the devices, applications, devices and protocols used by the Data Subject, as well as any other identifier, or any information specific to one or more of the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person, and the information derived therefrom that which may be used to identify the Data Subject. (Infotv. Section 3 Point 2; Article 4(1) of the Regulation);

Accounting Act: Act C of 2000 on Accounting;

Objection: a statement by which the Data Subject objects to the processing of his/her Personal data and requests the termination of Data processing or the deletion of the processed data;

Regulation/GDPR: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

Business Regulations: In this Privacy Policy, the Business Regulations refer to the Bank's Financial and Ancillary Financial Services and Investment Services.

III. Identity and contact details of the Data Controller

Name:	**KDB Bank Europe Private Limited Company**
Headquarters:	1054 Budapest, Bajcsy Zsilinszky út 42-46.
Registered by:	Metropolitan Court of Registration, company registration number: 01-10-041313
Postal address:	1382 Budapest, Pf. 1
Phone Number:	+36 (1) 473-4440 and +36 (1) 374-9990
Fax:	+36 (1) 328-5454
Email address:	info@kdbbank.eu
Website:	http://www.kdbbank.eu/

Name and contact details of the Data Protection Officer

Name:	dr. Szabolcs Attila Tóth
Postal address:	1382 Budapest, Pf. 1
E-mail:	adatvedelem@kdbbank.eu

1. Purpose, legal basis, duration of Data processing, scope of Personal data affected by Data processing, duration of Data processing

1. Purpose of Data processing

The exact purpose or purposes for which the Bank processes the data of the Data Subject are contained in the terms and conditions governing the contractual relationship planned or existing with the Data Subject (Client, Other Client) – the relevant Business Regulations, the terms and conditions governing the product or service, and the specific contracts concluded with the Client, as well as the related statements and information, Determine. The primary purpose of the Bank's Data processing is to provide the service to be provided/provided by the Bank to the Data Subject on the basis of the contract concluded or to be concluded with the Data Subject, as well as other services related to the Bank's activities, as well as to perform the Data processing based on these laws on the basis of the legal provisions governing the Bank's activities. In addition to complying with the provisions on the protection of Personal data, the Bank processes Personal data in accordance with the provisions on bank secrets, securities secrets, insurance secrets and other secrets specified by law. The further purposes of Data processing carried out by the Bank, the legal bases and the duration of the Data processing are presented in Appendix 1 of this Privacy Policy.

1. Legal basis and duration of Data processing

The Bank may process Personal data on one of the following legal bases:

1. **performance of a contract** on a legal basis (Article 6(1)(b) of the GDPR), or
2. **compliance with a legal obligation** on the basis of a legal basis (Article 6(1)(c) of the GDPR), or
3. **legitimate interest** on the basis of a legal basis (Article 6(1)(f) of the GDPR), or
4. **on the basis of the Data Subject's consent** (Article 6(1)(a) of the GDPR

The primary Data processing activity carried out by the Bank is the Data processing activity related to the provision of services, with its retention period (hereinafter referred to as the "general retention period") and its legal basis specified in Annex 1 of this Privacy Policy. The legal bases for each additional Data processing and the Data processing periods related to each Data processing activity are also included in this annex. In cases where abuse occurs and the Bank appears as a victim or it is necessary to enforce its legal rights in an official or court proceeding, it may establish a longer retention period for Data processing, which is adjusted to the date of the final or final termination of the official or judicial (litigation/non-litigation) proceedings.

Performance of the contract legal basis

The Bank shall use the legal basis for the performance of the contract if the Data Subject is the other party and the Data processing is necessary for the conclusion, performance or termination of the contract. In addition to the performance of a contract, this legal basis also includes Data processing prior to the conclusion of the contract, which is necessary for the preparation of the contract at the request of the Data Subject. The data processed on such a legal basis are typically provided by the Data Subject (Client/Other Client) at the time of concluding the contract, at the time of its preparation, or are generated about the Client/Other Client during the performance of the contract. In the case of the provision of financial or other ancillary financial services, as well as Investment or related ancillary services, the Bank processes various Personal data about the Client/Other Client. It makes all of these part of the concluded contract and constitutes additional identifiers related to the Client/Individual Client. These may serve the purpose of registering in the Bank's management systems, identification in various accounting and accounting systems, and other interests, such as the need for banks to know their Client, to operate appropriate systems against various abuses, etc.

Fulfilment of a legal obligation legal basis
In the case of mandatory Data processing based on law, the types of data to be processed, the purpose and conditions of Data processing, the availability of the data, the duration of Data processing, and the identity of the Data Controller are determined by the law ordering Data processing. Banking activities are regulated in detail, so the number of Data processing related to the fulfilment of legal obligations is also high. The list of relevant laws can be found in Annex 1 of this Privacy Policy.

Enforcement of legitimate interest legal basis
The Bank shall apply the legal basis of legitimate interest if the Data processing is necessary for the enforcement of the Bank's legitimate interests, provided that the enforcement of this interest is proportionate to the restriction of the Data Subject's right to the protection of his or her Personal data. In order to decide this, the Bank always carries out a balancing of interests and prepares a balancing test, the result of which determines whether Data processing can be lawfully continued on this legal basis.

The Data Subject's consent is a legal basis
The condition of Data processing based on the Data Subject's consent is the voluntary, specific, well-informed and unambiguous expression of the Data Subject's will, by which the Data Subject indicates by a statement or an unambiguous affirmative act that he/she gives his/her consent to the processing of the Personal data concerning him/her. If the Data processing serves several purposes at the same time, the Bank will request consent from the Data Subject separately for each Data processing purpose. The Data Subject shall have the right to withdraw his/her consent at any time, however, this withdrawal shall not affect the lawfulness of the processing of data based on consent prior to its withdrawal. The fact of withdrawal may not in itself cause any disadvantage to the Data Subject.
The Data Subject may give or withdraw his/her consent to Data processing in one of the following ways:

- By signing a declaration related to a written contract
- By postal mail, signed in a certified manner (in the case of the Client, in accordance with the specimen signature registered by the Bank, which may be included on the signature card or in the contract concluded with another client, or the signature of the last other document signed by the Data Subject and signed by the Bank).
- Electronically, by logging into the banking systems – after proper identification and authentication – by sending a free-form letter to the Bank.
- By means of an explicit and unambiguous statement over the phone (in this case, the telephone conversation will be recorded).

4.1. Source of Personal data, scope of Personal data affected by Data processing

4.3.1 Source of Personal data
Data relating to Clients or Other Clients is obtained by the Bank primarily through direct collection from the Clients and/or Other Clients, through the transfer of data from other Third parties, as well as from public and therefore publicly accessible data sources, and from statutory or other financial information databases that provide such data. If the Bank becomes aware of the Personal data of the Other Client

jointly with the Client or in connection with a contract to be concluded for a banking service, the Bank shall presume that the Other Client has consented to the processing of the data provided in connection with the contract, or that the Client has obtained such consent from the Other Client has obtained and has the right to transfer the data of these persons to the Bank. The Bank calls the attention of its Client and Other Clients to always provide data to the Bank only in possession of this authorisation and authorisation, lawfully and in good faith.

4.3.2 Scope of Personal data affected by Data processing

The data processed by the Bank about the Data Subjects is determined by the relationship between the Data Subject and the Bank, i.e. the contract concluded by the Client with the Bank or the other services the Client wishes to use from the Bank, as well as the purpose of the Data processing and the recording of the data. The scope of data processed in connection with certain Data processing activities performed by the Bank is defined in Annex 1 of this Privacy Policy.

