

DATA PROCESSING POLICY

Company name: Dental Network Szolgáltató Korlátolt Felelősségű Társaság

Registered office: 1111 Budapest, Bartók Béla út 41, 1st floor, door 1

Company registration number: 01-09-986279

Tax number: 23953662-2-43

Represented by: Melhem Omar

(hereinafter: the "Company")

This Policy sets out the rules governing the processing of personal data of natural persons by the Company (its data processing activities), for the purpose of ensuring compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and with Act CXII of 2011 on Informational Self-Determination and Freedom of Information.

The adoption and amendment of this Policy fall within the competence of the Managing Director.

Done at Budapest on 2 May 2023.

Melhem Omar
Managing Director

ANNEXES

Annex 1: Data Request Form for the Consent-Based Processing of Personal Data

Annex 2: Privacy Notice on the Rights of Natural-Person Data Subjects in Relation to the Processing of Their Personal Data

Annex 3: Notice to Employees on Participation in Fitness-for-Work Examinations

Annex 4: Notice on the Processing of Personal Data in Connection with the Conclusion of a Contract

Annex 5: Notice on the Processing of Contact Details of Natural-Person Representatives of Contractual Partners that are Legal Persons

Annex 6: Notice on the Use of a CCTV Surveillance System

Annex 7: Confidentiality Declaration for Employees of Undertakings Carrying Out Data Processing

Annex 8: Employee Declaration on Having Read and Applying the Data Processing Policy and on Undertaking Confidentiality Obligations

Annex 9: Record of Processing Activities

Annex 10: Record of Processing Activities Carried Out by the Processor on Behalf of Another Controller

CHAPTER I GENERAL PROVISIONS

Section 1 - Preamble

The Company undertakes to carry out its data processing activities, by adopting appropriate internal rules and technical and organisational measures, in a manner compliant with Regulation (EU) 2016/679 of the European Parliament and of the Council 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; hereinafter: the “Regulation” or “GDPR”), as well as with Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: the “Privacy Act”).

Section 2 - Purpose of the Policy

This Policy is based on the provisions of the Regulation and the Privacy Act and is intended to demonstrate that the Company complies with the rules and principles of the Regulation applicable to the processing of personal data.

Section 3 - Scope of the Policy

(1) This Policy applies to the processing by the Company of the personal data of natural persons who are in a contractual relationship with the Company or come into contact with the Company in the course of a contractual offer or negotiations, including, for example, employees, sole traders, sole proprietorships, primary agricultural producers, natural-person customers, sellers, suppliers and other natural-person contractual partners.

(2) This Policy also applies to the recording and processing of the contact details of natural-person representatives of legal persons that have a relationship with the Company.

Section 4 - Definitions and supplementary rules

(1) For the purposes of this Policy, the definitions set out in Article 4 of the Regulation shall apply. Individual chapters of this Policy may contain additional definitions.

(2) In the individual chapters, recipients of personal data means persons who may collect, access, record, organise, store, process, erase, transmit or otherwise handle personal data.

(3) A member of the body performing the Company's supervisory functions (Supervisory Board, Audit Committee) may, in the course of carrying out supervisory activities, access personal data processed by the Company, provided that such member has signed the confidentiality declaration forming Annex 10 to this Policy.

(4) Where legislation prescribes a retention period longer than that specified in this Policy, the retention period prescribed by law shall apply.

CHAPTER II

ENSURING THE LAWFULNESS OF PROCESSING

Section 5 - Processing based on the data subject's consent

(1) Where processing is based on consent, the data subject's consent to the processing of his or her personal data shall be requested by means of the data request form set out in Annex 1.

(2) Consent shall also include the data subject ticking a box on the Company's website indicating consent to the processing of personal data, or any other statement or conduct which clearly indicates the data subject's agreement to the intended processing. Silence, a pre-ticked box on the Company's website, or inactivity shall not constitute consent.

(3) Consent shall cover all processing activities carried out for the same purpose or purposes. Where processing serves multiple purposes, consent shall be given for all processing purposes.

(4) The Company shall not make the conclusion or performance of a contract conditional on consent to the processing of personal data that are not necessary for the performance of that contract.

