K&H PÉNZFORGALMI SZOLGÁLTATÓ KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

PRIVACY STATEMENT

Effective as of September 15, 2023

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 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.

II. LEGISLATIVE BACKGROUND

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

- Regulation (EU) 2016/679 of The European Parlaiment and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Act CXII of 2011 on the Right to Information Self-determination and Freedom of Information (hereinafter: Infotv.);
- 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. LEGAL BASIS FOR DATA PROCESSING

Legal compliance

Data processing is necessary to comply with a legal obligation applicable to the Company, such as the obligation to keep records pursuant to Section 169 of Act C of 2000 or the obligation to keep personal data obtained by the Company in the course of customer due diligence measures pursuant to Section 56 of Act LIII of 2017.

Consent of the data subject

Consent to the processing is a voluntary, specific, informed and unambiguous indication of the data subject's wishes, by which he or she unambiguously signifies his or her agreement to the processing of personal data concerning him or her. The Company explicitly draws the attention of the data subject to the fact that, where the processing of personal data is based on the data subject's consent, the data subject has the right to withdraw his or her consent at any time. If the data subject withdraws his or her consent, the Company will no longer process the personal data for the purposes for which the consent was given. The withdrawal of consent shall not affect the lawfulness of the processing based on consent prior to its withdrawal.

Legitimate interest

A legitimate, actual and existing interest on the part of the Company, which is based on the lawfulness of the processing, expressed in a lawful and valid manner and capable of being weighed against the interests of the Company.

Performance of the contract

Where the processing is necessary for the performance of a contract to which the data subject is a party and the Company is a party, or where the processing of personal data is necessary for the purposes of taking steps at the request of the data subject prior to entering into a contract, the legal basis for the processing by the Company is the processing necessary for the performance of the contract.

V. DATA PROCESSINGS PERFORMED BY THE COMPANY

1. **Merchant interest:**

The online interface on the Company's website (https://www.khpos.hu/kereskedoi-erdeklodes) allows interested natural and legal persons (hereinafter referred to as "Interested Party") to contact the Company. Upon completion and submission of the merchant registration form, the Company's sales representatives will contact the Interested Party to present our business offer. The Company will process the personal and non-personal data provided during the pre-registration process in the case of a merchant enquiry in compliance with the applicable legislation, as set out in this Privacy Notice.

The purpose of the data processing: to identify potential customers and/or their contact persons who have initiated contact on the Company's website and to prepare a contractual offer for them.

Legal basis for data processing: the consent of the natural person of the Interested Party or of a contact person acting on behalf of the Interested Party's legal entity, which may be withdrawn at any time without giving reasons.

The scope of personal data processed: the name, mobile phone number and e-mail address of the potential customer and/or contact person, as well as any personal data that the data subject and/or contact person discloses to the Company in connection with the callback request.

Duration of data processing: until consent is withdrawn or 30 days after contacting the data subject.

Indtermediate data processor: ShiwaForce.com Zrt.

2. Customer due diligence measures:

Legally mandated client identification, risk classification and beneficial ownership; identification of persons authorised to dispose of or represent the client and of the authorised representatives.

Purpose of the data processing: to carry out customer due diligence measures pursuant to Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ("AML/CFT Act").

Legal basis for processing: performance of a legal obligation

Scope of personal data processed: name, name at birth, place of birth, date of birth, mother's maiden name, nationality, permanent address, identification document details, type of identification document, copy of identification document, source of assets and funds, beneficial ownership declaration, prominent public figure declaration, signature of the data subject

Duration of data processing: 8 years from the end of the business relationship, or up to 10 years in the case of a request from a public authority

Intermediate data processor: K&H Bank Zrt., Bankovní informační technologie s.r.o., Československá obchodní banka, a. s., KBC Gloval Services NV (Shared Services Center CZ), CRIF Czech Credit Bureau

3. Contract Management

The Company enters into a contract with merchants wishing to join its payment card acceptance network, in connection with which the Company processes the personal data of the merchant and the contact persons mentioned in the contract.