4.3.3. Processing of sensitive data

The Bank processes Sensitive Data in limited cases, under strict conditions and only if the Data Subject expressly consents to the Data processing, or if one of the conditions set out in Article 9 (2) of the GDPR is met in relation to the Data processing[1] and the Bank has an appropriate legal basis in relation to the Processing of Sensitive Data.

5. Recipients or categories of recipients of the Data transfer

As a general rule, the employees of the Bank may become aware of the Personal data processed by the Bank to the extent strictly necessary for their work.

Data transfer outside the bank may take place to the following recipients and under the following conditions. The Bank shall disclose the data of the Clients and Other Clients to the authorised person (typically a state body) in the event of a legal obligation to do so, and may disclose the data of intermediaries in a contractual relationship with the Bank, organisations involved in the performance of the services provided by the Bank (agents), enterprises performing ancillary (outsourced) activities related to the Bank's normal operation, Data processing operations to Data Processors involved in the performance of related technical tasks (hereinafter collectively referred to as "**Recipients")** in compliance with the relevant legislation.
The contractual contributors undertake to ensure the fulfilment of data protection and data security requirements towards the Bank.

Recipients of data disclosure (Data transfer):

– **National Tax and Customs Administration Central Administration Anti-Money Laundering and Countering the Financing of Terrorism** Office in the event of the occurrence of data, facts or

[1] The Bank may process sensitive data if:
• the Data Subject has given his or her explicit consent to the Data processing,
• the Data processing is necessary for the performance of the obligations and exercise of the specific rights of the Data Controller or the Data Subject arising from the legal provisions regulating employment, social security and social protection,
• the processing is necessary for the protection of the vital interests of the Data Subject or another natural person, if the Data Subject is unable to give his or her consent due to his or her physical or legal incapacity,
• Data processing refers to personal data that the Data Subject has expressly disclosed,
• the Data processing is necessary for the submission, enforcement and defence of legal claims,
• the Data processing is necessary for reasons of significant public interest,
• the Processing is necessary for preventive health or occupational health purposes, to assess the employee's ability to work, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social systems and services,
• the processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring a high quality and safety of healthcare, medicinal products and medical devices, and is carried out on the basis of Union or Member State law;
• the processing is necessary for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes in accordance with Article 89(1).

circumstances indicating money laundering, terrorist financing or the origin of a thing from a criminal act;

- **the National Bank of Hungary** in order to fulfil the Bank's regular, ad hoc data reporting based on the designation of the National Bank of Hungary;
- **BISZ Central Credit Information Private Limited Company** in the case of the management of reference data and Data processing in connection with consumer statements enabling free cash withdrawals;
- **the National Revenue and Customs Administration** to provide data related to the tax residency examination of financial accounts (CRS Act) and the U.S. Tax Residency Examination (Fatca Act);
- **the financial institution holding the payee's payment account** in the case of Data processing related to the execution of the payment transaction;
- **National Deposit Insurance Fund** with regard to consolidated deposit data reporting;
- **other Recipients entitled to request data on the basis of the law**
  In the event of a data request, the investigating authority, the prosecutor's office, the court, the national security (special) service or any other authority (e.g. notary, notary, guardianship authority, MNB, GVH, NAV, MÁK, Commissioner for Fundamental Rights, NAIH, etc.) entitled to request data shall comply with the data request in order to ensure the performance of its statutory duties. The Bank is not bound by the obligation of confidentiality towards these bodies and organisations within the framework of the relevant legislation, so it may also forward Personal data to these bodies and organisations.
- **the Bank's data requests to the organisations managing the records as Recipients**
  The Bank is entitled to check the content of the information contained in the documents and other documents made available to the Bank by the Client in the course of the preparation of the contract and the conclusion of the contract, and to verify their veracity, correctness and validity. In the course of this audit, the Bank is entitled to compare the data and the data and documents relating to the assets offered to the Bank for security purposes with the data of public registers, to request information from them, and to forward and transfer data to these organisations for the purpose of data queries, in compliance with the provisions on the protection of Personal data and sectoral secrets, in particular bank secrecy, in compliance with the provisions on the protection of Personal data and sectoral secrets, in particular bank secrecy. Such bodies or registers may include, for example: personal and road traffic registers under the supervision of the Ministry of Interior, the land and company registers, various court and authority registers, tax authority registers, as well as Girinfo and KHR. The Bank shall be entitled to these audits during and in the interest of the preparation of the requested banking transaction, at the time of the establishment of the relevant contractual relationship, during its existence, or for as long as the Client has a debt to the Bank arising from the contract;
- **Outsourced Activities**
  Pursuant to Sections 68 and 164 (j) of the Securities Act and the provisions of Section 79 (1) of the Securities Act, the Bank may outsource any activity related to its financial and ancillary financial service activities, related to its investment service activities or ordered by law to be carried out in the course of which data management, Data processing or data storage is carried out, in compliance with data protection regulations. Within this framework, the Bank may transfer the Data Subject's Personal data to Data Processors commissioned by the Bank and performing outsourced activities.
  In the course of its financial and investment service activities, the Bank has entrusted the persons, organisations and enterprises indicated in its announcement posted in its premises open to Client traffic and in the list published on the https://www.kdbbank.eu/egyeb-tajekoztatok-hirdetmenyek-1 website to carry out the outsourced activities specified therein;
- **Intermediaries**
  Pursuant to Section 164 q) of the Hpt., in order to perform the contract relating to financial services mediated by the intermediary, your Personal data were transferred to the intermediary in a contractual relationship with the Bank for the period necessary by the Bank until the realisation of the purpose of Data processing. If a credit intermediary is involved in the transaction by the Client, by submitting the application, the Client authorises the credit intermediary and the Bank to share the Client's identification and contact data, as well as the data relating to the requested service,

with each other in order to prepare, conclude, perform and settle the contract, and for the purpose of contacting the Client.
The list of intermediaries used by the Bank at any given time is available in the searchable list on the website of the National Bank of Hungary: https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/piaci-szereplok-keresese/kozvetitok-keresese;

- **Debt Collectors**
  Pursuant to Section 161 (1) c) of the Hpt., the Bank may also transfer the Client's data to debt management companies for debt management purposes, if they are necessary for the sale of the Bank's claim against the Client or for the management and enforcement of its late, expired claim. The Bank may assign its claim against the Data Subject, in which case it shall transfer to the assignee all data and documents related to the Data Subject's outstanding claim on the basis of the assignment agreement (unless the assignor and the assignee have agreed otherwise in the assignment agreement). The Bank manages the accounting documents related to the assignment and the supporting documentation for 8 years after the assignment pursuant to Section 169 (2) of Act C of 2000 on Accounting. The Bank reserves the right to assign its claims to a Third party by way of assignment. Pursuant to Sections 6:197-6:198 of the Civil Code, the consent of the obligor/debtor is not required for assignment. Pursuant to the provision of Section 6:196 of the Civil Code, the assignor is obliged to provide the assignee with the information necessary for the enforcement of the claim and is obliged to hand over to the assignee the documents in its possession proving the existence of the claim;
- **Auditor, legal expert** A bank is based on the hpt. Section 164 d) of the Securities Act, and on the basis of a Data processing agreement, the may transfer data to an authorised auditor, asset controller, legal or other expert under contract with the Bank, or to an insurance company providing insurance cover, for the purpose of performing audit, asset control, legal or other expert activities for the duration of the Data processing purpose.

