

DATA PRIVACY POLICY

Effective as of October 20, 2026

NoBoMed Private Company Limited by Shares
(“Company”)

For the purpose of complying 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, hereinafter: GDPR or Regulation), the Company performs its own data processing activities falling under the scope of the Regulation in accordance with the rules set forth in this Policy.

Budapest, on October 20, 2026

Dr. Csilla Pozsgay m.p.

NoBoMed Private Company Limited by Shares
represented by
Dr. Csilla Pozsgay
Chairperson of the Board of Directors

CHAPTER I GENERAL PROVISIONS

1. Data of the Company as Data Controller:

Company Name: **NoBoMed Private Limited Company**

Registered Office: **1134 Budapest, Váci út 49.**

Company Registration Number: **01-10-141943**

Tax Number: **32019681-2-41**

Representative: **Dr. Csilla Pozsgay, Chairperson of the Board of Directors**

Phone Number: **+36 30 350 0053**

E-mail Address: **info@nobomed.hu**

Website: **www.nobomed.hu**

(hereinafter: Company or Data Controller)

2. Purpose of the Policy

In order to ensure that its data processing activities comply with the provisions of the Regulation and Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information (hereinafter: Info Act), the Company defines in this Policy the rules and lines of responsibility, and regularizes the measures that ensure the Company's data processing complies with the statutory provisions referenced in this section.

3. Scope of the Policy

(1) The scope of this Policy applies to the processing of data of natural persons by the Company. For the purposes of this Policy, sole proprietors and natural person representatives of legal entities shall also be deemed natural persons.

(3) The scope of the Policy does not extend to the processing of personal data concerning legal entities, including the name and legal form of the legal entity, and the contact details of the legal entity.

4. Definitions

The Company notes that the definitions specified in this section are based on the terminology of the Regulation.

1. **"data processing"**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
2. **"personal data"**: means any information relating to an identified or identifiable natural person ("data subject"); who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

3. **"controller"**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
4. **"consent of the data subject"**: a voluntary, specific, and unambiguous expression of the data subject's will, based on adequate information, by which the data subject indicates, through a statement or an action that unequivocally expresses such consent, that he or she consents to the processing of personal data concerning him or her;
5. **"pseudonymisation"**: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6. **"filing system"**: means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
7. **"restriction of processing"**: means the marking of stored personal data with the aim of limiting their processing in the future;
8. **"data processor"**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. **"recipient"**: means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
10. **"third party"**: means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
11. **"profiling"**: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
12. **"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.

CHAPTER II

ENSURING THE LAWFULNESS OF DATA PROCESSING

1. Data Processing Based on the Consent of the Data Subject

(1) In the case of data processing based on consent (Article 6(1)(a) of the GDPR), the data subject's consent to the processing of their personal data must be requested using a data collection form. The template for the data collection form is included in Annex 1 to this Policy.

(2) Where relevant to the website operated by the Company (www.nobomed.hu), consent shall also include the data subject ticking a box when visiting the Company's website, choosing technical settings, or making any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes, or inactivity therefore do not constitute consent.

(3) Consent covers all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent must be given for all data processing purposes.

(4) If the data subject's consent is given in the context of a written declaration which also concerns other matters – e.g., concluding a sales or service contract – the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration containing the data subject's consent that violates the Regulation shall not be binding.

(5) The Company may not condition the conclusion or performance of a contract on consent to the processing of personal data that is not necessary for the performance of the contract.

(6) It must be as easy to withdraw consent as it is to give it.

(7) If personal data was collected with the data subject's consent, the data controller may, in the absence of a statutory provision to the contrary, process the collected data for the purpose of fulfilling a legal obligation applicable to it without further specific consent, and even after the withdrawal of the data subject's consent.

(8) The Company makes its privacy notice available to data subjects on its website or in another manner compliant with the provisions of the Regulation and the Info Act. The purpose of this notice is to inform data subjects clearly and in detail, prior to and during the data processing, of all facts related to the processing of their data, in particular the purpose and legal basis of the processing, the identity of the person entitled to perform the processing and data processing operations, the duration of the processing, whether the data subject's personal data is processed by the controller pursuant to Article 6(1)(c) or (f) of the Regulation, and who may access the data. The notice must also cover the data subject's data processing rights and options for legal remedy. Data subjects must be informed about the availability of this notice.