Purpose of the data processing: to establish a contractual relationship and to perform a contract or service

Legal basis for data processing: performance of a contract

Scope of personal data processed: for natural person customers, name, registered office address, postal address, registration number, tax number, account number; for natural persons linked to legal person customers, name, position, landline telephone number, mobile telephone number, email address

Duration of data processing: for the duration of the contractual relationship

Intermediate data processor: K&H Bank Zrt., Bankovní informační technologie, s.r.o.

4. Relations with customers

The Company processes the data of customers and their contact persons when receiving, receiving and responding to notifications, requests and other submissions from customers by telephone, e-mail or in person, and for the purpose of providing technical support.

Purpose of the data processing: to contact customers

Legal basis for data processing: performance of a contract

Scope of personal data processed: name, mobile phone number, email address

Duration of data processing: during the contractual relationship

Intermediate data processor: Bankovní informační technologie, s.r.o.

5. Sending newsletter

The Company processes and uses the data of the persons registering on the www.khpos.hu website - provided during the registration process - in accordance with the applicable legal provisions in order to send its offers and advertisements to the registrants in a personalized manner. You can also unsubscribe from the newsletter via the "unsubscribe" link on the website or at the bottom of any newsletter or via the contact details provided on the website (https://www.khpos.hu/rolunk).

Purpose of the data processing is: sending offers, articles and newsletters including the Company's business advertising.

Legal basis for data processing: the data subject's consent, which may be withdrawn at any time without justification.

Scope of personal data processed: name and e-mail address of the subscriber, the fact of consent to the sending of the newsletter (channels), subscription and un-subscription data, primary analytical data relating to the deliverability and opening of messages.

Duration of data processing: until consent is withdrawn.

Intermediate data processor: the EDIMA.email Limited Liability Company. The data processor may receive: the name and e-mail address of the registrant. EDIMA.email Limited Liability Company's subcontractor (sub-processor) is INTEGRITY Kft., which provides server services.

6. Complaints handling

The Company processes personal data obtained in the course of complaint handling for the purpose of complaint handling and keeps records of customer complaints and the measures taken to resolve and resolve them. If the customer attaches to the complaint a document or data which the Company is not entitled to handle, it will be returned to the person who submitted it.

Purpose of processing: to investigate and respond to complaints

Legal basis for processing: to fulfil a legal obligation

Personal data processed: the name, mobile phone number and e-mail address of the customer, the first and last name of the person representing the customer, the audio recording of the complaint made by telephone, and any personal data that the customer brings to the attention of the Company in connection with the complaint, and, to the extent necessary for the investigation of the complaint, personal data relating to the contract with the Company.

Duration of processing: the Company will keep the complaint and the response (written documents) and the audio recording of the telephone complaint for 5 years.

7. Sending extracts, invoice letters:

Provision of contractual statements and invoice statements to Customers.

Purpose of the data processing: sending statements, invoice letters

Legal basis for data processing: fulfilment of a legal obligation

Scope of personal data processed: name of the customer, registered office and postal address

Duration of data processing: until the sending of extracts, billing letters

Intermediate data processor: XEROX Magyarország Kft.

8. Notification to the money laundering prevention authorities

The Company shall, pursuant to the relevant provision of the Money Laundering Act, report any data, facts or circumstances indicating that money laundering or terrorist financing has been derived from criminal offences (hereinafter collectively referred to as "the data, facts or circumstances giving rise to the report") and shall report any data, facts or circumstances indicating money laundering, terrorist financing or the derivation of property from criminal offences to the Central Office for the Prevention of Money Laundering and Terrorist Financing of the National Tax and Customs Administration.

