KDB Bank Europe Ltd.
Address: 1054, Budapest, Bajcsy-Zsilinszky street 42-46.
KDB Kontakt (Call Center): +36 1 473 4440, +36 1 374 9990
Fax: +36 1 328 5454
Web: www.kdbbank.eu
E-mail: info@kdbbank.eu

Announcement

Data management Informative

on the management of client's and other Data Subject's personal data

Effective as of 25.05.2018.

KDB Bank Europe Ltd. (seat:1054 Budapest, Bajcsy-Zsilinszky út 42-46.; registration n: 01-10-041313; tax n: 10326556-2-44; hereinafter referred to as **Bank**) as data manger manages the personal data of its clients and other effected persons in compliance with the laws and regulations on data protection under the conditions below, especially upon the Regulation 2016/679 of the European Parliament and of the Council (hereinafter referred to as the **GDPR**) and the Act CXII of 2011 on the right of informational self-determination and freedom of information (hereinafter referred to as the **Info Act**).

I. Definitions

a) **Data Subject:** shall mean a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly. The Data subject is primarily the client, ex-client of the Bank and those persons who are intending to enter into connection with the Bank and whose Personal Data are managed by the Bank in connection with the service rendering during the Data Management.

b) **Personal Data:** any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

c) **Special Data:** shall mean:

a. Personal Data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and Personal Data concerning sex life,
b. Personal Data concerning health, pathological addictions, or criminal record;

d) **Data Management:** shall mean any operation or set of operations which is performed on personal data, or on sets of personal data, whether or not by automated means, such as in particular collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and blocking the Personal Data from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images).

e) **Data Manager:** shall mean the natural or legal person, unincorporated body or other body which alone or jointly with others determines the purposes and means of the processing of personal data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them.

f) **Data Processor:** shall mean a natural or legal person, unincorporated organization or other body that is engaged under contract in the processing of personal data, including when the contract is concluded by virtue of law, or which processes personal data on behalf of the Data Manager.

g) **Recipient:** a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

h) **Third Party**: shall mean any natural or legal person, unincorporated organization or body other than the Data Subject, the Data Manager or the Processor and persons who, under the direct authority of the Data Manager or Processor, are authorised to process Personal Data.

i) **Data Subject Consent:** means any freely and expressly given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations.

j) **Bank secret:** All facts, information, know-how or data in the Bank's possession on clients relating to the person, data, financial standing, business activities, management, ownership and business relationships as well as the balance of and transactions executed on the account of a client at the Bank as well as to his contracts entered into with the Bank shall be construed bank secrets.

k) **Securities secret:** shall mean all data and information that is at the disposal of an investment firm, an operator of multilateral trading facilities or a commodity dealer concerning specific clients relating to their personal information, financial standing, business operations and investments, ownership and business relations, and their contracts and agreements with any investment firm or commodity dealer, and to the balance and money movements on their accounts;

l) **API** (Application Programming Interface): electronic platform sharing clients' data on which the Bank provides data to TPPs in line with its legal obligation

m) **TPP** (Third Party Provider): Service provider which base on 18 and 19 Points of PSD2 renders aggregated account infromation and mandate based online transfers.

n) **Authority**: Hungarian National Authority for Data Protection and Freedom of Information

II. Applicable legal regulations to Bank's Data Management

a) Regulation (EU) 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 (GDPR)

b) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Info. törvény);

c) Act V. of 2013 on the Civil Code (hereinafter: Ptk.);

d) Act CCXXXVII. of 2013 on the credit insitutions and financial enterprises (hereinafter: Hpt.);

e) Act CL of 2017 on the rules of taxation (hereinafter: Art.);

f) Act VI of 1998 on the protection of individuals and the automatic process of personal;

g) Act CLV of 2009 on the protection of qualified data;

h) Act CXX of 2001 on capital market (hereinafter: Tpt.);

i) Act CXXXVIII. of 2007 on the investment service providers, stock exchanges and the rules of thier activities (hereinafter: Bszt.);

j) Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: Pmt.);

k) Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators;

l) Act LXVI of 1992 on the regsitry of personal data and address of the citizens;

m) Act CXXII of 2011 on the Central Credit Information System (hereinafter: KHR Act);

n) Act LXXXV of 2009 on Payment Services (hereinafter: Pft.).