(9) Data processing based on the legal basis of fulfilling a legal obligation is independent of the data subject's consent, as the data processing is mandated by law. In this case, the data subject must be informed before data processing begins that the processing is mandatory, and must be clearly and comprehensively informed of all facts regarding the processing of their data, in particular the purpose and legal basis, the identity of

the person authorized to process and handle the data, the duration, whether the controller processes the personal data based on a legal obligation, and who may access the data. The notice must also cover the data subject's data processing rights and legal remedies. In the case of mandatory data processing, information may also be provided by publishing a reference to the statutory provisions containing the aforementioned information.

CHAPTER III

EMPLOYMENT-RELATED DATA PROCESSING

1. Employment Records

(1) Only data necessary for establishing, maintaining, and terminating an employment relationship, or for providing social welfare benefits, may be requested and recorded from employees, and occupational health checks may only be performed if they do not violate the employee's personality rights.

(2) For the purpose of fulfilling its legal obligations (Article 6(1)(c) of the Regulation, the Labor Code, and relevant tax and social security legislation) for the establishment, performance, or termination of an employment relationship, the Company processes the following data of the employee:

1. Name
2. Birth name
3. Place and date of birth
4. Mother's name
5. Home address
6. Nationality
7. Tax identification number
8. Social security (TÁJ) number
9. Pensioner registration number (for retired employees)
10. Phone number
11. E-mail address
12. ID card number
13. Official address card number
14. Bank account number
15. Online identifier (if any)
16. Start and end date of employment
17. Job position
18. Copy of documents certifying educational level and professional qualifications
19. CV / Resume
20. Amount of salary, data related to payroll and other benefits
21. Debts to be deducted from the employee's salary based on a legally binding decision, legislation, or written consent, and the entitlement thereto
22. Performance evaluation of the employee
23. Method and reasons for terminating employment
24. Certificate of good conduct (depending on the position)
25. Summary of occupational health fitness assessments
26. In the case of private pension fund and voluntary mutual insurance fund membership, name of the fund, identification number, and employee membership number
27. For foreign employees passport number; name and number of document certifying eligibility for employment
28. Data recorded in logs of accidents suffered by the employee

- 29. Data required to utilize welfare services and commercial accommodation
- 30. Data recorded by the access control system or location tracking systems used at the Company for security and asset protection purposes.

(3) Recipients of the personal data: the employer's manager and the person exercising employer rights, their deputies, employees and data processors of the Company involved in concluding the contract with the data subject, or performing labor, payroll, or HR duties.

(4) Retention period of personal data: 3 years following the termination of employment.

(5) Prior to commencing data processing, the data subject must be informed that the processing is based on the Labor Code, relevant tax and social security laws (fulfillment of legal obligation), and, regarding internal security systems, the legitimate interests of the employer.

(6) Concurrently with concluding the employment contract, the employer informs the employee about the processing of their personal data and their personality rights using the notice according to Annex 2 of this Policy.

2. Processing of Data Related to Fitness Assessments

(1) Only such fitness assessments may be applied to an employee that are prescribed by employment rules or are necessary to exercise a right or fulfill an obligation defined in employment rules. Prior to the assessment, employees must be informed in detail, among other things, about what skill or ability the fitness assessment is designed to measure, and what tool or method is used for the assessment. If the assessment is required by law, employees must also be informed of the title and exact section of the legislation. The template for the data processing notice related to this information is included in Annex 3 of this Policy.

(2) Test sheets concerning job aptitude and preparedness may be filled out by employees both before the establishment of employment and during the existence of employment.

(3) Test sheets suitable for psychological or personality trait research may only be filled out by a larger group of employees for the purpose of more efficient performance or organization of workflows clearly related to employment if the data surfaced during the analysis cannot be linked to specific individual employees, i.e., the processing of data occurs anonymously.

(4) Scope of personal data that may be processed: the fact of job fitness and the conditions required for it.

(5) Legal basis for data processing: the legitimate interest of the employer.

(6) Purpose of personal data processing: establishing and maintaining an employment relationship for the given job position.