Purpose of the data processing: to receive notifications related to the prevention of money laundering and terrorist financing

Legal basis for processing: to fulfil a legal obligation

Scope of personal data processed: Name, Name at birth, Mother's maiden name, Place of birth, Date of birth, Permanent address, Place of residence, Nationality, Type and number of identification documents

Duration of data processing: 8 years from the date of notification

9. Fraud prevention:

In this context, the Company processes personal data and the information extracted therefrom in order to carry out monitoring, preventive, detective and investigative measures required by law and to comply with other obligations. (i) Fraud and/or unethical conduct: in the course of its activities, the Company may use profile data resulting from the fraud prevention profiling process. The process involves monitoring and preventing fraud committed or attempted by Company employees, existing customers, potential customers and any other persons who may have fraudulent intentions towards the Company or its customers, including the whistleblowing process and additional checks carried out during the normal authorisation process. (ii) Physical and digital security: in this area, the Company monitors and investigates infiltration, attacks against the Company and leaks (data leakage) that could cause harm to the Company, its employees or its customers.

Purpose of the data processing: fraud prevention, chargeback management

Legal basis for data processing: legal and contractual obligations

Scope of personal data processed: *Customer (contact) data:* name, e-mail address, telephone number, postal address. Cardholder data: name, address, e-mail address

Duration of data processing: five years after the investigation of fraud, whistleblowing

10. Prior checking of contract terms:

The Company checks the customer's liabilities to other financial institutions in order to secure possible outstanding debts (cancellation of room reservations) arising from the nature of the business relationship (e.g. hotel, car rental service).

Purpose of the data processing: to assess the financial risks to the customer

Legal basis for data processing: contractual performance

Scope of personal data processed: name, name at birth, mother's maiden name, permanent address, postal address, place of birth, date of birth, e-mail address, nationality, identification document details, credit data

Duration of data processing: immediately after assessment of the conditions

Intermediate data processor: BISZ Központi Hitelinformációs Zrt.

11. Replying to requests from public authorities

The Company shall respond to requests received by the Company from various national or international authorities with the information and within the time limits specified by the authority.

Purpose of the data processing: to serve requests from public authorities

Legal basis for data processing: to fulfil a legal obligation

Scope of personal data processed: data indicated in the official request

Duration of data processing: the Company keeps the request and the reply for one year from the date of the reply

Data processor involved: TMF Hungary Kft.

12.Exercise and protection of the Company's rights:

The processing is necessary for the establishment, exercise or defence of the Company's legal claims, including the initiation of court and administrative proceedings, the use of legal experts and legal representatives.

Purpose of the data processing: to present, assert or defend legal claims

Legal basis for data processing: legitimate interest of the Company

Scope of personal data processed: data relevant for the establishment, exercise or defence of legal claims

Duration of data processing: within 5 years after termination of the contract and, in the case of legal proceedings, within 5 years after the final conclusion of the proceedings in respect of the documents and data relating to the proceedings

13.Carrying out clearing and settlement activities:

The direct business of the Company is to settle transactions initiated through virtual and physical terminals in the Company's network by accepting payment cards, in accordance with the contract with its customers. In the context of this activity, the Company processes the personal data necessary to settle the transactions.

Purpose of the data processing: settlement of credit card transactions

Legal basis for data processing: performance of contractual obligations

Scope of personal data processed: *Client (contact person) data:* name, e-mail address, telephone number, postal address; *Cardholder data:* card number, card expiry date, CVV/CVC code, name.

Duration of processing: eight years after the transaction

Data processor: NEXI/SIA S.p.A.**;** Global Payments Europe, s.r.o., Rubean AG

14.Filing

The Company operates an internal document management and filing system for the administration of its activities and legal requirements, whereby it stores documents including personal data.

Purpose of the data processing: filing

Legal basis for data processing: fulfilment of a legal obligation (e.g. 2017. évi LIII. tv.)

Scope of personal data processed: name, other descriptive data relating to documents

Duration of data processing: time limit prescribed by the relevant legislation (e.g. 8 years under LIII. 2017. évi LIII. tv.)

15.Supplier contract management

In order to keep records of its contracts with suppliers, the Company stores the relevant contracts, their details, including personal data of the partner and contact persons.

