K&H PÉNZFORGALMI SZOLGÁLTATÓ KFT's

DATA PROCESSING POLICY DOCUMENT

Effective as of September 1, 2020

contents

I. GENERAL INFORMATION

K&H Pénzforgalmi Szolgáltató Kft. (re.g.istered office: 1095 Budapest, Lechner Ödön fasor 9; company registration number: 01-09-338123) (hereinafter: the "Company") processes information in relation to its customers, its customers' contacts, the recipients of its marketing messages, the visitors to its facilities and other data subjects („data subject(s)") qualifying as „personal information" under section 1 of article 4 of EU 2016/679 General Data Protection Regulation (GDPR). This Data Protection Policy Document (hereinafter referred to as the "Policy Document") provides information on the processing of these personal data and on the data subjects' rights and legal remedies in relation to data processing.

Contact details of the Company:

Registered seat and mailing address: 1095 Budapest, Lechner Ödön fasor 9.
Company registration number: Cg. 01-09-338123, registered by the Company Court of the Metropolitan Court of Budapest
Telephone number: +36 1/20/30/70 335 3355
E-mail address: khpos@kh.hu
Website: https://www.khpos.hu
Name and contact details of its Data Protection Officer: Dr László Gábor Kürthy, dataprotection_khpos@kh.hu

UPDATING AND ACCESSING THE POLICY DOCUMENT

The Company reserves the right to amend this Policy Document unilaterally with effect from the date of the amendment, subject to the restrictions set out in the applicable legislation and, if necessary, by informing the parties concerned in good time in advance. In particular, this Policy Document may be amended if required by changes in legislation, data protection authority practices, business or employee needs, or newly discovered security risks.

INFORMATION OF DATA SUBJECTS

Prior to the commencement of data processing, the Company informs data subjects whether data processing is based on consent or is obligatory. Prior to the commencement of data processing, the Company shall provide clear and detailed information on all facts related to data processing, in particular its purpose and legal basis, the person authorized to process and control the data, the duration of data processing, and on who has access to the data and which data processing rights and remedies are available to data subjects. If the purpose of consent-based data processing is to perform a written contract concluded by the Company, the Contract shall contain all information that data subjects must be aware of in terms of the processing of personal data, thus, in particular, the definition of the data to be processed, the duration of data processing, the purpose of their use, the fact of the transmission of the data, the recipients, the fact that a data controller is used. The Contract shall unambiguously state

that by signing the Contract, data subjects consent to the processing of their data as specified in the Contract.

II. LEGISLATIVE BACKGROUND

In particular, the Company's data processing is governed by the provisions of the following legislation:

- EU 2016/679. General Data Protection Regulation („GDPR")
- Act CXII of 2011 on the Right to Information Self-determination and Freedom of Information (hereinafter: Infotv.)
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter: Hpt.)
- Act CCXXXV of 2013 on Individual Payment Service Providers. (hereinafter: Fsztv.)
- Act LIII of 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing. Act (hereinafter: Pmt.)
- Act CXXXIII of 2005 on the Rules for the Protection of Persons and Property and for Investigation by Private Investigators
- Act V of 2013 on the Civil Code
- Act C of 2003 on Electronic Communication (hereinafter: Eht.)
- Act CVIII of 2001 on Certain Aspects of Electronic Commercial Services and Information Society Services (hereinafter: Eker.tv.)
- Act C of 2000 on Accounting,
- Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activity. Act (hereinafter: Grt.)
- Act CXIX of 1995 on the Management of Name and Address Data for the Purpose of Research and Direct Business Acquisition (hereinafter: DM tv.)
- MNB Decree 19/2017. (VII. 19.) on the Detailed Rules concerning the Minimum Requirements for the Development and Operation of a Screening System applied in the course of the Implementation of the Act on the Prevention and Suppression of Money Laundering and Terrorism Financing vis-a-vis the Service Providers under the MNB's Supervision and the Financial and Property Restriction Measures Introduced by the European Union and the UN Security Council.

III. DATA PROTECTION TERMS

Customer: the Data Subject who uses a payment service by the Company.