(5) It shall be as easy to withdraw consent as to give it.

(6) Where personal data have been collected with the data subject's consent, the controller may, unless otherwise provided by law, continue to process the collected data without further consent for the purpose of complying with a legal obligation applicable to it, including after the withdrawal of the data subject's consent.

(7) The Company shall publish its general privacy notice set out in Annex 2 on www.dentalnetwork.hu. The purpose of the notice is to provide data subjects, before processing begins and throughout the period of processing, with detailed information on all material circumstances and facts relating to the processing of their data, in particular the purposes and legal bases of processing, the persons authorised to act as controller and processor, the duration of processing, the fact that the controller processes personal data in accordance with the Regulation and the Privacy Act, and the persons who may have access to the data. The notice shall also set out the data subject's rights in relation to processing and the available remedies. Before processing begins, data subjects shall be informed where the notice can be accessed.

Section 6 - Processing based on compliance with a legal obligation

(9) Processing based on compliance with a legal obligation is independent of the data subject's consent, because the processing is prescribed by law or other legislation. Before processing begins, the data subject shall be informed that the processing is based on compliance with a legal obligation and shall be provided with clear and detailed information concerning all facts relating to the processing of his or her data, in particular the purpose and legal basis of processing, the persons authorised to act as controller and processor, the duration of processing, whether the controller processes the personal data on the basis of a legal obligation applicable to it, and the persons who may access the data. The information shall also cover the data subject's rights relating to processing and the available remedies. In the case of mandatory processing, the information may also be provided by referring, for example on a website, to the statutory provisions containing the above information.

CHAPTER III

PROCESSING IN CONNECTION WITH EMPLOYMENT

For the purposes of this Chapter, “employees” means employees employed by the Company.

Section 7 - Employment and personnel records

(1) Only such data may be requested from and recorded in relation to employees, and only such fitness-for-work examinations (including occupational medical examinations) may be required, as are prescribed by rules applicable to employment, are necessary for the establishment, maintenance or termination of the employment relationship, and do not infringe the employee's personality rights.

(2) For the purposes of establishing, maintaining or terminating an employment relationship, the Company processes the following employee data on the basis of a legal obligation and/or the employer's legitimate interests (Article 6(1)(f) GDPR):

1. name;
2. birth name;
3. place and date of birth;
4. mother's name;
5. residential address;
6. nationality;
7. tax identification number;
8. Hungarian social security (TÁJ) number;
9. pensioner registration number (for pensioner employees);
10. telephone number;
11. e-mail address;
12. identity card number;
13. address card number;
14. bank account number (where salary is paid by bank transfer);
15. online identifier (if any);
16. commencement and end dates of employment;
17. position/job title;
18. copy of documents evidencing educational qualifications and professional qualifications;
19. curriculum vitae;
20. photograph (if requested, e.g. for the CV);
21. data relating to salary, salary payments and other benefits;
22. debts to be deducted from the employee's salary pursuant to a final decision, legislation or the employee's written consent, and documents evidencing the entitlement to such deduction;
23. documents containing an evaluation of the employee's work;
24. manner of termination of employment and the related documents;
25. certificate of good conduct/criminal record certificate (where required for the position);
26. documents relating to fitness-for-work examinations;
27. in the case of membership in a private pension fund or voluntary mutual insurance fund: the name and identification number of the fund and the employee's membership number;
28. for foreign employees: passport number and the name and number of the document evidencing the right to work;
29. data recorded in the report of an accident suffered by the employee;
30. where a privately owned motor vehicle is used for official purposes: vehicle registration number and driving licence number;
31. where a driving licence is required for the position: driving licence number and a copy of the licence.

(3) The Company shall process data concerning illness and trade-union membership only for the purpose of exercising a right or fulfilling an obligation laid down in the Labour Code.

(4) Recipients of personal data: the head of the employer and the person exercising employer's rights. Employees of the Company performing employment-related duties, including HR staff, payroll and accounting personnel, and processors may access only those personal data that are necessary for the performance of their respective tasks.

(5) Retention period: data listed in points 1-5, 7-9, 16, 21-22 and 27 shall be retained for 50 years after termination of employment; all other data shall be retained for 3 years.