o) REGULATION (EU) No 600/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (hereinafter: EUR)

p) Act C of 2000 on Accounting,

q) MNB Decree 19/2017. (VII. 19.) on the detailed regulations of the enforcement of Act on Prevention and Combating of Money Laundering and Terrorist Financing with regard to MNB's supervised service providers and of the minimum requirements for the design and operation of a filtering system according to the Act on the Implementation of the Financial and Pesticide Restrictive Measures imposed by the European Union and the United Nations Security Council;

r) REGULATION (EU) 2015/847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;

s) DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

t) MNB Decree 28/2017 (XI.22.) on the reporting obligations of the money and credit market organizations to the central bank information system primarily to fulfill the supervisory functions of the National Bank of Hungary;
u) MNB Decree 35/2017 (XII. 14.) on management of payment services

III. Principles of Data Management

The Bank shall manage any personal data only for determined aim, fulfillment of contract, in order to exercise any rights or fulfill any legal obligation, in order to protect the vital interests of the Data Subject or of another natural person, or for the purposes of the legitimate interests pursued by the Bank or by a third party. The data management shall comply in each phase to its aims, it has to be clearly defined and legitimate. Recording any management of the personal data shall be done in a lawful and fair way and in any case it must be carried out in a transparent way for the Data Subject. The Bank manages personal data according to the data minimisation principle, therefore it manages only those personal data which are essential for reaching the aim of the data management and adequate to reach the aims, suitable, relevant and necessary. Any personal data shall only be managed until in quantity and time it is necessary to reach its aims.

IV. Purpose of Data Management:

Preparation, conclusion and enforcement of the contract by and between the Bank and client, Bank's **direct marketing and market research** (by letter, telephone, or other, electronic and other means of communication), **using API or TPP in case under operation under PSD 2, performing transfer via instant payment system** and in case of the client's consent to this effect expressed in the Declaration for data management and **granting the same access to the services of the Bank**. Further purposes of the data management are (i) facilitating of the direct evaluation of the client's needs by Bank's employees in order to be able to satisfy such needs with higher level services (**preparing statistics**); (ii) **risk management** (analysis, appraisal, reduction, fulfilment of the criteria for the prudent operation, risk taking and capital reserve regulations); (iii) **combating, investigating and exploring the misuse of the products, services offered by the Bank**; (iv) **fulfilment of the Bank's legal obligations, exercising its legal interests**, such as fulfilment of the obligations set forth in the laws and regulations on the prevention and combating of money laundering and terrorism, and on the financial and investment services offered by Bank; (v) and exercise of the rights and fulfilment of the obligations arising from the contract following its termination, such as exercising the claim based on the contract as well as the Bank's internal control functions, compliance with accounting standards, fulfillment of reporting obligations (eg. towards OBA or other authorities). Further purpose of the data management is to handle customer complaints.

In case of compulsory data management set forth by law – besides the performance of the contract by and between the client and the Bank – purpose of the data management is the **fulfilment of Bank's legal obligation on data management.**

V. Legal ground of the data management:

Upon GDPR the Bank shall handle personal data existing under on one of the following legal bases

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing 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;
c) processing is necessary for compliance with a legal obligation to which the Bank as a controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the purposes of the legitimate interests pursued by the Bank as controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In case the Bank manages the data on the basis of the consent of the Data Subject then the data management is preceded by the registration of the voluntary, clear and explicit statement of consent of the Data Subject received appropriate information. The consent of the Data Subject is effective without any time limit and until withdrawal. The Data Subject may withdraw its consent at any time by mail sent to the KDB Bank Europe Ltd. of the PO. box of 1382 Budapest, Pf. 1 or by electronic massage sent to the e-mail address of info@kdbbank.eu to the Bank or via telephone on the phone numbers: +36 1 473 4440 or +36 1 374 9990. Relating to any data management that is based upon consent, in case of cancellation of the consent subject to that the data management has another legal ground – the Data Subject shall be immediately informed about changing to another legal ground. The cancellation of the consent shall not affect the lawfulness of data processing made upon the consent and before the cancellation.

Any personal data can only be handled at a single legal title at the same time (at the legal title the Data Subject was informed about by the Bank when the personal data was received), however, there is no obstacle to be marked more legal titles by the Bank in connection with one personal data. However, there may be a change between these legal titles only if for example the Data Subject withdraws the consent to the data management, but with regard to another legal title, the Banks still has to manage the personal data. In this case, the Data Subject must be properly informed of the new legal title.