(7) Recipients of the personal data: the results of the assessment may be disclosed to the assessed employees and the specialist performing the assessment. The employer may only receive information on whether the assessed person is fit for work or not, and what conditions must be provided for this. However, the employer may not access the details of the assessment or its full documentation.

(8) Duration of personal data processing: 3 years following the termination of employment.

3. Processing of Data of Job Applicants, Applications, and CVs

(1) Scope of personal data that may be processed: name, date and place of birth, mother's name, address, qualification data, photograph, phone number, e-mail address of the natural person, and employer notes made about the applicant.

(2) Purpose of personal data processing: assessing the application/candidacy, concluding an employment contract with the selected person. The data subject must be informed if the employer did not choose them for the given position.

(3) Legal basis for data processing: the consent of the data subject.

(4) Recipients or categories of recipients of personal data: the manager entitled to exercise employer rights at the Company, and employees performing labor, personnel, and HR duties.

(5) Retention period of personal data: until the evaluation of the application. Personal data of non-selected applicants must be deleted. The data of persons who withdrew their application or candidacy must also be deleted.

(6) The Company may retain the applications and CVs of non-selected applicants solely based on the explicit, prior, and voluntary consent of the data subject for the purpose of a potential later job offer. The Company requests this consent from the data subject in advance at the time of submitting the application (when sending the CV or applying on the career page). In the absence of consent, the data of the non-selected applicant must be immediately and permanently deleted upon the conclusion of the selection process.

(7) The rules specified in this chapter must be communicated to job applicants in a manner compliant with the provisions of the Regulation and the Info Act.

4. Data Processing Related to Monitoring the Use of Corporate Electronic Mail Accounts

(1) If the Company provides an e-mail account to the employee, the employee may use this e-mail address and account exclusively for their job duties, in order for employees to maintain contact with each other or correspond with clients, other persons, and organizations on behalf of the employer.

(2) The employee may not use the e-mail account for personal or private purposes, and may not store personal or private messages in the account.

(3) The employer is entitled to regularly – every 3 months – monitor the full content and use of the e-mail account, during which the legal basis for data processing is the legitimate interest of the employer. The purpose of the monitoring is to check compliance with the employer's directives regarding the use of the e-mail account, and to check employee obligations (Sections 8 and 52 of the Labor Code).

- (4) The manager of the employer or the person exercising employer rights is entitled to carry out the monitoring.
- (5) Unless the circumstances of the monitoring preclude this possibility, it must be ensured that the employee can be present during the monitoring.
- (6) Prior to the monitoring, the employee must be informed about the employer's interest motivating the check, who may perform the check on behalf of the employer, the rules governing the monitoring (compliance with the principle of gradualism), the course of the procedure, and their rights and options for legal remedy regarding data processing involved in monitoring the e-mail account.
- (7) The principle of gradualism must be applied during the monitoring; thus, it must first be determined from the e-mail address and subject line whether it relates to the employee's job duties and is not for personal purposes. The employer may examine the content of non-personal e-mails without restriction.
- (8) If, contrary to the provisions of this Policy, it can be established that the employee used the e-mail account for personal purposes, the employee must be requested to delete the personal data immediately. In the event of the employee's absence or lack of cooperation, the personal data shall be deleted by the employer at the time of the check. Due to use of the e-mail account contrary to this Policy, the employer may apply labor law consequences against the employee in accordance with effective labor law rules.
- (9) The employee may exercise the rights written in the chapter on data subject rights in this Policy regarding the data processing involved in checking the e-mail account.

5. Data Processing Related to Monitoring Desktop Computers, Notebooks, and Other IT Equipment Used for Work

- (1) Computers, laptops, and tablets provided by the Company to the employee for work purposes may be used by the employee exclusively for performing their job duties; the Company prohibits their private use, and the employee may not process or store any personal data or correspondence on these devices. The employer may check the data stored on these devices. In all other respects, the provisions of Chapter III/4 above apply to the monitoring of these devices and its legal consequences in an unaltered form.