(6) Before processing begins, the data subject shall be informed that the processing is based on the Labour Code, social security, tax and pension legislation, and the pursuit of the employer's legitimate interests.

(7) At the time the employment contract is concluded, the employer shall provide the employee with the Notice set out in Annex 2 to this Policy, informing the employee about the processing of personal data and his or her personality rights.

Section 8 - Processing in connection with fitness examinations, including occupational medical fitness examinations

(1) An employee may only be required to undergo a fitness examination prescribed by legislation or a rule applicable to employment, or necessary for exercising a right or fulfilling an obligation laid down in a rule applicable to employment. Before the examination, employees shall be informed in detail, inter alia, of the skill or ability to be assessed, the instrument and method used for the examination, and the reason for the examination. Where the examination is required by legislation, employees shall also be informed of the title and number of the legislation and the exact legal provision. A model privacy notice relating to fitness examinations is set out in Annex 3.

(2) Personal data that may be processed: the fact of occupational and medical fitness and the conditions necessary for such fitness.

(3) Legal basis: legislation (the Labour Code and Decree 33/1998 (VI.24.) NM on medical examinations and opinions concerning occupational, professional and personal-hygiene fitness) and the employer's legitimate interest.

(4) Purpose: establishment and maintenance of employment and filling the relevant position.

(5) Recipients/categories of recipients: the employee examined and the professional carrying out the examination may know the result. The employer may receive only information as to whether the person examined is fit or unfit for work/the relevant position and what conditions, if any, must be provided. The employer may not access the details or complete documentation of the examination.

(6) Retention period: 3 years following termination of employment.

Section 9 - Processing of job applicants' data

(1) Personal data that may be processed: name, place and date of birth, mother's name, residential address, qualification data and copies of related certificates, photograph, telephone number, e-mail address, CV, submitted application, and the employer's evaluation/notes concerning the applicant.

(2) Purpose: handling and assessing the application and concluding an employment contract with the selected applicant. The data subject shall be informed within 15 days after the rejection decision if the employer has not selected him or her for the position.

(3) Legal basis: the data subject's consent.

(4) Recipients: the manager or body entitled to exercise employer's rights at the Company and employees performing employment/personnel functions.

(5) Retention period: 15 days after the assessment of the application. The personal data of unsuccessful applicants shall be erased on the 16th day. The data of an applicant who withdraws his or her application shall also be erased.

(6) The employer may retain applications beyond the period specified in paragraph (5) only on the basis of the data subject's express, unambiguous and freely given consent, provided that retention is necessary to achieve a processing purpose consistent with applicable law. Such consent shall be requested from applicants after the recruitment procedure has ended and no later than the deadline specified in paragraph (2).

CHAPTER IV REGISTER OF MEMBERS

Section 10 - Register of members (shareholders' personal data) - in the case of a limited liability company

(1) The following personal data of a member of the limited liability company may be processed:

1. name;
2. birth name;
3. place and date of birth;
4. mother's name;
5. residential address;
6. tax identification number;
7. TAJ number;
8. telephone number;
9. e-mail address;
10. identity card number;
11. address card number;
12. bank account number (where any monetary payment is made by bank transfer);
13. online identifier (if any);
14. commencement and end dates of membership;
15. amount of the member's capital contribution.

(2) Recipients: the Managing Director. Employees of the Company performing employment-related tasks, payroll and accounting staff and processors, and the employee maintaining the register of members may access only the data necessary for the performance of their respective tasks.

(3) Retention period: data listed in points 1-7 and 14-15 shall be retained for 5 years following termination of membership; all other data shall be retained for 3 years.

(4) The Company shall provide the member with the Notice set out in Annex 2, informing the member about the processing of personal data and his or her personality rights.

CHAPTER V PROCESSING RELATED TO CONTRACTS

Section 11 - Processing of data of contractual partners - landlords (landowners, usufructuaries), customers, suppliers, etc.

(1) Legal basis/purpose of processing: steps taken prior to entering into a contract, conclusion, performance and termination of the contract.

(2) Categories of data subjects: natural persons acting as customers, suppliers, participants in integration arrangements, recipients of services, or persons otherwise having or entering into a business relationship with the Company, in respect of data prescribed by law.