VI. Types of personal data

a) Personal identification data: the aim of the management of these personal data is the identification and to connect the relevant person. The unit of the Bank responsible for the data management manages the following personal data of the Data Subject: name, original name, mother's maiden name, place and date of birth, citizenship, address, ID card (passport, card format driving license) no., number of other document which is adequate to identify itself in line with the Act LXVI of 1992 on personal data and address registry of citizens. The basis of the data management primarily is the fulfillment of the contract and, in addition, the fulfillment of the legal obligations, the protection of a vital interest and the enforcement of a legitimate interest. In case the Data Subject does not provide the personal data referred to in this paragraph this may entirely or partially result in the blocking of contracting or the usage of the service.

b) Phone numbers necessary for get into contact with the Data Subject and other contact details: Should the Data Subject give its phone numbers or email address after the consent was given, orally or in a written form, the unit of the Bank responsible for the data management manages these data primarily to fulfill contracts and, in addition, to fulfill of legal obligations, to protect of vital interest and to enforce of legitimate interests. In case the Data Subject does not provide the personal data referred to in this paragraph, this may entirely or partially result in the blocking of contracting or the usage of the service. If the Data Subject does not give the consent to direct marketing purpose data controlling, this does not influence the conclusion of the contract or the provision of other services.

c) Copy of documents: The unit of the Bank responsible for the data management manage the copies made about documents proving personal data of Data Subjects having business relationship with the Bank in order to fulfill legal obligations. According to the data minimum principle a copy shall be made only from those documents which verify those personal data which are necessary for reaching that aim, for which the management of the personal data is necessary. In case the Data Subject does not provide the personal data referred to in this paragraph, this may entirely or partially result in the blocking of contracting.

d) Personal data prescribed by AML Act: The unit of the Bank responsible for the data management shall manage the personal data prescribed by AML Act in order to fulfill legal

obligations. In case the Data Subject does not provide the personal data referred to in this paragraph, this may result in the blocking of contracting or the execution of given transaction.

e) Personal data required for the conclusion of the contract of used services or which are intended to be used and making a decision on the contract: This includes, in particular, personal data regarding the Data Subject's creditworthiness. Should the Data Subject enter into a contract with the Bank the unit of the Bank responsible for the data management is entitled to check before entering into a contract – in line with the applicable rules of the contract – whether the agreement can be concluded with the Data Subject. If not the Data Subject is the contracting person the personal data of the Data Subject shall be managed in connection with the preparation of the contract and the decision on the contract after the entire consent was given. This contains especially the data regarding the credit worthiness of the Data Subject. The primary legal basis for handling these data is the performance of the contract. In case the Data Subject does not provide the personal data referred to in this paragraph, this may entirely or partially result in the blocking of contracting.

f) Personal data created in connection with using and rendering the services: The unit of the Bank responsible for the data management shall manage the personal data created in connection with the rendered service in compliance with the applicable provisions of the contract and legal regulations personal data concerning to accounts, claims, transactions, etc.). The primary legal basis for handling these data is the performance of the contract. If the purpose of the data management is product developing, Bank asks consent from the Data Subject.

g) Personal data concerning the rights and obligations created in connection with the usage and rendering of the relevant services: The Parties are entitled to exercise the rights and fulfil their obligations during the fulfilment of the contract. The unit of the Bank responsible for the Data Management is entitled the personal data concerning the above-mentioned (e.g interest claim, breach of contracts). The legal basis for handling these data is the performance of the contract.

h) Personal data concerning the claims arising from existing or terminated contracts and the claiming thereof: The unit of the Bank responsible for the data management shall manage those personal data which are connected to contracts which were already terminated, and which are arising upon the provisions of the law, furthermore, personal data relating to eventual exercising of these claims and personal data which shall be kept upon the provision of the law. The legal basis for handling these data is the fulfillment of legal obligations and the enforcement of legitimate interests.

i) Personal data created during contacting the Bank or its contact center: Those personal data fall under this which were created in the contact center and which are created during the contact between the Data Subject and the contact center. The management of the personal data in this case relates to the processes initiated by the Data Subject, to the contract and the fulfilment of the contract. The legal basis for handling these data is primary the performance of the contract.

j) The phone conversation and electronic communication between the Data Subject and the Bank: The unit of the Bank responsible for the data management shall record on its own server and shall manage the voice records happened between the Data Subject and the contact centre in line with the applicable law and the provisions signed with the Data Subjects and the electronic communication related to services linked to client orders (including those conversations and communications upon which no deal was concluded or no services related to client orders was rendered) The legal basis for handling these data is fulfillment of legal obligations, protection of vital interest and enforcement of legitimate interests.

k) Records of the voice and picture recorder operated by the Bank: The Bank operates voice and picture recorders in its rooms, ATM machines in its own operation, in the branches. The records are deemed as personal data and it is managed by the unit of the Bank responsible for the data management. The legal basis for handling these data is fulfillment of legal obligations, protection of vital interest and enforcement of legitimate interests.

l) Special data: data managed in order to ensure the fair access with the same conditions which data are managed by the Bank on the basis of the consent of the Data Subject.