Data transfer to Data Processors

The Bank is entitled to involve a Data Processor in the performance of Data processing activities throughout the life cycle of the data in its possession, and therefore to transfer data to the Data Processors involved to the extent and to the extent necessary for the performance of the Data processing activity. In the course of its activities, the Data Processor may in certain cases access and be entitled to access the Data Subject's Personal data. Based on the relevant contract concluded with the Bank, the Data Processors process the Personal data on behalf of the Bank and for a specific purpose determined by the Bank. The Bank only uses a Data Processor who provides adequate guarantees in a contract for the protection of Personal data processed on behalf of the Bank.
The scope of Data Processors used by the Bank is contained in the document entitled "List of Data Processors", which is available on the Bank's "https://www.kdbbank.eu/adatvedelem-es-adatkezeles" website.

Further Data transfers

In addition, the Bank is also entitled to transmit data:

- for the performance of the contract concluded with the Client, or for the fulfilment of the obligations assumed in connection with the contract, or for the purpose of verifying these, if the Bank provides a given product or service jointly with another partner (e.g. state subsidies, etc.);
- for the notarial deed of notarial of contracts, declarations and other documents, to the notary who made or has been asked to do so;
- for the purpose of verifying the authenticity or authenticity of the document, to the body, company, employer, authority, etc. that issued the document;
- in the case of a payment order (in particular direct debit), to the service provider concerned as defined by law;
- in the case of using mobile banking services (e.g. sending SMS), to the telecommunications service provider(s) used.

Provision of services using cloud services
The Bank uses cloud services to perform certain of its services and to operate its internal processes. In this context, the Bank proceeds in accordance with the recommendation and regulation issued by the National Bank of Hungary in connection with the use of community and public cloud services. The cloud service provider(s) used by the Bank primarily:

- Microsoft Ireland Operations Ltd. (South County Business Park, One Microsoft Place)

6. Transfer of data to third countries/international organisations

At present, data management and Data processing takes place exclusively in the European Economic Area. Data transfers to countries outside the European Economic Area (EEA) may take place on the basis of an adequacy decision issued by the European Commission, in the absence of which appropriate safeguards (e.g. application of binding corporate rules, general data protection clauses adopted by the European Commission). In the absence of an adequacy decision or adequate safeguards, Article 49 of the GDPR provides for the possibility of derogation in special situations (e.g. the transfer of data is necessary for the performance of the contract between the Client and the Bank). If the Data transfer cannot be based on an adequacy decision, there are no adequate guarantees in place and none of the derogations for special situations apply, the Data transfer to Third countries and international organisations may only take place if the Data transfer is not repetitive, concerns only a limited number of Clients, the Bank is necessary for a compelling legitimate interest which is not overridden by the interests of the Client, and the Bank has examined all the circumstances of the Data transfer and, on the basis of this investigation, provided adequate guarantees with regard to the protection of Personal data. In order to comply with its commitment to the protection of Personal data and the fulfilment of its relevant obligations, the Bank takes measures to ensure an adequate level of protection of Personal Data transferred to countries outside the EEA. If Data is transferred abroad, further information on the details of this is available in the information published separately for this purpose on the following website: https://www.kdbbank.eu/adatvedelem-es-adatkezeles.

7. Automated decision-making and Profiling
In the case of loan applications, the Bank carries out credit assessment activities in accordance with Government Decree 361/2009. and Government Decree 32/2014 (IX.10.) MNB on the Functioning of the Museum. In the course of this, the income of the loan applicant and the collateral of the transaction are examined based on the criteria defined in the law by means of so-called profiling. The logic of profiling is based on determining the ratio of the loan applicant's income to the installment of the loan applied for, as well as the ratio of the total loan amount to the value of the collateral. Based on the decision, it is decided whether the loan applicant qualifies as creditworthy or whether the law excludes granting credit to him. This process helps the Bank to make fair and responsible lending decisions.

8. Data security measures
Pursuant to the GDPR and certain provisions of Government Decree 42/2015 (III.12.) on the protection of the IT systems of financial institutions, insurers and reinsurers, as well as investment firms and commodity exchange service providers, the Bank is obliged to ensure the secure operation of its IT system and the appropriate protection of data. The Bank ensures the secure storage of data in all cases in accordance with the legal provisions, by complying with the strict statutory and regulatory supervisory requirements prescribed for the banking sector and the recommendations of professional organisations, under the continuous auditing and control of the supervisory authority and by introducing the appropriate technical and organisational measures in its closed systems.
In order to protect and secure Personal data, the Bank shall implement internal regulatory technical, organisational,
measures to ensure the security of Data processing. As part of this, the Bank will ensure:

- physical security, which includes the physical protection of all elements of the entire IT infrastructure,
- logical security, which includes the allocation of rights based on the principle of minimum logical access to the given IT service, which ensures the confidentiality and integrity of the stored data,

- to carry out risk analyses in which it reveals the possible internal and external risks arising in connection with data management and processing, such as the risk of unauthorized access,
- the smooth execution of backups,
- to protect against certain risks (e.g. phishing emails, viruses, spyware, etc.)
- the application of filtering programs.

9. MANAGE YOUR PRIVACY REQUESTS, EXERCISE OF RIGHTS, ENFORCEMENT AND REMEDIES

Manage your privacy requests
In order to exercise his or her data protection rights, the Data Subject may submit a data protection (data subject) request to the Bank, the deadline for the assessment of which is as a general rule 30 days from the receipt of the request and its content in full. The deadline may be extended once by 60 days, if justified by the complexity of the application or the number of applications. The Bank shall inform the Data Subject of the extension of the deadline within 30 days of receipt and shall also indicate the reasons for it.

If the Data Subject requests the release of an audio recording recorded in connection with the handling of complaints on the telephone concerning him/her, the administrative deadline is 25 days pursuant to Section 288 (2) of the Hpt.

The Bank may refuse to comply with the request if:
- the Data Subject is unable to prove that he/she is the Data Subject with the Data processing or his/her authorised representative;
- the fulfilment of the request is excluded by law or by the contract concluded with the Data Subject;
- if a reimbursement of costs is determined (Article 12 (5) of the GDPR) and the amount thereof is not paid by the Data Subject;
- the request is clearly unfounded or excessive.

If the Bank fails to comply with the Data Subject's request, the Bank shall inform the Data Subject of the reasons for this and of the legal remedies. Information under Articles 13 to 14 of the GDPR and information and action under Articles 15 to 22 and 34 shall be provided free of charge. If the Data Subject's request is clearly unfounded or excessive, in particular due to its repetitive nature, the Bank may charge a reasonable fee or refuse to take action on the basis of the request, taking into account the administrative costs involved in providing the requested information or information or taking the requested action. Data protection requests and responses to them are retained by the Bank for 5 years from the date of their final closure.

9.1. Rights of the Data Subject(s)

9.1.1. Transparent information
The Data Controller shall provide all the information required by the Regulation in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner, in particular in the case of any information addressed to children acting through their legal representative. The information shall be provided by the Data Controller in writing or in another way, such as electronically, but it may also provide oral information at the request of the Data Subject, provided that the identity of the Data Subject has been verified in another way.

9.1.2. Right to Access Your Personal Information
At the request of the Data Subject, the Data Controller shall provide feedback on whether the processing of the Data Subject's Personal data is in progress. If it is established that the Data Subject's Personal data is being processed, the Data Subject may request access to his/her Personal data and the following information:

a) the purpose of the Data processing;
b) the category of Personal data concerned;
c) the recipients or categories of recipients to whom the Personal data have been or will be disclosed by the Data Controller, in particular recipients located in non-EU Member States;

d) the duration for which the Personal data will be stored or, if this is not possible, the criteria for determining this period;
e) the Data Subject's right to request the Data Controller to rectify, delete or restrict the processing of their Personal data, or to object to the processing of their Personal data;
f) the Data Subject's right to lodge a complaint with the Supervisory Authority;
g) if the Data Controller did not collect the Personal data directly from the Data Subject, the source of these Personal data;
h) whether Automated Decision-Making, Profiling has been carried out on the basis of the Personal data and, if so, comprehensible information about the logic used and the significance of such Processing and the expected consequences for the Data Subject;
i) if the Data Controller transfers the Data Subject's Personal data to a country outside the EU or to an international organisation, the Data Subject has the right to be informed about the information related to the transfer.