6. Data Processing Related to Monitoring Workplace Internet Usage

- (1) The employee may only view websites related to their job duties; the employer prohibits personal workplace internet usage.
- (2) Internet registrations completed in the name of the Company as a job duty are owned by the Company; identifiers and passwords referring to the Company must be used during registration. If providing personal data is also necessary for registration, the Company is obliged to instruct the employee to delete them upon termination of employment.
- (3) The employer may monitor the employee's workplace internet usage, to which and to the legal consequences of which the provisions of Chapter III/4 apply in an unaltered form.

7. Data Processing Related to Monitoring Corporate Mobile Phone Usage

(1) The employer does not authorize the private use of corporate mobile phones; mobile phones may be used exclusively for work-related purposes. The Company is entitled to check job-related data stored on the mobile phone, as well as company call logs, based on the employer's legitimate interest (Article 6(1)(f) of the Regulation) for the purpose of monitoring the performance of duties.

(2) Since private use is prohibited, private calls may not be made from the company subscription. If the employee verifiably breaches this prohibition and uses the phone for private purposes, the employer is entitled to demand reimbursement of the cost of private calls and apply disadvantageous labor law consequences against the employee under effective labor law rules. During the monitoring, the employer is not entitled to learn call data belonging to the employee's private sphere (e.g., names of called parties, content of personal messages); if such data is detected, the check must be suspended immediately, and the employee must be requested to delete the data.

(3) In all other respects, the provisions of Chapter III/4 apply to the monitoring and its legal consequences in an unaltered form.

8. Data Processing Related to Workplace Entry and Exit

(1) The operator of the reception operating at the Company's registered office (1134 Budapest, Váci str. 49.) and the data controller of the personal data under paragraph (2) is:

Name:	Dunyov Projekt Ingatlanfejlesztő Kft.
Registered Office:	1036 Budapest, Lajos utca 78.
Tax Number:	13826938-2-41
Company Registration Number:	01-09-875299
Representative:	Éva Erdélyi, Managing Director
E-mail:	erdelyie@fercom.hu
Phone Number:	+36 1 250 4910

(2) Scope of personal data that may be processed: name of the natural person, time of entry and exit.

(3) Legal basis for data processing: enforcement of the employer's legitimate interests.

(4) Purpose of personal data processing: asset protection, performance of contract, monitoring compliance with employee obligations.

(5) Recipients of personal data or categories of recipients: the manager entitled to exercise employer rights at the Company, and personnel employed by the Company's asset protection contractor as data processors.

(6) Duration of personal data processing: 6 months.

9. Data Processing Related to the Application of GPS Navigation Systems

- (1) The legal basis for the application of the GPS system is the employer's legitimate interest.
- (2) Purpose of data processing: work organization, logistics, monitoring compliance with employee obligations.
- (3) Data processed: vehicle license plate number, route taken, distance, time of vehicle use.
- (4) Monitoring may only occur during working hours, and the geographical location of employees may not be monitored outside working hours.
- (5) In all other respects, the provisions of Chapter III/4 apply to the monitoring and its legal consequences in an unaltered form.

CHAPTER IV DATA PROCESSING RELATED TO OBLIGATORY (CONTRACTUAL) LEGAL RELATIONSHIPS

1. Processing of Data of Contracting Partners

- (1) On the legal basis of contract performance, for the purpose of concluding, performing, and terminating contracts, and providing contractual discounts, the Company processes the following data of natural persons contracting with it: name, birth name, date of birth, mother's name, address, tax identification number, tax number, sole proprietor or primary producer certificate number, ID card number, address, registered office/site address, phone number, e-mail address, website address, bank account number, customer number (client ID, order number), online identifier (list of customers, suppliers, loyalty lists). This data processing is deemed lawful also if the processing is necessary to take steps at the request of the data subject prior to entering into a contract. Recipients of the personal data: employees of the Company performing customer service tasks, employees performing accounting and tax tasks, and data processors. Retention period of personal data: 5 years following the termination of the contract.
- (2) Prior to commencing data processing, the natural person concerned must be informed that the processing is based on the legal basis of contract performance; this information may also be provided within the contract itself. The data subject must be informed about the transfer of their personal data to a data processor. The text of the data processing clause related to contracts concluded with natural persons is included in Annex 4 to this Policy.