Payment secret: any fact, information, solution or data available to the payment institution or electronic money institution about each customer, relating to the customer's person, data, financial position, business activities, management, ownership, business relations, as well as the balance and turnover of their account with the payment institution, electronic money institution, and their contracts with the payment institution and electronic money institution.

The rules on payment secrecy shall also apply to a person who contacts a payment institution to use a service but does not use the service.

Data subject: any natural person identified or - directly or indirectly - identifiable based on personal data.

Personal data: any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular on the basis of an identifier such as name, number, location, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data; the data controller or the special aspects of the appointment of the data processor may also be determined by law.

Data processing: any operation or set of operations on personal data or files, whether automated or non-automated.

Data processor: the natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the data controller.

Third person: the natural or legal person, public authority, agency or any other body which is not the data subject, the data controller, the data processor or the persons who have been authorized to process personal data under the direct control of the data controller or the data processor.

Third country: any State that is not a member of the European Economic Area (EEA).

Data protection incident: a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored, or otherwise processed.

Health data: personal data concerning the physical or mental state of health of a natural person, including data relating to health services provided to a natural person which contain information on the state of health of the natural person.

IV. CATEGORIES OF PERSONAL DATA PROCESSED BY THE COMPANY

The Company defines the categories of personal data in which it processes detailed personal data (data types) within the data processing purpose categories, assigned to each data processing:

Basic data: data and information obtained from the data subject in an identification procedure set forth by legislation or from administrative records (e.g. full name, sex, permanent address, nationality, place and date of birth), (ii) other official personal identification data (identity card number, business identity number, social security number, driving license number, passport number), (iii) photo ID.

Contractual customer data for the use of a product or service (i) customer product requests / orders (including unsuccessful ones), (ii) sales-related data, including pricing, individual pricing, pricing history, commissions, (iii) contractual data, product and service parameters (e.g. limits) and information on changes to the product / service contract or parameters, historical data of the product, details of product parameters, iv) authorization, signing authority, authentication, signing and service use authorization.

Product / service usage data: (i) transactions (between customer and third party), (ii) other usage event data (e.g. balance checks, transaction listings)

Contact information: contact details of the data subject (email address, telephone number)

Sensitive customer data: closed-circuit camera system (head office video recording), audio recording, cookies and similar techniques or Internet protocols, interaction on or from the Company's Internet interfaces (IP address, browsing habits).

Data related to bank card acceptance activity: (i) in case of payment via physical terminal, the bank card number, validity period, (ii) in case of internet card payment in addition to those listed in (i), additional data requested but not directly necessary for the performance of the transaction (issuer bank, card type, cardholder's name, card control number (CVV / CVC)) (iii) in case of a telephone/mail order (MOTO) other data (product data, product delivery data) not directly necessary for the Company to perform the transaction

V. CERTAIN DATA PROCESSING OPERATIONS BY DATA PROCESSING PURPOSE CATEGORIES

Based on its business operations, the Company defines the categories of data processing objectives and the essential characteristics of the data processing activities (sub-objectives) assigned to these categories as described below. The recipients of the data transfer are presented in a separate chapter.
The Company expressly draws the attention of data subjects to the fact that if the processing of personal data is based on the data subject's consent, the data subject has the right to object to the processing of personal data relating to the data subject at any time. If the data subject objects to the processing of his or her personal data, the Company will not process the personal data for the purpose to which the consent relates.

1. Customer identification and authentication:

Collection, registration, management, updating and disclosure of data of potential and existing customers and individuals related to the customer through the Company's channels for the following purposes: (i) customer identification, (ii) customer authentication, and (iii) central management of customer identification and contact information. Customer administration includes both centralized customer management in a central customer database (customer portfolio) and decentralized customer management, such as e.g.. contact information managed by the Company's employees in their contact lists.

2. **Customer convenience services (online):**

The management and disclosure of basic customer information relating to an identical situation to facilitate subsequent customer administration and enhance customer experience. The data is used by the Company on the initiative of the customer only. (Example 1: Customer's website preferences. If the customer chooses English, the English website will open. Customers give their consent by accepting the cookies).