(3) Categories of data processed: name, birth name, place and date of birth, mother's name, residential address, tax identification number, tax number, entrepreneur's licence/identity card

number, address, registered office, telephone number, e-mail address, website address, bank account number, customer number/order number and online identifier.

(1) Retention period: 8 years following termination of the contract. [Where legislation (e.g. legislation governing a subsidy or grant) prescribes a longer period for the registration or retention of contracts, the period specified by such legislation shall be stated/applied.]

(2) The data subject shall be informed of any transfer of his or her personal data to a processor (e.g. an accounting firm).

(3) The wording of the data processing clause relating to contracts concluded with natural persons is contained in Annex 4 to this Policy.

Section 12 - Personal data of natural-person representatives of legal-person partners

(1) Personal data that may be processed: name, address, telephone number, e-mail address and online identifier.

(2) Purpose: conclusion and performance of contracts with the Company's legal-person partner and maintenance of business contacts.

(3) Legal basis: the Company's legitimate interest.

(4) Recipients/categories of recipients: employees of the Company responsible for concluding/recording contracts and employees performing accounting duties.

(5) Retention period: 5 years following the end of the business relationship or the end of the data subject's status as representative. Where legislation (e.g. tax legislation) prescribes a longer period for the registration or retention of contracts, the statutory period shall apply.

(6) A model information sheet for data collection is contained in Annex 6 to this Policy. The employee who is in contact with the customer, buyer or supplier shall present this notice to the data subject. The declaration shall be retained for the duration of the processing.

CHAPTER VI PROCESSING BASED ON LEGAL OBLIGATIONS

Section 13 - Processing for compliance with tax and accounting obligations and data-reporting obligations relating to land use

(1) The Company processes the data prescribed by law concerning natural persons acting as customers, suppliers, participants in integration arrangements, recipients of services, or persons otherwise having or entering into a business relationship with it.

(2) Personal data that may be processed: natural identification data of the natural person, including name (former name), place and date of birth, mother's name, residential address, tax number, tax identification number and entrepreneur's licence number.

(3) Legal basis: compliance with obligations under tax legislation (including Act CXXVII of 2007 on Value Added Tax, Act CXVII of 1995 on Personal Income Tax and Act CL of 2017 on the Rules of Taxation), and steps taken prior to entering into a contract (conclusion of a contract); in the case of amendment of a contract: performance of the contract.

(4) Recipients: employees of the Company performing tasks relating to the conclusion and recording of contracts, accounting and taxation, and the head of the Company.

(5) Retention period: 8 years following termination of the contract. [Where legislation (e.g. legislation governing a subsidy or grant) prescribes a longer period for the registration or retention of contracts, the period specified by such legislation shall apply.]

Section 14 - Processing by the Company as payer

(1) For the purpose of complying with statutory tax and contribution obligations (assessment of tax, tax advances and contributions, payroll and social-security administration), and on the legal basis of compliance with a legal obligation, the Company processes the personal data prescribed by tax legislation of data subjects - employees, other persons engaged by the Company, recipients of other benefits and contractual partners - with whom it has a payer relationship within the meaning of Section 7(31) of Act CL of 2017 on the Rules of Taxation.

(2) Categories of data: natural identification data, including name (former name), place and date of birth, mother's name, residential address, tax number and tax identification number, social-security identification number (TAJ), and, where the data subject is a pensioner, pensioner registration number. Where tax legislation attaches legal consequences to such data, the Company may process employees' health data (Section 40 of the Personal Income Tax Act) and data concerning trade-union membership (Section 47(2)(b) of the Personal Income Tax Act) for the purpose of complying with tax and contribution obligations, including payroll and social-security administration.

(3) Legal basis: compliance with obligations laid down in tax legislation, including Act CXXVII of 2007 on Value Added Tax, Act CXVII of 1995 on Personal Income Tax and Act CL of 2017 on the Rules of Taxation, and in Act LXXX of 1997 on Persons Entitled to Social Security Benefits and Private Pensions and the Funding of These Services.

(4) Retention period: 8 years following termination of the legal relationship constituting the legal basis.