9.1.3. Rectification of inaccurate Personal data

If the Data Controller processes inaccurate or incomplete Personal data about the Data Subject, it shall rectify them without undue delay after receiving the Data Subject's request. The Data Subject may also request the completion of incomplete Personal data.

9.1.4. Right to erasure (to be forgotten)

The Data Subject has the right to delete his or her Personal data and to request the Data Controller to comply with this request without undue delay, if one of the following reasons applies:

a) the Data Subject's Personal data is no longer needed in connection with the original purpose of the Data processing;
b) the Data Subject withdraws his/her consent to Data processing and there is no other legal basis for Data processing;
c) the lawfulness of the Data processing is based on the legitimate interest of the Data Controller, against which the Data Subject objects, and there is no overriding legitimate reason for the Data processing;
d) the purpose of the Data processing is direct marketing, against which the Data Subject objects;
e) the Data Controller unlawfully processed the Data Subject's Personal data;
f) the Data Subject's Personal data must be erased in order to comply with a legal obligation imposed on the Data Controller by EU or Member State law;
g) the lawfulness of the processing of Personal data by the Data Controller is based on the consent given by a child's guardian, and or
ga) the Data Subject is the child's guardian and the affected child has not yet reached the age of 16 required for consent;
gb) the Data Subject is a child who has already reached the age of 16 required for consent.

The Data Controller may not delete the Personal data if the Data processing is necessary for the following reasons:

a) for the purpose of exercising the right to freedom of expression and information;
b) for the purpose of complying with a legal obligation requiring the processing of Personal data or for the performance of a task carried out in the public interest or in the exercise of official authority;
c) for preventive health or occupational health purposes, necessary under Union or Member State law or under a contract with a healthcare professional, for the assessment of a worker's ability to work, for the provision of medical or social care or treatment, or for the management of health or social systems and services;
d) the processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring a high quality and safety of healthcare, medicinal products and medical devices, and is carried out on the basis of Union or Member State law which provides for appropriate and specific measures to safeguard the rights and freedoms of the data subject; and in particular professional secrecy;

e) for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes, where the Data Subject's right to erasure would be likely to render impossible or seriously jeopardise such Data processing;
f) for the establishment, exercise or defence of legal claims.

9.1.5. Right to restriction of processing

At the request of the Data Subject, the Data Controller shall restrict the processing of Personal data if one of the following is met:

a) the Data Subject contests the accuracy of the Personal data;
b) the Data processing is unlawful and the Data Subject opposes the erasure of the data and instead requests the restriction of their use;
c) the Data Controller no longer needs the Personal data for the purpose of Data processing, but the Data Subject requires them for the establishment, exercise or defence of legal claims;
d) the Data Subject objects to the Data processing carried out by the Data Controller on the basis that the Data Controller has named the legitimate interest of the Data Controller as the legal basis, but the Data Subject claims that its interests take precedence over the interests of the Data Controller.

If Data processing – based on the Data Subject's request – is subject to restriction, such Personal data shall only be

a) with the consent of the Data Subject, or
b) to establish, exercise or defend legal claims, or
c) to protect the rights of another natural or legal person, or
d) important reasons of public interest of the Union or of a Member State
e) can be treated.

The Data Controller shall inform the Data Subject in advance about the lifting of the restriction of Data processing.

9.1.6. Right to data portability

The Data Subject shall have the right to receive the Personal data concerning him or her, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format, and shall be entitled to transmit these data to another Data Controller if:
a) the Data processing is based on consent or a contract; and
b) the Data processing is carried out by automated means.
The Data Subject is also entitled to request the direct transfer of Personal data between Data Controllers.

9.1.7. Right to object

The Data Subject has the right to object to the processing of his or her Personal data if:
a) the Data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
b) the Data processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, including Profiling;
c) the Processing is carried out for the purpose of direct marketing, including Profiling if it is related to direct marketing.

In the case of Data processing based on legitimate interest as defined in point b) above, the Data Subject may not object to the Data processing if the Data Controller proves that:
a) the Processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject, or
b) for the establishment, exercise or defence of legal claims.

If the Data Subject objects to the processing of Personal data for the purpose of direct marketing, the Data Controller will no longer process the Personal data for this purpose.

9.1.8. Automated decision-making in individual cases, including Profiling

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including Profiling, which would produce legal effects concerning him or her or similarly significantly affect him/her.

The Data Subject may not exercise the above right if the decision
a) it is necessary for the conclusion or performance of a contract between the Data Subject and the Data Controller;
b) the adoption of the Act is made possible by Union or Member State law applicable to the Data Controller, which also lays down appropriate measures for the protection of the rights and freedoms and legitimate interests of the Data Subject;
c) is based on the Data Subject's explicit consent.
In the cases referred to in points a) and c) above, the Data Subject may request human intervention, express his/her position and file an objection to the decision.

9.1.9. Withdraw consent
The Data Subject is only entitled to withdraw his consent at any time in Data processing cases based on his or her consent. The withdrawal of consent does not affect the lawfulness of the Data processing based on consent prior to its withdrawal. The Data Controller shall inform the Data Subject thereof before giving the consent.

The Data Subject's statement withdrawing his or her consent is valid with the clear indication of the given Data processing.

9.2. Enforcement, complaint, remedy

9.2.1. Enforcement
The Data Subject may exercise the Data processing rights listed above by e-mail sent to the Data Controller's e-mail address or registered office address from the Data Subject's identifiable e-mail address, or by post in a letter signed by the Data Subject. The Data Subject's statement regarding the exercise of rights is valid with the clear indication of the given Data processing. The Data Controller shall respond to the request submitted electronically in electronic form or in the manner requested by the Data Subject.

9.2.2. Complaining
If the Data Subject considers that the processing of Personal data concerning him or her infringes the provisions of the Regulation, the Data Subject shall have the right to lodge a complaint with the relevant Supervisory Authority, in particular in the Member State of his habitual residence, place of work or place of the alleged infringement.

Complaints may be lodged with the National Authority for Data Protection and Freedom of Information (hereinafter referred to **as the NAIH)** as the Supervisory Authority in the territory of Hungary . Contact details of the NAIH:

E-mail: ugyfelszolgalat@naih.hu
Registered office address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf.: 9.
Phone: +36 (30) 549-6838, +36 (30) 683-5969, +36-1-391-1400,
Fax: +36-1-391-1410
Home page: www.naih.hu

The names and contact details of the data protection authorities in the EU can be found at the http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm link.

9.2.3. Legal remedy

a) Judicial remedy against the Supervisory Authority

Each Data Subject is entitled to an effective judicial remedy:

aa) against a legally binding decision of a supervisory authority, or

ab) if the competent Supervisory Authority does not deal with the complaint or does not inform the Data Subject within three months of the procedural developments related to the complaint submitted or its outcome.

Proceedings against the Supervisory Authority shall be brought before the courts of the Member State in which the Supervisory Authority is established.

b) Judicial remedy against the Data Controller or Data Processor

The Data Subject may turn to court against the Data Controller or the Data Processor if, in his or her opinion, the Data Controller or the Data Processor commissioned or acting on the basis of the Data Controller or acting on the basis of the Data Controller processes his or her Personal data in violation of the provisions on the processing of Personal data specified in the law or in a binding legal act of the European Union.