3. **Preparation of contracts on data subjects' request:**

During the pre-sale steps prior to the signing of the contract, the Company will only use personal data if the data subject makes an offer. Data collection and processing is limited to what is necessary for the offer. After signing the contract, the Company stores personal data to execute the contract. In the event of non-conclusion of the contract, the retention period of the data will be determined in accordance with the purpose given.

4. **External marketing:**

In external marketing, the Company initiates contact with existing and / or potential customers through email, electronic channels, texting, or telephone calls providing commercial information and business offer. External marketing includes: (i) preparing and sending business advice and product / service offers to existing and potential customers, (ii) compiling and sending general information to existing and potential customers, without mentioning a specific banking product, (iii) creating and sending newsletters.

5. **External service messages:**

Use of personal data when delivering service messages to the customer (phone call, email, text message, letter, etc.) A service message is one that relates to services and products only that the customer already has but are not explicitly included in the contract concluded with the customer. Service messages are not of a marketing nature and do not contain a business offer.

6. **Product/service use:**

The recording, managing, updating and disclosure of personal information through the Company's channels for the purpose of using the product and / or service, to the extent necessary to perform the contract or provide the agreed service only.

7. **Mandatory risk assessment profiling to prevent money laundering:**

The Company prepares the customer's profile based on legal regulations in order to prevent money laundering (acceptance and monitoring of customers and transactions on the basis of risk).

8. **Risk assessment profiling to prevent fraud:**

The Company prepares the customer profile for the purpose of fraud prevention, detection and investigation using profile indicators and other information (e.g.. stolen identity card) that may materially indicate the possibility of fraud. It does not cover the detection of fraud and the subsequent investigation of potential fraud, but only the compilation of a profile that facilitates these activities. In this context, the Company also considers compliance, internal control, and physical and digital security.

9. **Control and prevention (money laundering, fraud, embargoes, terrorism):**

In this context, the Company processes personal data and the information extracted from them for the implementation of control, prevention, detection and investigation measures required by law, as well as for the provision of data and reports to the Financial Intelligence Unit (FIU) and authorities, as well as for discharging other obligations related to procedures concerning money laundering, embargoes and terrorism. i) Fraud and / or Unethical Behaviour: During its activities, the Company may use the profile data generated by the fraud prevention profiling process. The process controls and prevents fraud committed or attempted by Company employees, existing customers, potential customers and any other persons who intend to defraud the Company or its customers, including the whistleblowing process and the additional checks carried out as part of the normal licensing process. ii) Physical and digital security: in this context, the Company inspects and investigates intrusions, attacks against the Company and leaks (data leaks) that may cause harm to the Company, the Company's employees, or customers.

10. **Exercise and protection of the Company's rights:**

Data processing takes place during the definition, exercise, and protection of the Company's rights, including court and regulatory proceedings and the use of an outside counsel.

11. **Software modification testing, demos, training:**

The Company uses and processes personal data from a live (operational) environment to test software code changes, resolve incidents or reproduce them, and to train Company employees and users to achieve the most accurate results possible.

12. Complaint handling:

The Company manages personal data to register complaints and respond to them.

VI. DATA TRANSFER AND DATA TRANSMISSION

1. Data transfer and data transmission conditions

Personal data will be transferred by the Company if the data subject has consented to it or if it is permitted by law. The Company is entitled, by authorization of the data subject or by law, to transfer the data recorded in connection with the data subject's contracts for the purposes of risk management, statistical analysis, control and the recording of court proceedings to Československá obchodní banka, a.s. (Radlická 333/150 15057 Prague 5, CZECH REPUBLIC) having qualified influence in the Company. The transfer of data to an EEA state shall be considered as if the transfer took place within the territory of Hungary, in accordance with the applicable data protection legislation.

The Company transfers personal data to a non-EEA state (third country) only if the data subject has expressly consented to this, or the conditions for data processing required by law are met and an adequate level of protection of personal data is ensured in the third country.

Data may also be transferred to a third person without the consent of the data subject conferred by law (e.g. in the cases specified in Sections 60-64 of the Fsztv and in Act CXXII of 2011 on the Central Credit Information System).