(5) Recipients: employees of the Company performing taxation, payroll, social-security/payer and accounting duties.

Section 15 - Processing for compliance with anti-money-laundering obligations

[This section is required where the controller carries out an activity listed in Section 1(k) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing, including acting as a trader in goods where, in the course of its activities, it accepts cash payments of HUF 2,500,000 or more.]

(1) On the legal basis of compliance with a legal obligation, and for the purpose of preventing and combating money laundering and terrorist financing, the Company processes the data of its customers, their representatives and beneficial owners as specified in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "AML Act"), including: (a) family name and given name; (b) birth family name and given name; (c) nationality; (d) place and date of birth; (e) mother's birth name; (f) residential address or, failing this, place of stay; (g) type and number of identification document and number of the official address card, as well as copies of the documents presented.

(2) Recipients: employees of the Company performing tasks related to the conclusion of contracts, the head of the Company and the person designated by the Company under the AML Act.

(3) Retention period: 8 years from the termination of the business relationship or completion of the transaction order (Section 56(2) of the AML Act).

CHAPTER VII PROCESSING IN CONNECTION WITH CAMERA SURVEILLANCE

Section 16 - Processing in connection with workplace CCTV surveillance

(1) At its registered office, premises and areas open for customer reception, the Company operates an electronic surveillance system for the purposes of protecting human life, physical integrity, personal liberty, business secrets and property. The system may allow image, audio, or combined image-and-audio recording; accordingly, the conduct of a data subject recorded by a camera also constitutes personal data.

(2) The legal basis for such processing is the pursuit of the employer's legitimate interests and the data subject's consent.

(3) Where an electronic surveillance system is used in a given area, a clearly visible and legible warning sign and notice shall be displayed in a manner enabling third persons intending to enter the area to obtain information. Where the Company uses more than one camera, information shall be provided in respect of each camera. The notice shall cover the fact of surveillance, the purpose of making and storing image/audio recordings containing personal data, the legal basis for processing, the place and duration of storage, the identity of the person operating the system, the persons authorised to access the data, and the rights of data subjects and the procedure for exercising those rights. A model notice is contained in Annex 7 to this Policy.

(4) Image and audio recordings of third persons entering the monitored area (customers, visitors and guests) may be made and processed with their consent. Consent may also be given by conduct. In particular, conduct indicating consent includes entering the monitored area despite the displayed sign and notice informing the person of the operation of the electronic surveillance system. In the case of employees, the legal basis for processing is the employer's legitimate interest.

(5) Unless used for a specific purpose, recordings may be retained for a maximum of 3 (three) working days. Use means the intended use of recorded image, audio, combined image-and-audio recordings or other personal data as evidence in judicial or administrative proceedings.

(6) A person whose right or legitimate interest is affected by the recording of image, audio, or combined image-and-audio data may, within three working days of the recording, request - upon substantiating his or her right or legitimate interest - that the controller not destroy or erase the data.

(7) An electronic surveillance system may not be used in rooms where surveillance could violate human dignity, in particular changing rooms, showers, toilets, medical rooms or their waiting areas, or rooms designated for employees to spend work breaks.

(8) Outside working hours or on public holidays/non-working days, the entire workplace may be monitored.

(9) Recipients of data recorded by the electronic surveillance system/persons authorised to view recordings: operating staff for the purposes of detecting infringements and checking the operation of the system, the head of the employer, and the manager responsible for the monitored workplace area.

Section 17 - Processing in connection with the use of a GPS navigation system

(1) Legal basis: the employer's legitimate interest. Purposes: work organisation, logistics and monitoring compliance with employee obligations.

(2) Data processed: vehicle registration number (or identifier of the power-driven machine/work machine), route travelled, distance travelled and duration of vehicle/machine use.

(3) Monitoring may extend only to the employer's vehicle, power-driven machine or work machine.

Section 18 - Processing in connection with workplace entry and exit

(1) Where a non-electronic access-control system is operated, information shall be displayed identifying the controller and explaining the manner in which data are processed.

(2) Personal data that may be processed: name, residential address, vehicle registration number, time of entry and time of exit.

(3) Legal basis: pursuit of the employer's legitimate interests.