The procedure shall be initiated before the courts of the Member State in which the Controller or the Processor(s) are established. Such proceedings may also be initiated before the courts of the Member State of the Data Subject's habitual residence, unless the Data Controller or the Data Processor(s) are public authorities of a Member State acting in its capacity as a public authority. In Hungary, the Data Subject may also initiate the lawsuit before the court competent for his or her place of residence or residence, at his or her choice.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

1. ANNEX

NAME OF DATA PROCESSING	PURPOSE OF DATA PROCESSING	SCOPE OF PROCESSED DATA	LEGAL BASIS FOR DATA PROCESSING	DURATION OF DATA PROCESSING
CREDIT SCORE ASSESSMENT	The examination of the creditworthiness and creditworthiness of the (potential) Client and Other Client in the course of credit assessment is carried out in accordance with Section 14 of Act CLXII of 2009 on Credit Granted to Consumers and Sections 3-5 of Government Decree 361/2009 (XII.30) on the Conditions of Prudent Retail Lending and the Assessment of Creditworthiness.	Personal, financial, income and property data necessary for the assessment of creditworthiness.	Compliance with a legal obligation [Article 6(1)(c) of the GDPR].	The Bank shall delete the Client's data constituting bank secrecy in connection with the service contract that has not been concluded, in particular the data related to the rejected loan application, at the same time as the decision on the rejection of the application is made. In the case of a positive (credit) assessment, the Data processing shall last for six years after the termination of the business relationship with regard to the Personal data constituting bank secrecy in connection with the concluded service contract (in particular the (credit) application.
DATA PROCESSING RELATED TO THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORIST FINANCING	Fulfilment of tasks to be performed by law in order to prevent and prevent money laundering and terrorist financing: Fulfilment of Client due diligence obligations; compliance with the obligation to report money laundering; filling out a Client knowledge questionnaire; continuous monitoring of the business relationship; completing screenings; suspension of a transaction; control of sanctions and prohibited lists as defined by law; the implementation of financial and property restrictive measures; keeping a record of the data and documents recorded in the course of the Client Due Diligence, as well as of all other data and documents (original or copies) recorded in connection with the individual transactions and ensuring their identification.	PMT. (2), 8 (2)-(3), 9 (1)-(2), 10 (1)-(2), 30 (2), the data specified in Article 4 of Regulation (EU) 2023/1113 of the European Parliament and of the Council , the data specified in Act LII of 2017 on the Implementation of Financial and Property Restrictive Measures Ordered by the European Union and the UN Security Council (Kit.) and the data specified in Section 14. § (1)-(3) , and 15 § of the Decree No. 14/2025. (VI. 16.) of the MNB.	Compliance with a legal obligation [Article 6(1)(c) of the GDPR].	Data processing lasts for eight years from the termination of the business relationship or the completion of the transaction order. (Pmt. 56. § (2) ,57. § (1)-(3) paragraphs) In the event of a request from the financial intelligence unit, the investigating authority, the public prosecutor's office or the court, Data processing shall continue for the period specified in the request, but for no longer than ten years from the termination of the business relationship or the completion of the transaction order (Section 58 (1) of the Pmt.).
CRS (TAX RESIDENCY EXAMINATION FOR FINANCIAL ACCOUNTS)	Conducting a tax due diligence procedure in order to determine in which CRS participating country(s) account holders are tax residents, and in accordance with Act XXXVII of 2013 on Certain Rules of International Administrative Cooperation in Relation to Taxes and Other Public Charges, Annex II-VII of CRS. Fulfilment of the data reporting obligation in accordance with the due diligence rules set out in the	Data specified in Section I of Annex 1 of Act XXXVII of 2013.	Compliance with a legal obligation [Article 6(1)(c) of the GDPR] on certain rules of international administrative cooperation in relation to taxes and other public charges pursuant to Section 43/H of Act XXXVII of 2013.	With regard to the data generated in connection with the examination of the tax residence of financial accounts, the Data processing lasts for six years after the termination of the business relationship.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

	Tax Act to the State Tax Authority by 30 June of the year following the tax year.			
FATCA (US TAX RESIDENCY INVESTIGATION)	Conducting the due diligence procedure in accordance with Annex I of Act XIX of 2014 (Fatca Act) and reporting annually to the NAV on the information specified in Article 2(2)(a) in the manner and at the time specified in Article 3.	The Bank processes tax residency data and the data specified in Article 2 (2) (a) of Act XIX of 2014.	Compliance with a legal obligation [Article 6(1)(c)] of the GDPR Pursuant to Article 4(1)(a) of Act XIX of 2014.	With regard to the data generated in connection with the examination of the tax residence of financial accounts, the Data processing lasts for six years after the termination of the business relationship.
PROVISION OF SERVICE	Prior to the conclusion of the service contract, taking steps at the request of the (potential) Client and Other Client, preparing the service contract, establishing the contractual relationship, exercising the rights and fulfilling obligations arising from the service contract, providing services; registering and storing the contract and any type of document related to it, keeping the credit file; monitoring and controlling the life cycle of the contract.	Data necessary for the establishment, performance, maintenance and termination of the service relationship, (Client) identification (authentication) data, contact data (mailing address, e-mail address, telephone number), data of the (Client) contract, including data necessary for the conclusion of the contract for the provision of the given service or for the performance of the contract, data necessary for Client qualification, the results of the Client qualification, payment transactions, account transactions necessary data, data of individual Client transactions.	Performance of a contract pursuant to Article 6(1)(b) of the GDPR.	Data processing shall continue for eight years after the termination of the business relationship with regard to Client data constituting banking secrets in connection with the service contract concluded. Accounting documents, in particular contracts, settlement and installment payment agreements, cash flow statements, bank statements, cash receipts, property rights and cost-related court decisions, final judgments, and the data contained therein shall be retained by the Bank for eight (8) years following the year of approval of the annual report for the year in which the last accounting document related to the service contract was issued (Section 169(2) of the Accounting Act and Sections 56-57 of the Payment Services Act). The Bank shall delete any sectoral secrets related to the service contract that did not come into effect, in particular Client data constituting banking secrets, at the same time as it makes its decision to reject the request for the provision of the service.
PRIOR INFORMATION OBLIGATION (APTITUDE AND COMPLIANCE TEST)	To explore the income situation and investment objectives of the Prospective (contracting party) Client and the Client in order for the Bank to recommend to the Prospective Client or the Client an appropriate transaction or financial instrument that is in line with its circumstances and in line with its ability to bear losses and is suitable for the realisation of its investment expectations.	Prospective Client and Client's completed compliance and suitability test data, other data and documents that may be requested on the basis of the Business Regulations for Investment Services data of a declaration of assets or income.	Fulfilment of a legal obligation [Article 6(1)(c) of the GDPR] with regard to the provisions of Sections 44-46 of the Criminal Code.	Data processing shall continue for eight years from the termination of the relevant framework agreement or the claim arising therefrom, in accordance with Sections 56-59/A of Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (Pmt.) and Sections 56-59/A thereof, for the purposes specified therein, and for 5 and 7 years, respectively, pursuant to Section 55(10) of the Bszt. for the purposes specified therein.
PROCESSING OF PERSONAL DATA OF	Handling Other Client's requests, requests for quotations and inquiries related to the conclusion of contracts.	Contact details provided by the Data Subject: home address, mailing or other contact address; phone number, e-mail address.	Consent of the Data Subject GDPR pursuant to Article 6 (1) (a).	Data processing lasts until the withdrawal of the Data Subject's consent, and if no contract is concluded, the Bank shall arrange for the deletion of the data after the conclusion of the contract fails.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