2. Data processing

The rights and obligations of the data processor appointed by the Company in relation to the processing of personal data are determined by the Company within the framework of the law on data processing. The Company is responsible for the legality of the instructions given by it. During his or her activities the data processor may use an additional data processor in accordance with the Company's instructions. The data processor may not make a substantive decision concerning data processing, may process personal data obtained in accordance with the provisions of the Company only, may not process data for its own purposes, and must store and retain personal data in accordance with the provisions of the Company. The contract for data processing shall be entered into by the Company in writing. The Company shall not entrust data processing to an organization that has an interest in the Company's business activities.

3. Outsourcing

Pursuant to article 14 of Fsztv., the Company – while complying with the data protection regulations - may outsource any element of its activities, i.e. it may entrust the engagement in such activities to another organization.

The transfer of data necessary for the engagement in the outsourced activity by the Company to the outsourcee does not constitute a breach of insurance secrecy. An outsourcee may only use the services of a contributor with the prior written approval of the Company.

The Company ensures that these organizations ensure the secure handling of the data subject's data in accordance with the conditions specified in the legislation on data protection and insurance secrecy.

4. Persons authorised to process data (data processors)

The Company uses the services of the following data processors. The rights and obligations of the data processor related to the processing of personal data are defined by the Company as data controller within the framework of the GDPR and the specific laws on data processing. The Company uses the services of the following data processors. The Company, as data controller, is responsible for the legality of the instructions given by it. Data processors are not entitled to make substantive decisions concerning data processing, may only use the personal data they come into the knowledge of according to the Company's instructions acting as data controller, they may not process data for their own purposes, and must store and preserve the personal data according to the instructions of the Company as data controller.

Data processor	Personal information it can access
name: XEROX Magyarország Kft. registered seat: 1037 Budapest, Szépvölgyi út 35-37	Prints and packs statements, invoice notification letters and other forms, and forwards the packed account statements to Magyar Posta.
name: K&H Csoportszolgáltató Központ Kft. registered seat: 1095 Budapest, Lechner Ödön fasor 9.	Carries out the dispatch activities of the Company (receipt, processing, delivery to the destination, provision of internal documents, etc.).
name: SIA S.p.A. registered seat: Italy, Via Gonin 36, I20147 Milan	Responsible for the card clearing and ancillary activities of the Company and its acquirers.

VII. DATA SECURITY MEASURES APPLIED BY THE COMPANY

1. IT support for the management of data protection incidents and data protection records

In this context the Company carries out regular self-audits, during which it checks whether the operation of its IT system and the applicable corporate regulations comply with legal requirements. In addition to the compliance review, the Company also tests technology resilience as part of the self-audit (IT security review). The Company regularly analyses the records of data processed and stored in IT systems (IT security inventory) and the IT security risks that threaten them.

2. Identification systems

The Company identifies users accessing its systems and monitors access rights. The Company uses a central directory system and electronic signatures (for identification, signing, encryption) in order to verify user rights, the Company also provides distributed authorization management (different persons are authorized to set the rights related to each system / system group), password management (prescribing and enforcing minimal password complexity and password changes) and uses multi-factor authentication (using multiple authentication components, not just the username and password).

3. **Protection against malicious programs**

The Company operates a multi-level, multi-technology, and multi-vendor heterogeneous protection system against common malicious programs (bots, malware, spyware, etc.) on client and server computers, network devices, and content filters.

4. Security incident management

The Company collects and stores technical logs of systems and applications for the purpose of reconstructing and possibly investigating data security, data protection or IT

security incidents. To avoid and reduce data protection damages, the Company contacts the persons concerned in the event of security incidents and cooperates with external bodies and service providers in the monitoring and management of security incidents.

5. User support and education

If necessary, the Company informs its employees about possible hazards with targeted warnings, as well as develops and maintains the IT and data security preparedness of employees through specialized training and education programs and, if necessary, targeted awareness campaigns.

6. Network security

The Company separates processing systems and the company's internal network from public networks and protects them from unauthorized access. When network connections are established, it identifies the connected endpoint devices so that computers with enabled status can communicate on its network only. It also ensures the confidentiality of data and messages transmitted and handled during network communication through secure identification and encryption.