(4) Purposes: protection of property, performance of contracts and monitoring compliance with employee obligations.

(5) Recipients/categories of recipients: the manager entitled to exercise employer's rights at the Company and, as processor, employees of the Company's contracted security provider.

(6) Retention period: 6 months.

CHAPTER VIII DATA SECURITY MEASURES

Section 19 - Data security measures

- (1) In relation to all processing activities, the Company shall take the technical and organisational measures and establish the procedural rules necessary to ensure the security of personal data and to give effect to the Regulation and the Privacy Act.
- (2) The Company shall protect data by appropriate measures against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure or unauthorised access.
- (3) The Company treats personal data as confidential. Employees are subject to confidentiality obligations concerning the processing of personal data, for which the declaration set out in Annex 8 shall be used. The Company restricts access to personal data by assigning access levels.
- (4) The Company protects its IT systems by firewall and anti-virus protection.
- (5) Electronic data processing and record-keeping are carried out by means of computer software that complies with data-security requirements. The software ensures that access to data is purpose-limited, takes place under controlled conditions, and is granted only to persons who need access to perform their duties.
- (6) In the course of automated processing of personal data, the controller and processor shall ensure through additional measures: (a) prevention of unauthorised data entry; (b) prevention of unauthorised use of automated processing systems by means of data-transmission equipment; (c) the ability to verify and establish the bodies to which personal data have been or may be transmitted by means of data-transmission equipment; (d) the ability to verify and establish which personal data were entered into automated processing systems, when and by whom; (e) recoverability of installed systems in the event of a malfunction; and (f) reporting of errors occurring during automated processing.
- (7) To protect personal data, the Company shall ensure the monitoring of incoming and outgoing electronic communications.
- (8) Documents currently being worked on or processed may be accessed only by the competent administrators. Personnel, payroll and employment documents, and documents containing the personal data of natural persons in a contractual relationship with the Company, shall be kept securely locked, and the Company shall ensure that keys to the relevant rooms/cabinets are accessible only to authorised persons.

CHAPTER IX THE COMPANY'S ACTIVITIES AS DATA PROCESSOR

Section 20 - Data processing activities

The Company acts as a processor in relation to the following activities:

- (a) Personal data relating to the taxation, social-security relationships and applications for subsidies/grants of natural persons participating in integration arrangements.

For the purposes of this Chapter:

processor: the Company;

principal/controller: the natural persons on whose instructions the Company performs the activities described in point (a).

(a) Guarantees provided by the Processor

- (1) In its capacity as processor, the Company guarantees - in particular with regard to expertise, reliability and resources - that it will implement technical and organisational measures ensuring compliance with the requirements of the Regulation, including the security of processing.

(2) In the course of its processing activities, the Processor shall ensure that persons authorised to access the personal data concerned - unless they are otherwise subject to an appropriate statutory duty of confidentiality - undertake a confidentiality obligation in respect of the personal data of which they become aware. The applicable Confidentiality Declaration is contained in Annex 8.

(3) The Company has appropriate hardware and software and undertakes to implement technical and organisational measures suitable for ensuring the lawfulness of processing and protecting data subjects' rights.

(4) The Company has the legal and technical conditions necessary for electronic communication with public authorities.

(5) The Company undertakes to make available to the principal all information necessary to demonstrate compliance with the legal provisions governing the use of processors.

(b) Obligations and rights of the Principal

(1) The Principal is entitled to verify the existence and implementation by the Processor of the contractual data-security commitments.

(2) It is the Controller's obligation to inform the natural-person data subjects about the processing and, where required by law, to obtain their consent.

(c) Obligations and rights of the Processor

(1) Right of instruction: in the course of its activities, the Processor shall act solely on the written instructions of the Principal.

(2) Confidentiality: the Processor shall ensure that persons authorised to access the personal data concerned - unless otherwise subject to an appropriate statutory duty of confidentiality - undertake confidentiality obligations in respect of the personal data of which they become aware.