VII. Transmission of Data

The Bank transmits data (1) to service provider carrying out outsourced activity to enable outsourcing the activities or to service provider whose activities are not classified as outsourced activities being essential to the Banking activities (2) by legal obligation or for the request of the authority.

Bank shall be entitled to determine the rights of the engaged (by Bank) data processor regarding the processing of personal data within the provisions of GDPR, Info tv. and other laws and regulations on data management. Bank shall be held liable for the legality of such instructions given by the engaged data processor. Bank - in full compliance with data protection provisions - shall be entitled to outsource and conclude an exclusive contract with a business company organizationally independent from Bank for the continuous or regular performance of its activities such as (i) activities connected to Bank's financial and auxiliary financial services, (ii) activities prescribed by law involving data management, data processing and storing, (iii) investment or auxiliary investment activities, or any activities or services not under Bszt. If data management is carried out by another person on behalf of the Bank then the Bank may only use data processors, who are providing adequate guarantees to comply with the GDPR requirements of data management and to execute appropriate technical and organizational measures protecting Data Subject's rights. Without the prior written adhoc or general consent of the Bank, the data processor may not uses any additional data processor.

Bank shall publish the list of entities performing outsourced activities as well as the list (along with the name of the data types transmitted) of other entities authorised to manage and/or process personal data transmissed by Bank in announcement at its branches open for public and on the website www.kdbbank.eu according to as set out in the General Business Terms of the Bank.

Bank shall be entitled to engage an agent for its financial and auxiliary financial, investment and auxiliary investment services. The list of agents engaged by Bank shall be found on the MNB website, here: http://felugyelet.mnb.hu/bal_menu/piaci_szereplok/kereso/kozvetitok/kozvetitok_keresese.html

The Bank is currently carrying out the following regular data transfers:

a) Bank shall retain the right of assigning its claims to Third party in accordance with the provisions of Civil Code. The entitled person will be changed after assignment. The acting employee of responsible unit of data management shall give the personal data of data subject to the entitled person after the assignment.
b) The acting employee of responsible unit of data management shall transfer the personal data of data subject to the financial enterprise (BISZ Zrt.) who operates Credit Information Registry (KHR) in accordance with KHR Act (Act 122 of 2011). KHR operating financial enterprise shall transfer personal data to third persons (reference data provider) in accordance with the law. The Business Rules, General Terms and Conditions of the Bank shall provide details of Disclosure by transmission.
c) If the Data Subject gives a mandate to the Bank under which transmission of personal data is necessary, the acting employee of responsible unit of data management may transfer the personal data.
d) Bank shall be entitled to disclose secrets and personal data of Data Subject, and facts pertaining to such data before any court with initiating a closed hearing, or before any authority acting within its competence, if the Bank shall prove in front of court or authority the fact, content, circumstances or appropriateness of provided or rejected service
e) Bank shall be entitled for the transmission of data - included transmission to the European Union or to a third country - considered Bank Secret and personal data to contracted employees, legal representatives, agents, persons, and entities hired for claim management services; persons, entities performing outsourced activities; organizations and its agents and representatives performing client and consumer satisfaction related researches, telephone

marketing and research of the Bank in all cases involved in performing the services of the Bank and obliged to keep Bank Secret.
The Data Subject shall contribute to the transmission of Personal Data to third countries at the date of contracting. To that extent, the Data Subject shall grant exemption from confidentiality to the Bank. Transmission of personal data shall be after concluding outsourcing, data processing contract in accordance with the relevant Hungarian legislation and EU legal acts.

f) In accordance with Section 36/A of Pft. from 2014.02.01. the data subject shall be entitled to withdraw money without transaction duty on the first 2 times in every month in a maximum HUF 150.000 (one hundred and fifty thousand HUF) amount, after it stated its declaration with a relevant content. Title XII/A of Pft. established a central registry in order to record the declarations of each account. The aim of central registry is to give the possibility to check, whether the data subject stated a declaration, or a withdrawal, or not. This registry also provides that it can be checked which declaration is valid, if the data subject gave declarations to different provider of declaration data at different times. The data of central registry shall only be used for these purposes. The central registry is operated by BISZ Zrt. (who operates KHR).