7. Data management of external partners

The Company provides information on data management with external partners, regulates communication and information flow with IT service providers, and enters into confidentiality agreements with all service providers and partners.

8. Vulnerability management

The Company regularly assesses, analyses, and evaluates IT security vulnerabilities and takes the necessary actions based on this. The Company regularly installs security updates on company computers and devices and scans the security of its services to customers.

9. Content filtering

The Company uses technological and administrative measures to identify and filter e-mails and traffic containing spam, phishing, and malware. As part of this, it monitors network access and browsing activities on its network, analysing system access and network traffic to detect and manage attacks that threaten clients and services.

10. Protection of storage media

The Company maintains a record of the storage media used and ensures their safe handling through technological and administrative measures.

11. Physical protection of records and data

With regard to the physical protection of electronic and paper-based documents, the Company has lockable server rooms and up-to-date records management regulations

which provide for the secure storage of paper documents in accordance with an appropriate security protocol and their exclusive access by duly authorized persons.

VIII. DATA PROTECTION RIGHTS AND REMEDIES FOR STAKEHOLDERS

1. Privacy rights and remedies

The data protection rights and remedies of data subjects are detailed in the relevant provisions of the GDPR (in particular Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80 and 82). The following summary contains the most important provisions, and the Company accordingly provides information to the data subjects about their rights related to data processing and their legal remedies.

The Company shall, without undue delay, but in any case within one month of receipt of a request to exercise the right in question (see Articles 15-22 of the GDPR), inform the data subject of the action taken in response to his or her request. If necessary, considering the complexity of the application and the number of applications, this time limit may be extended by a further two months. The Company shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month from the receipt of the request. If the data subject has submitted the request by electronic means, the information shall, as far as possible, be provided by electronic means, unless the data subject requests otherwise.

If the Company does not take action on the data subject's request, it shall inform the data subject of the reasons for the non-action without delay, but not later than within one month from the receipt of the request, so that the person concerned may lodge a complaint with a supervisory authority and may exercise his or her right to a judicial remedy.

The Company shall provide the information requested by the data subject in writing or, in the case of an application submitted electronically, electronically. Oral information may also be given to the data subject if the data subject proves his / her identity to the Company.

2. The data subject’s right of access

(1) The data subject has the right to receive feedback from the Company as to whether the processing of his / her personal data is in progress. If such processing is in progress, the data subject shall have the right to access the personal data and the following information:

a) the purpose of data processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients, to whom personal data have been or will be communicated by the Company, including particularly recipients in third countries or international organizations;

d) where applicable, the intended period for which the personal data will be stored or, if that is not possible, the criteria for determining that period;
e) the right of the data subject to request the Company to rectify, delete or restrict the processing of personal data concerning him or her and to object to the processing of such personal data;
f) the right to lodge a complaint with a supervisory authority; and
g) if the data were not collected from the data subject, all available information on their source;
h) the fact of automated decision-making (Article 22 (1) and (4) GDPR), including profiling, and, at least in these cases, comprehensible information on the logic used and the significance of such processing and the expected consequences for the data subject.

(2) Where personal data are transmitted to a third country, the data subject shall be entitled to be informed of the appropriate guarantees regarding the transmission.

(3) The Company shall make a copy of the personal data subject to data processing available to the data subject. The Company may charge a reasonable fee based on administrative costs for additional copies requested by the data subject. If the data subject has submitted the request electronically, the information shall be provided in a widely used electronic format, unless the data subject requests otherwise.

3. Right to rectification

The data subject has the right to have the Company rectify inaccurate personal data concerning him / her at his/her request without undue delay. The data subject is also entitled to request that the incomplete personal data be supplemented, inter alia, by means of a supplementary statement.

4. Right of cancellation ("right to forget")

(1) The data subject shall have the right to have the Company delete personal data concerning him or her without undue delay if one of the following reasons exists:
a) the personal data are no longer required for the purpose for which they were collected or otherwise processed by the BANK;
b) the data subject withdraws his or her consent on which the data processing is based and there is no other legal basis for the data processing;
c) the data subject objects to the processing and, where applicable, there is no overriding legitimate reason for the processing;
d) the personal data have been processed unlawfully;
e) the personal data must be deleted to fulfil a legal obligation under Union or Member State law applicable to the Company;
f) the personal data have been collected in connection with the provision of information society services.