PERSONS WISHING TO CONTACT THE BANK				
IMPLEMENTATION OF DEBT MANAGEMENT AND DEBT COLLECTION MEASURES IN JUDICIAL, OUT-OF-COURT AND ADMINISTRATIVE PROCEEDINGS, ENFORCEMENT OF LEGAL CLAIMS AS WELL AS THE REGISTRATION OF CLAIMS	Management of claims, implementation of measures with the goal of collection , protection of legal claims (in judicial, out-of-court, and administrative proceedings), and the registration and administration of claims for the purpose of settling the Bank's claim and/or legal demand against the Client.	Natural identification data, other personal identification data, copies of documents, photo copies, copies of signatures, traceability addresses, data related to liability/performance liability and its enforceability, legal facts.	The Bank's legitimate interest [pursuant to Article 6(1)(f) of the GDPR.	The Data processing lasts until the time when the Client has an overdue, non-overdue or ancillary debt to the Bank arising from the transaction in question. or there is or is expected to arise in connection with the transaction, which is a maximum of 8 (eight) years from the termination of the claim or legal dispute, taking into account Section 169 (2) of the Sztv.
DEBT MANAGEMENT, COMMUNICATION, REPRESENTATION AND REGISTRATION RELATED TO DEBT COLLECTION	Investigation of contact and representation in connection with the collection of a claim against the Client.	Natural identification data, other data for personal identification, copies of documents, photographic copies, copies of signatures, contact addresses, data related to the type, subject, duration and extent of representation.	The Bank's legitimate interest [pursuant to Article 6(1)(f) of the GDPR.	The Data processing lasts until the time when the Client has an overdue or non-overdue debt against the Bank arising from the transaction in question, or there is a legal dispute or is expected to arise in connection with the transaction, which is no more than 8 (eight) years from the termination of the claim or legal dispute, taking into account Section 169 (2) of the Sztv.
MANAGEMENT AND SALE OF ASSETS OWNED BY BANKS IN CONNECTION WITH DEBT MANAGEMENT AND RECORDS	Ensuring the documentation of the management and sale of assets owned by the Bank in connection with debt management.	Recording of identity and other data of contracting parties, transaction agents, in particular witnesses and lawyers, copies of documents Name ID and contact details of other 3rd person interested parties or their representatives.	The Bank's legitimate interest [pursuant to Article 6(1)(f) of the GDPR.	Data processing lasts until the time when the asset ,acquired by the Bank, in connection with the receivables management is sold, or if there is or is expected to be a legal dispute in connection with the sale, the duration of the Data processing shall last for a maximum of 8 (eight) years from the termination of the sale or legal dispute, taking into account the provisions of the Actv. Section 169 (2) of the Sztv.
COMPLAINT HANDLING	Fulfilment of the statutory complaint handling and record-keeping obligations.	Data necessary for the fulfilment of the complaint handling and record-keeping obligation, in particular the Client/Other Client identification (authentication) data and the data of the Client/Other Client communication, including	Compliance with legal obligations pursuant to Article 6(1)(c) of the GDPR, with regard to Section 288(1) of the Hpt., Section 121(1) of the Bszt., Section 70(1) of the Fsztv., Section 16(4) of the KHR tv.and Sections 3(2)-(3) of Government Decree 435/2016 (XII. 16).	Data processing shall continue for the period specified in Section 288(3) of the Hpt., Section 121(3) of the Bszt. and Section 70(3) of the Fsztv. (for 5 years following the closure of the complaint).

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

		any Personal data related to the Data Subject presented in the course of complaint handling.		
RECORD AUDIO	- Fulfilment of the statutory obligation to record for complaint handling and registration purposes Hpt. Section 288 (2), (Section 121 (2) of the Bszt, Section 70 (1) of the Fsztv.	Client/Other Client Identification (Authentication) Data, Client /Other Client Communications Data, Human Voice.	Compliance with a legal obligation pursuant to [Article 6(1)(c)] of the GDPR with regard to the provisions of the Hpt. Section 288 (2), Section 121 (2) of the Bszt. Section 70 (1) of the Fsztv.	Data processing shall be carried out in accordance with Section 288(2) of the Hpt., Section 121(2) of the Bszt. Section 121(2) of the Bszt. and Section 70(2) of the Fsztv. for a period of five years from the date of recording, or for a maximum of seven (7) years if so required by the Hungarian National Bank acting in its supervisory capacity.
	- Conclusion of contracts within the framework of distance selling (Section 55 (4) of the Bszt); - Provision of client order services related to the taking, forwarding and execution of orders (Section 55 (4) of the Bszt);	Client/Other Client Identification (Authentication) Data, Client /Other Client Communications Data, Human Voice.	Fulfilment of a legal obligation pursuant to [Article 6(1)(c)] of the GDPR, taking into account the provisions of Section 55 (4)-(6) of the Bszt.	Data processing, pursuant to Section 55 (10) of the Bszt., for five years from the date of recording, or for a maximum of seven (7) years if required by the Hungarian National Bank acting in its supervisory capacity.
RECORDING OF COMMUNICATIONS RELATED TO CLIENT ORDERS TAKEN WITHIN THE FRAMEWORK OF INVESTMENT SERVICES	Recording communications related to client orders taken within the framework of investment services, including conversations and exchanges of messages that do not lead to the provision of client order services.	Client/Other Client identification data, including the name of the Other Client, data of communication related to client orders, including data of conversations and exchanges that do not lead to the provision of client order services, as well as voice recordings and the telephone number of Other Clients.	Compliance with a legal obligation [Article 6(1)(c) of the GDPR]. MiFID II. Article 16 (6)-(7), recital (57); Article 25(1) of MiFIR;Article 74-76 of Regulation (EU) 2017/565 and Sections 1-2 of Annex IV, Section 55 of the Decree on Consumer Rights. §.	The Data processing shall be kept by the Bank for five years from the date of recording, or for a maximum of 7 (seven) years if required by the competent authority.
MANAGE REFERENCE DATA	Fulfilment of the statutory Data processing obligation by handing over the registered reference data to the Central Credit Information System (hereinafter referred to as: KHR) and by receiving, maintaining and registering reference data from the KHR; a more informed assessment of creditworthiness and the promotion of credit risk reduction in order to ensure the safety of reference data providers.	Act CXXII of 2011 on the Central Credit Information System (KHR Act.) of Annex II, Section 1.	Compliance with a legal obligation under [Article 6(1)(c)] of the GDPR KHR tv. Section 5 (2) a), (7) points a)-b) KHR Act , Section 6 (3)-(6), (7) b) KHR Act §§ 11-13, 18 § (1) 19 (1) of the GDPR. and the consent of the Data Subject pursuant to Article 6 (1) a) of the GDPR pursuant to Section 5 (3) of the KHR Act.	Data processing is based on the provisions of Section 8 (2) of the KHR Act. from the start of the retention period 5 years.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