Purpose of the data processing: management of supplier contracts

Legal basis for data processing: performance of the contract and the Company's legitimate interest in the personal data of its contacts

Scope of personal data processed: name and other personal data indicated in the contracts (e.g. contact details of contact persons)

Duration of data processing: 5 years after termination of the contract

VI. DATA TRANSFER AND DATA TRANSMISSION

1. Data transfer and data transmission conditions

Personal data will be transferred by the Company if it is permitted or required 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.

The list of data processors used by the Company is set out in the table below.

Data processor	Personal information it can access
XEROX Magyarország Kft. (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
K&H Csoportszolgáltató Központ Kft. (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.)
NEXI/SIA S.p.A. (Italy, Via Gonin 36, I20147 Milan)	Responsible for the card clearing and ancillary activities of the Company and its acquirers
EDIMA.email Kft. (1075 Budapest, Holló utca 3-9/A 3. em. 10.) Sub-processor **INTEGRITY Kft.** (8000 Székesfehérvár, Gyetvai u 6.)	Bulk email service for subscribers
K&H Bank Zrt. (1095 Budapest, Lechner Ödön fasor 9.)	Call centre activities
K&H Bank Zrt. (1095 Budapest, Lechner Ödön fasor 9.)	IT operational services (hardware, software, network, printing, scanning, telephone services, GIRO line)
KBC Global Services NV (Shared Service Center Brno) Czech Republic, Radlická 333/150 150 57 Praha 5	Operation of the system used to check existing clients on international sanctions (embargo) lists, carrying out primary screening
CRIF - Czech Credit Bureau Czech Republic, Štětkova 1638/18, 140 00 Praha 4	Operation of a system to monitor prospective and existing customers for the prevention of money laundering and terrorist financing
Československá obchodní banka, a. s. Czech Republic, Radlická 333/150 150 57 Praha 5	Operation of a system to monitor prospective and existing customers for the prevention of money laundering and terrorist financing
ShiwaForce.com Zrt. (1123 Budapest, Alkotás utca 17-19.)	Operation of the Company's website (including the chat function)
Global Payments Europe, s.r.o. (Czech Republic, V Olšinách 626/80, Strašnice, 100 00 Prague 10) Sub-processor: **Rubean AG** (Kistlerhofstraße 168, 81379 München, Germany)	Allow transactions with debit cards
Bankovní informační technologie, s.r.o. (Czech Republic, Radlická 333/150 150 00 Praha 5) Sub-processor: **Monet+ a.s.**	Operation and maintenance of IT systems

(Czech Republic, 763 14 Zlín, Za Dvorem 505) **DabiS Group s.r.o** (Czech Republic, Chopinova 1478/22, 120 00 Praha)	
TMF Magyarország Kft. (1138 Budapest, Népfürdő utca 22. B. ép. 13. em.) Sub-processor: **Manage IT d.o.o.** (Serbia, 11030 Belgrad, Zmanjska 3.) **Török István Attila EV** (1131 Budapest, Rokolya utca 19. IV. em. 4.) **Kis-Vörös Péter EV** (7632 Pécs, Aidinger János út 7. 2. em. 7.) **Microsoft Limited** (United Kingdom, Microsoft Campus, Thames Valley Park, Reading, Berkshire, RG6 1WG)	Accounting, tax and payroll services
CARDNET Zrt. (1135 Budapest, Reitter Ferenc utca 46-48.) Sub-processor: **Pandant TMSZ Kft.** (1045 Budapest, Istvántelki út 8.)	POS terminal operation
UNICOMP Kft. (8000 Székesfehérvár, Palánkai utca 3.)	POS terminal operation

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 payment secrecy.

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 payment secrecy.

The list of outsourced activities for the Company is available on the Company's website, under "documents", sub-menu "other documents".

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.

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 DATA SUBJECTS

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. Photo- and video recordings

The partner renting office space to the Company (Millennium Irodaház Kft.) at the Company's headquarters, which is suitable for semi-reception, uses surveillance by an electronic asset

protection system pursuant to the Act on the Rules of Personal and Property Protection and Private Investigation, and may take photographs and video recordings with the help of the electronic asset protection system. Further information on data management can be found on the partner's website.

2. 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.

3. 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 Company’s website (www.khpos.hu).