2. Contact Details of Natural Person Representatives of Legal Entity Clients

- (1) Scope of personal data that may be processed: name, address, phone number, e-mail address, online identifier (if any) of the natural person.
- (2) Purpose of personal data processing: performance of the contract concluded with the Company's legal entity partner, business contact.

- (3) Legal basis for data processing: the consent of the data subject.
- (4) Recipients or categories of recipients of personal data: managers of the Company, their deputies, and other employees of the Company performing or involved in partner relations tasks.
- (5) Retention period of personal data: the duration of the business relationship or until the termination of the data subject's capacity as representative/contact person. If the partner company indicates that the natural person concerned no longer handles representation or contact, the Company shall immediately delete their contact details (phone number, e-mail address) from active registries. This provision does not affect the statutory 8-year retention obligation under the Accounting Act for names and signatures appearing on official contracts and accounting documents concluded with the legal entity partner.
- (6) The template for the data collection sheet is included in Annex 5 to this Policy. This declaration must be presented to the data subject by the employee communicating with the client, customer, or supplier, and their consent to the processing of their personal data must be requested by signing the declaration. The declaration must be preserved for the duration of the data processing.

3. Visitor Data Processing on the Company's Website - Information on the Application of Cookies

- (1) Cookies are short data files placed on the user's computer by the visited website. The purpose of cookies is to make the given infocommunication or internet service easier and more convenient. Numerous types exist, but they are generally classified into two large groups. One is the session cookie, which the website places on the user's device only during a specific session (e.g., during security identification for online banking); the other type is the persistent cookie (e.g., language settings of a website), which remains on the computer until the user deletes it. Based on European Commission directives, cookies [unless strictly necessary for the use of the given service] may only be placed on the user's device with the user's permission.
- (2) In the case of cookies not requiring the user's consent, information must be provided during the first visit to the website. It is not necessary for the full text of the cookie notice to appear on the website; it is sufficient if the website operators briefly summarize the essence of the information and refer via a link to the availability of the comprehensive notice.
- (3) In the case of cookies requiring consent, the information may also be linked to the first visit to the website if the data processing involved in the application of cookies already begins upon visiting the page. If the application of the cookie is linked to a function explicitly requested by the user, the information may also appear in connection with utilizing this function. In this case, it is also not required for the full text of the cookie notice to appear on the website; a short summary of the essence of the information and a reference via a link to the availability of the comprehensive notice is sufficient.
- (4) Visitors must be informed about the application of cookies on the website within the privacy notice according to Annex 2. Through this notice, the Company ensures that the visitor can learn at any time before and during the use of the website's information society services which data types the Company processes for which data processing purposes, including the processing of data that cannot be directly linked to the user.

(5) The Company provides an online price quotation request interface for interested parties on the website <https://nobomed.hu>. The legal basis for processing personal data provided during the quotation request (name, e-mail address, phone number, text of message) is Article 6(1)(b) of the Regulation (taking steps at the request of the data subject prior to entering into a contract). The purpose of data processing is compiling and sending the quotation and maintaining contact. Recipients of the data are employees of the Company performing sales and customer service duties, as well as IT data processors. The retention period of personal data is the validity period specified in the quotation, or if no contract is concluded based on the quotation, 1 (one) year from sending the quotation to handle delays in the business decision process. Following the expiry of this period, the data shall be permanently deleted. If a contract is created based on the quotation, the processing of data shall be governed by Section IV/1 of this Policy (Processing of Data of Contracting Partners).

CHAPTER V

DATA PROCESSING BASED ON LEGAL OBLIGATIONS

1. Data Processing for the Purpose of Fulfilling Tax and Accounting Obligations

(1) On the legal basis of fulfilling a legal obligation, for the purpose of fulfilling statutory tax and accounting obligations (accounting, taxation), the Company processes the legally specified data of natural persons entering into a business relationship with it as customers or suppliers. Based on Sections 169 and 202 of Act CXXVII of 2007 on Value Added Tax, the processed data include, in particular: tax number, name, address, tax status; based on Section 167 of Act C of 2000 on Accounting: name, address, designation of the person or organization ordering the economic operation, the signature of the person authorizing and certifying the execution of the order, and depending on the organization, the signature of the controller; on inventory movement documents and cash management documents, the signature of the recipient, on counter-receipts, the signature of the payer; based on Act CXVII of 1995 on Personal Income Tax: sole proprietor certificate number, primary producer certificate number, tax identification number.