(2) If the Company has disclosed the personal data and is obliged to delete them in accordance with the above, it shall take the reasonably expected steps with a view to the available technology and the costs of implementation- including technical measures – required to inform the controllers processing the relevant data that the data subject has requested the deletion of the links to the personal data in question or of the copy or duplicate of those personal data.

(3) Paragraphs 1 and 2 shall not apply where processing is necessary, inter alia:
   a) for the purpose of exercising the right to freedom of expression and information;
   b) for the purpose of complying with an obligation under Union or Member State law applicable to the Company which requires the processing of personal data;
   c) for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes, in so far as: the right referred to in paragraph 1 is likely to make such processing impossible or seriously jeopardize it; or
   d) to submit, assert or defend legal claims.

5. Right to restrict data processing

(1) The data subject has the right to have the Company restrict the processing of his or her data if any of the following is met:
   a) the data subject disputes the accuracy of the personal data, in which case the restriction shall apply to the period that allows the Company to verify the accuracy of the personal data;
   b) the processing is unlawful, and the data subject opposes the erasure of the data and instead requests that their use be restricted;
   c) The Company no longer needs the personal data for the purpose of data processing, but the data subject needs them to submit, enforce or protect legal claims; or
   d) the data subject has objected to the processing; in this case, the restriction applies to the period until it is determined whether the legitimate reasons of the Company take precedence over the legitimate reasons of the data subject.

(2) Where the processing is restricted pursuant to paragraph (1), the processing of such personal data, with the exception of storage, shall be subject to the consent of the data subject or to the submission, enforcement or protection of legal claims or the protection of the rights of other natural or legal persons, or in the overriding public interest of a Member State.

(3) The Company shall inform the data subject at whose request the data processing has been restricted based on the above of the lifting of the restriction of data processing in advance.

6. Obligation to notify in connection with the rectification or erasure of personal data or restrictions on data processing

The Company shall inform all recipients to whom or to which the personal data have been communicated of any rectification, erasure, or restriction of data processing, unless this proves impossible or requires a disproportionate effort. Upon request, the Company shall inform the data subject of these recipients.

7. The right to data portability

(1) The data subject shall have the right to receive personal data relating to him or her made available to the Company in a structured, widely used, machine-readable format and to transfer such data to another controller without the Company preventing him or her from doing so, if:
   a) data processing is based on consent or contract; and
   b) data processing is automated.

(2) In exercising the right to data portability pursuant to paragraph (1), the data subject shall have the right, if technically feasible, to request the direct transfer of personal data between data controllers (such as the Company and other data controllers)

(3) The exercise of the right described above shall be without prejudice to the provisions relating to the right of cancellation ("right to forget") and shall not adversely affect the rights and freedoms of others.

8. Right to protest

(1) The data subject shall have the right to object at any time to the processing of his or her personal data, including profiling, on grounds relating to his or her situation. In this case, personal data shall not be further processed by the Company unless it proves that the processing is justified by overriding legitimate reasons which take precedence over the interests, rights and freedoms of the data subject or which are related to the submission, enforcement or protection of legal claims.

(2) If the processing of personal data is for the purpose of direct business acquisition, the data subject shall have the right to object at any time to the processing of personal data relating to him or her for that purpose, including profiling, in so far as it relates to direct business acquisition.

(3) If the data subject objects to the processing of personal data for the direct acquisition of business, the personal data may no longer be processed for that purpose.

(4) In connection with the use of information society services and by way of derogation from Directive 2002/58 / EC, the data subject may also exercise the right to object by automated means based on technical specifications.

(5) If personal data are processed for scientific and historical research or statistical purposes, the data subject shall have the right to object to the processing of personal data relating to him or her on grounds relating to his or her own situation, unless the processing is necessary for the performance of a task carried out in the public interest.

9. Right to complain to a supervisory authority

The data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State in which he or she has his or her habitual residence, place of work or where the suspected infringement has taken place, if the data subject considers that the processing of personal data infringes GDPR.