g) The Bank provide access to online payment initiation service providers and the account information service providers (herein collectively referred to as the **TPP**) pursuant to the PSD 2 in relation to the customer's personal data, classified as bank secret falling under the activity of TPP, at time points unpredictable and at the time point initiated by the Data Subject.
The provision of access to TPPs is based on statutory obligations. Access is provided by the Bank via an electronic platform (API) developed for this purpose. Nevertheless and in the absence of API, the TPP is able and entitled to enter into the Netbank of the Data Subject via the netbank login data provided by the Data Subject to the TPP and consequently to learn all personal data (even personal data that are not specifically relates to the scope of the TPP's activity) available there.

h) After July 1, 2019, data specified in 35/2017. (XII.14.) MNB regulation on payment transactions the Bank shall transfer to fulfill its legal obligations, the organization operating the central database in the processing, settlement and execution of payment service and processing of payment transactions and requests for initiation thereof, for the execution of the payment order and for the transmission of the request for payment payment service providers who are not considered financial institutions and financial institutions involved in the processing, accountancy and settlement of payment transactions, and which provide repetitive data on the dates initiated by the customer.

VIII. Persons entitled to data management, data processing

All employees of the Bank concerned with data processing and data processing and the entities performing outsourced activities and other entities authorised to manage and/or process personal data transmissed by Bank, all employees, agents, subcontractors of the entities involved in data management or data processing activities are entitled to get to know the personal data of the Data Subject.

IX. Period of data management and storage:

Bank shall cancel the different groups of data managed following the expiration of the periods set out herein as follows:

- For personal data of the client after the 6. (Sixth) year following the termination of the business relationship.
- For transaction data following the 8. (eighth) year after the transaction. In case of official requests of the MNB, authority acting as a financial information unit, investigation authority, public prosecutor's office, and the court in which cases Bank shall be obliged to store the transaction data for the period of time indicated in the official request, but not more than 10 (ten) years.

- For other data necessary for the risk-taking in connection with the clients after the 6. (sixth) year following the termination of the business relationship.
- For data of the rejected petitions (credit or account opening) and related documents until the end of the 5. (Fifth) year following the rejection.
- For the video recordings recorded for security purposes until the 60. (sixtieth) day, if not used for security purposes.
- Voice recordings during telephone complaint handling after the 5 (five) years following the recording. The complaint and the Bank's reply to it shall be stored for 5 (five) years by Bank.
- Voice recordings of telephone conversations necessary for the exercise and performance of rights and obligations until the end of the 6. (sixth) year following the termination of business relationship.
- Data provided in order to grating the same access to the Bank's services shall be kept for 20 (twenty) years.

X. Data Subject's rights related to data management:

Acceptance of an application for the exercise of the Rights of the Data Subject may be denied only if the Data Subject could not been identified. In the interests of the above, any person who receives the application, if applicable, is obliged to identify the person before any request for access to the Data Subject is received. In the event of an unsuccessful identification, the employee shall inform the Data Subject or the person acting as the Affiliate of the Data Subject or the person acting as Data Subject that his / her application can not be accepted due to unsuccessful identification and because of the protection of the relevant personal data.

In the case of a successful identification, the Data Subject is entitled to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object, and has right to data portability.
The request shall be performed without undue delay and in any event within one month of receipt of the request.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Bank may either:

(i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(ii) refuse to act on the request.

Right of access
The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the informations recorded in legal regulations. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Bank may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Right to rectification
The data subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(i) the purpose no longer exists;
(ii) the contribution has been withdrawn;
(iii) objects against data handling and there is no legitimate reason for data handling
(iv) to comply with a legal obligation it has to be canceled,
(v) personal data were collected in the context of the use of information society services.

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request. . If the obligation is too expensive or in the event of an obligation exceeding the available technology, to provide information is not necessary if duly documented reasons are available.

The above mentioned shall not apply to the extent that processing is necessary:

(i) for exercising the right of freedom of expression and information;
(ii) for compliance with a legal obligation
(iii) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, likely to render impossible or seriously impair the achievement of the objectives of that processing;
(iv) for the establishment, exercise or defense of legal claims.

That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data.