(2) The retention period of personal data is 8 years following the termination of the legal relationship providing the legal basis.

(3) Recipients of the personal data: managers of the Company, their deputies, and employees and data processors of the Company performing taxation, accounting, payroll, and social security tasks.

2. Remitter (Employer/Paying Agent) Data Processing

(1) On the legal basis of fulfilling a legal obligation, for the purpose of fulfilling statutory tax and contribution obligations (determining tax, tax advances, contributions, payroll, social security administration), the Company processes the personal data, prescribed by tax laws, of data subjects – employees, their family members, personnel, other beneficiaries – with whom it stands in a remitter relationship (Section 7(31) of Act CL of 2017 on the Rules of Taxation (Art.)). The scope of processed data is defined by Section 50 of the Art., highlighting in particular: the natural person's natural identification data (including previous name and title), gender, nationality, tax identification number, and social security identification number (TAJ number). If tax laws attach legal consequences thereto, the Company may process employees' health data (Section 40 of the Personal Income Tax Act) and trade union membership data (Section 47(2)(b) of the

Personal Income Tax Act) for the purpose of fulfilling tax and contribution obligations (payroll, social security administration).

(2) The retention period of personal data is 8 years following the termination of the legal relationship providing the legal basis.

(3) Recipients of the personal data: employees and data processors of the Company performing taxation, payroll, and social security (remitter) duties.

3. Data Processing for the Purpose of Fulfilling Anti-Money Laundering Obligations

(1) On the legal basis of fulfilling a legal obligation, for the purpose of preventing and combating money laundering and terrorist financing, the Company processes the data, specified in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (Pmt.), of its clients, their representatives, and beneficial owners: a) surname and first name, b) birth surname and first name, c) nationality, d) place and date of birth, e) mother's birth name, f) home address, or in the absence thereof, place of residence, g) type and number of identification document; official address card number, and copies of the presented documents (Section 7).

(2) Recipients of the personal data: the manager of the Company, employees performing duties related to the fulfillment of contractual obligations, the manager of the Company, and the designated person of the Company under the Pmt.

(3) The retention period of personal data is 8 years from the termination of the business relationship or the execution of the transaction order (Section 56(2) of the Pmt.).

CHAPTER VI DATA SECURITY MEASURES

1. Data Security Measures

(1) Regarding all its data processing operations, the Company takes the technical and organizational measures and establishes the procedural rules necessary to comply with the provisions of the Regulation and the Info Act in order to ensure the security of personal data.

(2) The Data Controller protects data through appropriate measures against accidental or unlawful destruction, loss, alteration, damage, unauthorized disclosure, or unauthorized access.

(3) The Company classifies and treats personal data as confidential data. It imposes a confidentiality obligation on employees regarding the processing of personal data, for which the clause according to Annex 6 must be applied. The Company restricts access to personal data by granting authorization levels.

(4) The Company protects IT systems with firewalls and provides them with virus protection.

(5) The Company performs electronic data processing and registration in a manner that complies with data security requirements. The Company ensures that data is accessed only for specific purposes, under controlled conditions, and only by persons who require it to perform their duties.

- (6) During the processing and handling of personal data, the controller and data processor ensure:
- a) the prevention of unauthorized data entry;
 - b) the prevention of use by unauthorized persons using data transmission equipment;
 - c) the verifiability and determinability of which bodies personal data have been or may be transmitted to using data transmission equipment;
 - d) the verifiability and determinability of which personal data were recorded, when, and by whom;
 - e) that a report is prepared on errors occurring during processing and handling.
- (7) To protect personal data, the Company ensures the monitoring of incoming and outgoing electronic communication.
- (8) Documents under active processing or handling may be accessed only by competent administrators; documents containing personnel, payroll, labor, and other personal data must be kept securely locked away.
- (9) Appropriate physical protection of data, data-bearing devices, and documents must be ensured.