In Hungary, the competent supervisory authority is the Nemzeti Adatvédelmi és Információszabadság Hatóság (webpage: http://naih.hu/; address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c; mailing address: 1530 Budapest, Pf.: 5.; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu).

10. The right to an effective judicial remedy against a supervisory authority

(1) The data subject shall have the right to an effective judicial remedy against a legally binding decision of the supervisory authority on the data subject.

(2) The data subject shall have the right to an effective judicial remedy 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 or the outcome of the complaint.

(3) Proceedings against the supervisory authority shall be brought before a court of the Member State in which the supervisory authority has its seat.

11. **The right to an effective judicial remedy against the Company or the data processor**

(1) Without prejudice to any administrative or non-judicial remedies available, including the right to complain to the supervisory authority, the data subject shall have an effective judicial remedy if he or she considers that his or her rights under the GDPR have been breached by a processing of his or her personal data in violation of the GDPR.

(2) Proceedings against the Company or the processor shall be brought before a court of the Member State in which the Company or the processor is established. Such

proceedings may also be brought before a court of the Member State in which the data subject has his habitual residence.

IX. DATA PROTECTION CHARACTERISTICS ARISING FROM THE OPERATION OF THE COMPANY

1. Data management related to advertising activities

Pursuant to Section 6 (1) of the Grt., advertising for the purpose of direct business acquisition by direct contact with a natural person as the recipient of an advertisement (thus in particular by electronic mail or other equivalent means of individual communication, with the exception of addressed postal advertising) may be communicated only with the prior and express consent of the recipient of the advertisement. The Company keeps a register of the personal data of the persons making such consent statements, considering the provisions of the consent statement and the related legal regulations (Grt., DM Act, Eht., etc.). The data contained in this register concerning the recipient of the advertisement may only be processed in accordance with the statement of consent, until it is revoked, and may only be passed on to third parties with the prior consent of the data subject concerned or as required by law. The data subject may therefore authorize the Company and consent to the Company informing the data subject about its own services by direct mail or other means of communication (telephone, e-mail, e-bank, text message, etc.) for marketing purposes and to the Company processing the data subject's data for this purpose. The data subject has the right to initiate at any time with the Company, without restriction or justification, that the Company should not send to him or her advertising material for direct business acquisition purposes, the data Subject may at any time withdraw his or her consent to receive advertisements and have his or her data processed for this purpose free of charge. The data subject may declare his / her request in this direction through the contact details published on the Company's website and in other ways indicated in the mails. In this case, the Company will no longer contact the Data Subject for advertising purposes.

2. Photo- and video recordings

At its registered office, the Company uses surveillance by an electronic property protection system in accordance with the Act on the Protection of Personal and Property and the Rules of Private Investigation, and may take photographs and videos with the help of the electronic property protection system. The purpose of monitoring and recording is to ensure the uninterrupted operation of financial and ancillary financial services, to protect human life, physical integrity, personal liberty, to protect property, and to protect payment and trade secrets. The Company shall keep the recordings made for the above security purposes for 60 (sixty) days when not in use. It is considered a use if the recorded recording is used as evidence in court or other official proceedings. The image recording system is operated by the data processor used by the Company for this purpose and the recordings are stored in the data processor’s systems until the deletion takes place. The recordings will be disclosed only if they are indispensable for the

prevention or interruption of an offense related to the above purposes, or if they have to be forwarded by the Company at the request of a court or other authority for use in court or other official proceedings. The recordings will not be made available by the Company to the data subjects, however, they will be made available for viewing at the Company's premises within the retention period, respecting the personal rights of other data subjects and taking into account the protection of the Company's business secrets. Data subjects may request that the recordings be blocked during the retention period. In this case, the Company shall not destroy the recording for 30 (thirty) days from the request for blocking and for maximum 60 (sixty) days from the making of the recording. The Company shall display signs indicating that photography and video recording is taking place at its registered office.