(3) Data security: taking into account the nature, circumstances and purposes of processing and the rights of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Processor shall take measures to ensure that natural persons acting under its authority who have access to personal data process such data only on instructions from the controller, unless they are required to do otherwise by Union or Member State law. The Processor shall ensure that stored data may be accessed, whether through internal systems or by direct access, only by authorised persons and only in connection with the purposes of processing. The Processor shall ensure the necessary regular maintenance and development of the equipment used. Equipment storing data shall be kept in a closed room with appropriate physical protection, and its physical security shall also be ensured. For the performance of the tasks specified in the contract, the Processor shall use persons with appropriate knowledge and experience and shall ensure that such persons are properly trained regarding applicable data-protection legislation, contractual obligations, and the purpose and manner of data collection.

(4) Engagement of another processor: [This applies where the Company uses a third party - a person or organisation not employed by the Company, e.g. an accounting firm - in connection with accounting activities undertaken for external persons.] The Processor shall engage another processor only subject to the conditions laid down in the Regulation and the Privacy Act. This also requires the Principal to authorise the Processor, in a private document with full probative force, to engage another processor/subcontractor. Before engaging another processor, the Processor shall inform the Principal of the identity of the further processor and the intended tasks to be performed by it. If the Principal objects on the basis of this information, the further processor may be engaged only if the conditions specified in the objection are satisfied. Where the Processor engages another processor to carry out specific processing activities on behalf of the Principal, it shall conclude a written contract with that processor imposing the same data-protection obligations as those set out in the contract between the Principal and the Processor. The further processor shall provide sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of the Regulation. If the further processor fails to fulfil its data-protection obligations, the Processor that engaged it shall remain fully liable to the Principal for the performance of the

further processor's obligations.

(4) Cooperation with the Principal:

(a) In the course of its activities, the Processor shall assist the Principal by all appropriate means in facilitating the exercise of the Principal's rights and fulfilment of its related obligations.

(b) Taking into account the nature of processing and the information available to it, the Processor shall assist the Principal in ensuring compliance with the obligations under Articles 32-36 of the Regulation (security of processing, data protection impact assessment and prior consultation).

(c) The Processor shall make available to the Principal all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the Regulation (Processor) and shall allow for and contribute to audits, including inspections, conducted by the Principal or another auditor mandated by the Principal. In connection with this provision, the Processor shall immediately inform the Principal if, in its opinion, an instruction infringes the Regulation or other Union or Member State data-protection provisions.

CHAPTER X MANAGEMENT OF PERSONAL DATA BREACHES

Section 21 - Definition of a personal data breach

(1) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) GDPR).

(2) Examples include the loss of a laptop containing personal data; insecure storage of personal data; insecure transmission of data; unauthorised copying or transmission of customer/buyer/partner lists; attacks against servers; and hacking of the website.

Section 22 - Handling and remediation of personal data breaches

(1) The prevention and management of personal data breaches and compliance with the applicable legal requirements are the responsibility of the head of the Company.

(2) Access and attempted access to IT systems shall be logged and continuously analysed.

(3) If employees of the Company authorised to perform monitoring detect a personal data breach in the course of their duties, they shall immediately notify the head of the Company.

(4) Employees of the Company shall report to the head of the Company or the person exercising employer's rights if they detect a personal data breach or an event indicating a possible breach.

(5) A personal data breach may be reported via the Company's central e-mail address or telephone number, through which employees, contractual partners and data subjects may report the underlying events.

(6) Upon receipt of a personal data breach report, the head of the Company - with the involvement of the employee responsible for data security - shall investigate it without delay. The incident shall be identified and it shall be determined whether it constitutes an actual breach or a false alarm. The following shall be examined and established: (a) the time and place of the incident; (b) its description, circumstances and effects; (c) the categories and quantity of data accessed without authorisation; (d) the categories of persons affected; (e) measures taken to remedy the incident; and (f) measures taken to prevent, remedy or mitigate damage.

(7) In the event of a personal data breach, the affected systems, persons and data shall be identified, delimited and isolated, and evidence substantiating the occurrence of the incident shall be collected and preserved. Restoration of damage and lawful operation may commence thereafter.

Section 23 - Record of personal data breaches

(1) A record shall be kept of personal data breaches containing: (a) the categories of personal data concerned; (b) the categories and number of data subjects affected; (c) the date/time of the breach;

(d) the circumstances and effects of the breach; (e) the measures taken to remedy the breach; and
(f) any other data required by the legislation governing the processing.