DATA PROVISION THAT DOES NOT VIOLATE BANK SECRECY TO CLOSE RELATIVES	In connection with all services provided by the Bank to the testator, in particular but not exclusively: the amount of the outstanding debt in connection with the loan taken out and not yet repaid by the deceased and the unexpired financial lease, the amount of the overdue debt, the monthly instalment due, the account number to which the instalment is to be paid (credit account number) and the remaining term for the close relative of the testator - at the written request of the Student Union.	– Name of a close relative – place and date of birth – mother's name – Address / mailing address – ID Type: ID Card / New Type Driver's License / Passport – ID number – Telephone number	Fulfilment of a legal obligation pursuant to [Article 6 (1) c) of the GDPR] pursuant to the Hpt. Section 164 (y) of the Bszt.	Data processing lasts until the day of becoming aware of the final closure of the probate procedure, and the Hpt. 164 (y) of the Bszt.
ENFORCEMENT OF CLAIMS AGAINST HEIRS	Enforcement of the property claim against the heir who is financially liable for the debts of the estate - to a limited extent - in an out-of-court procedure, or in the event of failure of this in a litigation procedure.	Data necessary for the enforcement of claims, in particular natural identification data, contact details, data of the claim; as well as data generated in the course of the enforcement of the claim, data necessary for the verification of representation and identification, copies of documents, photographic copies, copies of signatures.	The Bank's legitimate interest in enforcing its financial claim against the heir who has the legal status of the testator in respect of the claim [Article 6(1)(f) of the GDPR].	Data processing shall continue for eight (8) years from the date of extinction of the claim, in accordance with Section 169(2) of the Sztv.
DATA PROCESSING RELATED TO INTERNAL AUDIT	Ensuring the operation of the internal banking control function prescribed in Section 107 (1) of the Hpt.	Personal data of Clients and Ad hoc Clients that are strictly necessary for the performance of internal audit activities.	Fulfilment of legal obligations [GDPR Article 6(1)(c)] with regard to the provisions of Sections 107(1) and 108(5) of the Hpt.	Data processing lasts for 10 years after the completion of the verification procedure.
OPERATION OF AN ELECTRONIC SURVEILLANCE SYSTEM	Property protection, prevention, detection and proof of crimes against property, violent crimes against property, offences against property, crimes against life, physical integrity and health, catching the perpetrator in the act, as well as the protection of business, payment, banking and securities secrets; and to enable the establishment of legal consequences in the event of a breach of protection.	His/her image and situational data displayed on video recordings of the movements of those entering and staying in the banking area monitored by security cameras during opening hours.	The legal basis of Data processing is the Bank. the Bank's legitimate interest in the protection of property, persons and secrecy pursuant to Article 6(1)(f) of the GDPR or in the performance of the Bank's legal obligation pursuant to Article 6(1)(c) of the GDPR, taking into account the provisions of Section 11(3) of Government Decree No. 297/2001 (XII.27.) on currency exchange activities.	Data Management is critical to the Bank's operation, The period of storage of motion pictures in protected banking units or closed to the public, as well as in areas of bank branches directly affected by cash flow, lasts for 30 days from the date of recording, and in the case of recordings recorded due to currency exchange activities, for 50 days from the date of recording.
DATA PROCESSING RELATED TO DIRECT MARKETING, MARKET RESEARCH AND CLIENT	Direct marketing inquiries, market research and Client satisfaction measurement.	Client/Other Client's name, contact details (mailing address, e-mail address, phone number).	Consent of the Client and Other Clients [Article 6(1)(a) of the GDPR]	Data processing shall continue until the withdrawal of consent, at the latest for five (5) years from the date of giving the consent.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

SATISFACTION MEASUREMENT				
BACKUP	Providing a backup that allows the recovery of the given banking system within the critical recovery period of the service provided by the system, ensuring the safe restoration of the system.	Client/Other Client Data generated during backup.	Compliance with a legal obligation [Article 6(1)(c) of the GDPR] pursuant to Section 3(3)(e) and Section 5/B (d) of Government Decree No. 42/2015 (III.12.) on the protection of the IT systems of financial institutions, insurance companies and reinsurers, investment firms and commodity exchange service providers.	Data processing lasts for 5 years from the date of backup.
PROCESSING OF SENSITIVE DATA	Ensuring equal access to banking services for Clients and Other Clients.	The need to use special devices provided within the framework of the service provided to the disabled Client/Other Client in view of their special condition and the named special device.	Consent of the Client/Other Client [Article 9(2)(a) of the GDPR].	The Data processing lasts for twenty years from the date on which the sensitive data concerned were recorded.
GIRINFO	In relation to the Client and Other Clients: -carrying out identity verification as part of the performance of Client due diligence tasks; - reducing credit risks and resulting losses, - quick lending decision-making, - the fight against money laundering, - checking the address and most important documents of natural persons, - access to the most up-to-date and extensive company information Performing a verification of the identity of the Client/Other Client in the context of debt management and collection procedures	Name; place and date of birth; citizenship; type of identification document; identifier document number; the expiry of the validity of the identification document; effigy; address card number; address card date of issue; permanent address; temporary address; copies of documents.	The legal basis for the inquiries carried out within the framework of the Client due diligence obligation is the fulfilment of the Bank's legal obligation [Article 6(1)(c)] of the GDPR, taking into account the provisions of the Pmt. Section 7 (3) .The legal basis for inquiries regarding debt management and collection procedures is the Bank's legitimate interest [Article 6(1)(f) of the GDPR.	Data processing shall continue for eight years from the termination of the Client relationship, pursuant to Sections 56-59/A of the Pmt. and Section 169(2) of the Sztv. In the event that the conclusion of the contract fails, the Bank shall delete the Personal data processed after the failure of the contract.
DATA BREACHES (INCLUDING THE INCIDENT MANAGEMENT STEPS TAKEN IN RELATION TO THE DOCUMENTATION)	Registration of Personal data breaches and their possible reporting to the NAIH and the Data Subjects' information on the matter.	Personal data of the data subjects related to the data breach.	Article 6 (1) c) of the GDPR (DFata processing is necessary for compliance with a legal obligation to which the Bank is subject as Data Controller**).** The obligation to keep an incident record is prescribed by Article 33(5) of the GDPR.	Unless otherwise required by the authorities, Data processing lasts for 5 years from the occurrence of the Personal data breach, given that within this period it can be realistically expected that any data protection claims will be enforced before the data protection authority or the court (Section 6:22 (1) of the Civil Code – unless otherwise provided by the Civil Code, claims expire in 5 years).

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

HANDLING OF DATA RELATED TO THE OBJECTION PROCEDURE	To ensure that the objection handling procedure initiated by the Client/Other Client is conducted.	- Client/Other Client's name, bank account number, e-mail address, telephone number - the name and bank account number of the beneficiary involved in the objection handling procedure	Consent of the Client/Other Client [Article 6(1)(a) of the GDPR].	The Data processing lasts for 5 years after the termination of the payment account of the Client affected by the objection handling procedure.
PROCESSING OF DATA RELATED TO THE PAYMENT MORATORIUM	Compliance with the [2]provisions of the law in connection with the Client's application for a payment moratorium.	Personal data provided by the Client.	The Client's consent is Article 6(1)(b) of the GDPR, taking into account the provisions of the moratorium legislation.	Data processing shall be retained for 8 years from the termination of the contract affected by the moratorium or the claim arising therefrom, in accordance with Sections 56-59/A of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.
PROCESSING OF DATA RELATED TO THE OPERATION OF THE CENTRAL ABUSE SCREENING SYSTEM (KVR)	To determine the risks of misuse related to payment transactions and to ensure the fulfilment of Data transfer to the Central Fraud Screening System operated by GIRO Zrt. for the purpose of determining the risks of misuse related to these payment transactions and supporting the detection and prevention of misuse related to these payment transactions. **Information on joint Data processing:** With regard to this Data processing, the Bank and GIRO Zrt., as the operator of the Central Abuse Screening System (DIP), **qualify as joint Data Controllers.** Data subjects may turn to any Data Controller in connection with Data processing activities qualifying as joint data management. The Bank shall proceed with regard to the response to any request addressed to the Data Controller for the exercise of the right of the data subject.	The data of the HUF payment orders to be processed, settled and executed in the payment system operated by GIRO Zrt., as well as the data specified in Sections 1-19 of Annex 2 of Act LXXXV of 2009 on the Provision of Payment Services (Pft.), as well as the data returned from the Bank's own Clients.	Compliance with a legal obligation pursuant to Article 6 (1) c) of the GDPR (Data processing is necessary for the fulfilment of a legal obligation pertaining to the Bank as Data Controller), taking into account the provisions of Section 55/D (1) of the Pft.	Data processing lasts for 8 (eight) years following the year of adoption of the annual report on the year of issuance of the last accounting document related to the Contract (which also includes the termination of the Contract), taking into account the provisions of Section 169 (2) of the Sztv.