Complaint handling, audio-recording

The Company provides an opportunity for its customers to communicate a complaint about the Company's conduct, activities or omissions orally (in person, by telephone) or in writing (by a document handed over in person or by other means, by post, fax, e-mail). The Company receives oral complaints from its customers in person at its registered office, during opening hours, as well as by telephone and telephone customer service. In the case of telephone complaint handling, the Company records the telephone communication between it and the customer with a voice recording and keeps the voice recording for 5 (five) years. At the request of the Client, the Company - in accordance with the sectoral legislation - ensures the replay of the voice recording, and provides a copy of the voice recording or a certified record of the voice recording within 25 (twenty-five) days free of charge. The Company shall keep the complaint and the response thereto for 5 (five) years to fulfil a legal obligation (provision of a register and a copy) and shall present it at the request of the Magyar Nemzeti Bank. The handling of the voice recording, as well as the complaint and the response thereto, are necessary to fulfil the legal obligation of the Company, the purpose of which is to ensure compliance with the law. More information on the Company's complaint handling is available on the following website: https://www.khpos.hu/panaszkezeles

3. Audio recordings

The Company shall record the telephone communication between it and the customer through the following channels with the consent of the data subject following prior information. The recordings are managed by the Company for the purposes explained below, which can be summarized in the following target groups:

- Fulfilment of a legal obligation (retention and access related to complaint handling, record keeping related to investment services, retention related to identification obligation, accounting retention obligation);
- Protection of legal claims (submission, enforcement, protection of legal claims);
- Internal corporate governance objectives (quality control, process optimization, abuse and fraud prevention, control).

The Company's telephone communication channels are as follows:

TeleCenter contact information

The Company receives the oral complaints and other reports of its customers at the telephone customer service and provides them with general and personalized information upon request.

At the beginning of the administration, the Company informs its customers about the recording of their telephone communication. For customers who do not wish to consent to voice recording, any other contact information of the Company is open for contact. The processing of telephone communication is obligatory for the Company in the case of a call for complaint handling, the legal basis is the fulfilment of a legal obligation, in the case of a call for another subject the audio recording is based on the consent of the person concerned. The Company processes the telephone conversation about complaint handling to fulfil the legal obligation about complaint handling, and keeps the voice recording for 5 (five) years from the recording. Telephone conversations with general and personalized information are stored and handled by the Company for 5 (five) years from the date of recording to protect legal claims.

Telephone contacts for Merchant Fraud Management staff

The above area of the Company also receives inquiries from prospective credit card accepting customers by telephone regarding the conclusion of a contract, as well as notifications from contracted credit card accepting customers, especially those related to the prevention of abuse, and accepts take-back requests. At the beginning of the administration, the Company informs its customers about the recording of their telephone communication. For customers who do not wish to consent to voice recording, any other contact information of the Company is open for contact. The processing of the voice recording is based on the consent of the data subject, the legal basis is the consent of the data subject. The Company processes the telephone conversation for the purpose of fulfilling the contract and protecting legal claims, and keeps the voice recording for 5 (five) years from the recording.

In addition to the purposes set out above, the Company may use the recordings for internal corporate governance purposes (e.g., quality control, process optimization, abuse and fraud prevention, control) during their retention period.

At the request or information request of the data subject who contacts the Company or is visited by the Company, the Company shall provide a copy of the voice recording to the data subject during the data processing.

The recordings are managed by the Company in a closed manner, only the Company's employees involved in the given service provision process, in the case of quality control, fraud prevention or internal control investigations, the staff who carry them out, and in the case of data processing for the purpose of filing, enforcing and protecting legal claims, the persons providing legal representation may have access to them. The recordings may be used in court or other official proceedings, either on the initiative of the Company or at the request of the acting authority, during which the recordings may become known

to the persons conducting the official proceedings to the extent necessary. If the recordings are not used, the recorded conversations will be deleted after the retention period.

4. Data management on the Company's websites

The Company occasionally uses technology on its websites accessible to anyone on the Internet, in the course of which - in order to enhance the user experience - it stores settings for image and sound display, settings to support the use of various services, etc. on the computer of the visitor of the site (cookies) in a way that can be changed or deleted by the user at any time.

Detailed cookie information is available on the website “cookie szabályzat” (cookie policy).