(2) Data relating to personal data breaches contained in the record shall be retained for 5 years.

CHAPTER XI RIGHTS OF THE DATA SUBJECT

Section 24 - Information on the rights of the data subject

For the purposes of this Chapter, “data subject” means any natural person whose data are processed by the Company as controller.

(a) Right to prior information

The data subject has the right to receive information about facts and information relating to the processing before processing begins. (Articles 13-14 GDPR)

(b) Right of access

The data subject has the right to obtain confirmation from the Controller as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and the related information specified in the Regulation. (Article 15 GDPR)

(c) Right to rectification

The data subject has the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement. (Article 16 GDPR)

(d) Right to erasure ('right to be forgotten')

The data subject has the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay, and the Controller is obliged to erase such data without undue delay where one of the grounds specified in the Regulation applies. (Article 17 GDPR)

(e) Right to restriction of processing

The data subject has the right to obtain from the Controller restriction of processing where the conditions specified in the Regulation are met. (Article 18 GDPR)

(f) Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the data subject about those recipients if the data subject so requests. (Article 19 GDPR)

(g) Right to data portability

Subject to the conditions laid down in the Regulation, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another Controller without hindrance from the Controller to which the personal data were provided. (Article 20 GDPR)

(h) Right to object

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her based on Article 6(1)(e) GDPR (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller) or Article 6(1)(f) GDPR (processing necessary for the purposes of the legitimate interests pursued by the Controller or by a third party). (Article 21 GDPR)

(i) Automated individual decision-making, including profiling

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (Article 22 GDPR)

(j) Restrictions

Union or Member State law to which the Controller or Processor is subject may, by way of legislative measures, restrict the scope of the obligations and rights provided for in Articles 12-22 and Article 34, as well as Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12-22. (Article 23 GDPR)

(k) Communication of a personal data breach to the data subject

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the personal data breach to the data subject without undue delay. (Article 34 GDPR)

(l) Right to lodge a complaint with a supervisory authority (administrative remedy)

The data subject has the right to lodge a complaint with a supervisory authority - the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), 1025 Budapest, Szilágyi Erzsébet fasor 22/c - if the data subject considers that the processing of personal data relating to him or her infringes the Regulation. (Article 77 GDPR)

(n) Right to an effective judicial remedy against a supervisory authority

Every natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, or where the supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged. (Article 78 GDPR)

(p) Right to an effective judicial remedy against a controller or processor

Each data subject has the right to an effective judicial remedy where he or she considers that his or her rights under the Regulation have been infringed as a result of processing of personal data in non-compliance with the Regulation. (Article 79 GDPR)

CHAPTER XII

SUBMISSION OF REQUESTS BY DATA SUBJECTS AND ACTION BY THE CONTROLLER

Section 25 - Measures taken on the basis of a data subject's request

(1) The Company, as Controller, shall inform the data subject without undue delay and in any event within one month of receipt of the request of the action taken on a request concerning the exercise of the data subject's rights.

(2) Where necessary, taking into account the complexity and number of requests, that period may be extended by a further two months. The Controller shall inform the data subject in writing - including by e-mail where the request was received by e-mail - of any such extension within one month of receipt of the request, together with the reasons for the delay.

(4) If the Controller does not take action on the data subject's request, it shall inform the data subject without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint with the supervisory authority (NAIH) and seeking a judicial remedy.

(5) The Company, as Controller, shall provide the information referred to in Articles 13 and 14 of the Regulation, information on the data subject's rights (Articles 15-22 and 34), and measures taken in response to requests free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may refuse to act on the

request.

The Company shall bear the burden of demonstrating the manifestly unfounded or excessive character of a request.

CHAPTER XIII FINAL PROVISIONS

Section 26 - Adoption and amendment of the Policy

The Managing Director of the Company is authorised to adopt and amend this Policy.

Section 27 - Measures to ensure awareness of the Policy

The provisions of this Policy shall be made known to all employees (other persons engaged) of the Company, and contracts for the performance of work shall stipulate that compliance with and enforcement of this Policy form part of the duties of every employee (other person engaged).

....., 2023

.....