[2] Moratorium legislation, payment moratorium: Government Decree 47/2020 (III.18.) on the immediate measures necessary to mitigate the impact of the coronavirus pandemic on the national economy and Government Decree No. 47/2020 (III.18.) on the detailed rules of the payment moratorium on the immediate measures necessary to mitigate the impact of the coronavirus pandemic on the national economy, as well as the Act LVIII of 2020 on Transitional Rules Relating to the End of the State of Emergency and on Epidemiological Preparedness, Act CVII of 2020 on Temporary Measures to Stabilise the Situation of Certain Priority Social Groups and Enterprises in Financial Difficulties, and Government Decree No. 637/2020 (XII.22.) on the introduction of special rules on loan repayment in connection with the state of emergency, and payment moratorium under the derogation set out in Act CXXX of 2021 on certain regulatory issues related to the Consumer Protection Act.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

PROCESSING OF DATA RELATED TO THE PROVISION AND/OR TRANSFER OF DATA TO AUTHORITIES	In the event of a data request, ensuring compliance with requests for the provision of data submitted by investigative authorities, the public prosecutor's office, courts, national security services, or other authorities (e.g. municipal clerks, civil law notaries, guardianship authorities, the Central Bank of Hungary (MNB), the Hungarian Competition Authority (GVH), the National Tax and Customs Administration (NAV), the Hungarian State Treasury (MÁK), the Commissioner for Fundamental Rights, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), etc.), where such requests are authorized by law.	Personal data recorded in the request submitted by the authority legally entitled to request such data, as well as in the Bank's written response to that request.	Compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR (i.e. the processing is necessary for compliance with a legal obligation to which the Bank, as Data Controller, is subject), taking into account the data disclosure obligations set out in the specific legislation governing the request, as well as the provisions of Hpt. relating to banking secrecy (Sections 160–165).	The data processing shall continue for a period of 5 years from the completion of the request, taking into account the general limitation period of 5 years pursuant to Section 6:22(1) of the Ptk.
PROCESSING OF DATA RELATED TO JUDICIAL AND NON-JUDICIAL COURT PROCEEDINGS, AS WELL AS OTHER ADMINISTRATIVE PROCEEDINGS, FOR THE PURPOSE OF LEGAL CLAIMS ENFORCEMENT OR DISPUTE RESOLUTION CONCERNING NATURAL PERSONS (WHERE DEBT MANAGEMENT AND DEBT COLLECTION-RELATED DATA PROCESSING IS OTHERWISE NOT CARRIED OUT)	The purpose of data processing in connection with judicial and administrative proceedings, whether litigious or non-litigious, is to effectively ensure the resolution of disputes or the enforcement and protection of rights before courts and other authorities (unless data processing is carried out for the purposes of CLAIM MANAGEMENT, DATA PROCESSING FOR COLLECTION PURPOSES, in which case data processing takes place within the framework of the latter).	- personal identification data, including in particular: name, birth name, mother's name, place and date of birth - contact information, including in particular: residential address, current address, mailing address, email address, phone number - official identifiers: tax identification number, ID card number - procedural data, in particular: content of submissions, image and audio recordings - special personal data in certain court cases - any other personal data necessary for the resolution of the legal dispute (this information depends on the type of case), as well as other personal data contained in documents generated during the litigation process	The Bank's legitimate interest pursuant to Article 6(1)(f) of the GDPR.	Data processing shall continue for a period of 5 years from the date on which the final decision concluding the proceedings becomes final, in accordance with the general statute of limitations (5 years) set forth in Section 6:22(1) of the Ptk.

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

DATA PROCESSING RELATED TO INQUIRIES/REQUESTS RECEIVED FROM NATURAL PERSONS ACTING AS THIRD PARTIES AND THE BANK'S RESPONSES THERETO	Ensuring that inquiries and requests received from natural persons classified as third parties are handled and responded to (unless such processing constitutes DATA SUBJECT REQUEST PROCESSING, in which case the processing is carried out within the framework of the latter).	Personal data recorded in inquiries/requests received from natural persons qualifying as Third parties, as well as in documents containing the Bank's responses to such inquiries/requests.	The consent of the natural person qualifying as a Third party pursuant to Article 6(1)(a) of the GDPR, where such consent to the processing of personal data is deemed to be granted within the scope of the data provided in the inquiry/request and for the purpose specified therein.	The data processing shall continue until the purpose of the processing has been fulfilled, or until the consent is withdrawn, but for no longer than 6 (six) months.
PROCESSING OF DATA RELATED TO DATA SUBJECT REQUESTS	Handling data protection-related questions and requests concerning the processing of personal data of the Data Subject (Client / Other Client) and natural persons qualifying as Third parties, as well as ensuring cooperation in any related administrative proceedings conducted by the competent supervisory authority.	Personal data recorded in the data protection-related questions and requests submitted by the Data Subject (Client / Other Client) and natural persons qualifying as Third parties concerning the processing of their personal data, in the Bank's responses thereto, as well as in documents containing requests from the data protection authority related to the data subject request and the Bank's responses to such requests.	The Bank's legitimate interest pursuant to Article 6(1)(f) of the GDPR.	The data processing shall continue for a period of 5 years from the date of the Bank's response to the request or, where the supervisory authority initiates proceedings, from the date on which the substantive decision concluding such proceedings becomes final, taking into account the general limitation period of 5 years pursuant to Section 6:22(1) of the Ptk.
DATA PROCESSING CARRIED OUT WITHIN THE FRAMEWORK OF THE DIGITAL CITIZENSHIP PROGRAM (DÁP)	**Processing of the Digital Citizenship Identifier (DÁP ID) following successful registration** The purpose of the data processing is to enable regular login via eligible electronic channels using the Digital Citizenship application.	- Client's name - Client's place and date of birth - Client's citizenship - Digital Citizenship Identifier (DÁP ID)	The Bank's legitimate interest pursuant to Article 6(1)(f) of the GDPR.	The data processing shall continue for a period of 8 (up to a maximum of 10) years following the termination of the business relationship, taking into account the provisions of Sections 56–58 of the Pmt.
	Processing of the Digital Citizenship Identifier (DÁP ID) and other personal data in the event of unsuccessful registration The purpose of the data processing is to facilitate error handling in the event of an unsuccessful DÁP ID registration.	- Client's name - Client's place and date of birth - Client's citizenship - Digital Citizenship Identifier (DÁP ID)	The Bank's legitimate interest pursuant to Article 6(1)(f) of the GDPR.	---------- ----------

KDB Bank Európa Zrt.
Address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Central fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

	Retrieval and updating of data via the DÁP Consent-Based Data Provision Service (HAASZ) The purpose of the data processing is to enable the Bank to automatically update the Clients' identification data using the information available through the Consent-Based Data Provision Service (HAASZ) operated within the framework of the Digital Citizenship Program (DÁP).	- Client's name - Client's place and date of birth - Client's citizenship - Digital Citizenship Identifier (DÁP ID)	The Client's consent (as provided in the DÁP application) pursuant to Article 6(1)(a) of the GDPR.	The data processing shall continue for a period of 8 (up to a maximum of 10) years following the termination of the business relationship, taking into account the provisions of Sections 56–58 of the Pmt.