Right to restriction of processing

The data subject shall have the right to obtain from the Bank restriction of processing where one of the following applies:

(i) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(iii) the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(iv) the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing shall be informed by the Data manager before the restriction of processing is lifted.

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data

are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or 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 concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

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 a Bank, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(i) the processing is based on consent or on a contract and
(ii) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The right shall not adversely affect the rights and freedoms of others.

Before ensuring the data portability, special attention must be paid to the identification of the data subject and where the data subject requests to transfer the data.

Exercising of the data subject rights (e.g asking for information) is free if charge, if the person asking for information has not been submitted any request in the given year for the same data scope.

In other cases – including especially repeated exercise of data subject rights (e.g. asking for information), unfounded exercising of rights (e.g asking for information) or exceeding or repreated nature of exercising of data subject rights (e.g. asking for information) – the Bank is entitled for compensation, as precondition of exercising of data subjects rights which is set forth in the annex of the related General Terms and Condition of the Bank.

Exercising of data subject rights shall be deemed as *unfounded* if the Bank does not manage such data and the Related Person or the person who submitted the request shall (or should) be aware of, or such a data (e.g lists) are required for which the Bank is not obliged to prepare. Special requests (e.g. request for preparing of sending special registries, calculations) shall not be deemed as unfounded, if in the request the legal basis thereof is clearly and detailed way showed – especially detailed the legal basis of this obligation of the Bank and this obligation (preparing and sending the registries, lists and calculations etc.) of the Bank is clearly, unbias way determined in a legal norm.

Exercising of data subject rights under Articles 15-22 and 34 shall be deemed as *repeated* if the given personal data were affected by another request in the given year which wa ssubmitted for exercising of data subject rights – based upon Section 2 of Articles 12 of GDPR, including exercising of any data subjects right set forth in Articles 15-22 and 34 of GDPR.

Exercising of data subject rights shall be deemed as *exceeding* if (i) another request was submitted in connection with the personal data of the Related Person in the previous 6 (six) months before the submission date of the new request or (ii) the number of the requested personal data's type is more than

5 (five) (e.g. in case seeing, hearing or handing over any copy, this is related to the number of the documents) or the request is more than one page or can only be fulfilled only over more than one working hours e.g. in case of seeing or hearing.

In case of *mixed requests* the above shall be evaluated in their context and in the light of their complexity. If any request contains other request also (besides the data management request), so, - as those shall be read also by responding the data management response and shall be maneged also – these not data management related parts shall also be taken into view and shall be considered.

XI. Joint Data Management

The Bank informs its Data Subjects possessing bankcard issued by the Bank concluded a service contract with SIA Central Europe Zrt. (Cg.01-10-041848; seat: 1117 Budapest, Alíz utca 4.; hereinafter referred to a s the **SIA**) for the processing of the credit card transactions. Based on the service contract the SIA is the one blocking bank cards upon the request of the Data Subject. This is done by putting through the relevant customers' calls of the Data Subject to SIA and both the Bank and the SIA (independently from each other and for quality assurance purposes) capture and manage the discussion made through the telephone line. Bank informs the Data Subject that irrespective of the service contract that the Data Subject may exercise its rights, under the GDPR Regulation and the present Informant, against both the Bank or the SIA relating to both of them

XII. Automated decision making

Upon section 11 of the Act LIII of 2017 on Anti money laundering and prevention and hindrance of terrorism, the Bank informs the Data Subject opening an account with the Bank that the Bank is obliged to keep track of its business relations - including the analysis of transactions carried out during the existence of a business relationship - in order to determine whether the particular transaction is consistent with the Bank 's information available by law about the Data Subject Customer; In this respect the Bank must pay particular attention to all complex and unusual transactions and financial transactions. The Bank complies with its above mentioned statutory obligation by the continuous monitoring of the accounts of the Data Subjects opened with the Bank and the performed transactions thereon.

XIII. Data protection Officer

The Bank hereby inform the Data Subjects that there is a data protection officer in operation at the Bank's organization. The contact details of the data protection officer are the followings:

Dr. Nádasi-Szabó Tamás (address: 1054 Budapest, Bajcsy-Zsilinszky út 42-46.; phone: 374 - 9947; e-mail: adatvedelem@kdbbank.eu)

XIV. Right to turn to the Authority

The Data Subject is entitled to turn to the Authority with his/her complaint on the following contacts:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Post address: 1530 Budapest, Pf.: 5.
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL: http://naih.hu

Budapest, 2017.05.22.

KDB Bank Europe Ltd.