CHAPTER VII MANAGEMENT OF PERSONAL DATA BREACHES

1. Definition of Personal Data Breach

- (1) A personal data breach is an event as specified in Chapter I, Section 4, Point 12.
- (2) The most common reported breaches may include, for example: loss of a laptop or mobile phone, insecure storage of personal data (e.g., payroll slips thrown in the trash); insecure transmission of data, unauthorized copying or transmission of client, customer, or partner lists, attacks against the server, website hacking.

2. Management and Remediation of Personal Data Breaches

- (1) Preventing, managing, and complying with relevant legal provisions regarding personal data breaches is the task of the Company's manager.
- (2) Accesses and access attempts must be logged on IT systems and must be continuously analyzed.
- (3) If the Company's employees authorized to perform monitoring detect a personal data breach during their duties, they must immediately notify the Company's manager.
- (4) Employees of the Company are obliged to report to the Company's manager or the person exercising employer rights if they detect a personal data breach or an event indicating one.
- (5) A personal data breach may be reported via the Company's central e-mail address or phone number, through which employees, contracting partners, and data subjects can report the underlying events or security weaknesses.

(6) Upon a personal data breach report, the Company's manager immediately investigates the report, during which the breach must be identified, and it must be decided whether it is a real breach or a false alarm. The following must be investigated and established:

- a. the time and place of the breach occurrence,
- b. description, circumstances, and impacts of the breach,
- c. scope and quantity of data compromised during the breach,
- d. circle of persons affected by the compromised data,
- e. description of measures taken to eliminate the breach,
- f. description of measures taken to prevent, eliminate, or mitigate damage.

(7) Upon the occurrence of a personal data breach, the affected systems, persons, and data must be contained and isolated, and care must be taken to collect and preserve evidence supporting the occurrence of the breach. Following this, the restoration of damages and the re-establishment of lawful operation can begin.

3. Registry of Personal Data Breaches

(1) A registry of personal data breaches must be maintained, containing:

- a) the scope of personal data affected,
- b) the circle and number of persons affected by the personal data breach,
- c) the time of the personal data breach,
- d) the circumstances and impacts of the personal data breach,
- e) measures taken to remedy the personal data breach,
- f) other data specified in the legislation prescribing data processing.

(2) Data concerning personal data breaches in the registry must be preserved for 5 years.

4. Informing the Supervisory Authority about a Personal Data Breach

(1) Based on Article 33(1) of the Regulation, the Controller shall without unreasonable delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is mandatory and is not made within 72 hours, the Controller shall accompany the notification with reasons for the delay.

(2) In the notification under paragraph (1), the Controller shall:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (1)
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(3) Where, it is not possible to provide the information at the same time, the information may be provided later without undue further delay.

(4) The Controller documents any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken.

CHAPTER VIII RIGHTS OF THE DATA SUBJECT

1. The concepts and provisions defined herein contain rules that are fully identical to the terminology and provisions of the Regulation. For the sake of clarity and transparency, this chapter briefly summarizes the rights of the data subject, while detailed information regarding the exercise of these rights is provided in the following chapter. Contact with the Data Controller may be established through the contact details listed under the Company's data.

Right to be informed prior to data processing

The data subject shall have the right to receive information regarding the facts and information related to data processing prior to the commencement of the data processing operations. *(Articles 13–14 of the Regulation)*

Right of access by the data subject

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

Right to rectification

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

Right to erasure (“right to be forgotten”)

1. The data subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay, and the Data Controller shall have the obligation to erase personal data without undue delay where one of the grounds specified in the Regulation applies. *(Article 17 of the Regulation)*

Right to restriction of processing

The data subject shall have the right to obtain from the Data Controller restriction of processing where one of the conditions specified in the Regulation applies. *(Article 18 of the Regulation)*

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Data Controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves

impossible or involves disproportionate effort. The Data Controller shall inform the data subject about those recipients if the data subject requests it. *(Article 19 of the Regulation)*

Right to data portability

Under the conditions set forth in the Regulation, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller without hindrance from the Data Controller to which the personal data have been provided. *(Article 20 of the Regulation)*

Right to object

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

Automated individual decision-making, including profiling

The data subject shall have 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 of the Regulation)*

Restrictions

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

Communication of a personal data breach to the data subject

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

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

The data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the Regulation. *(Article 77 of the Regulation)*

Right to an effective judicial remedy against a supervisory authority

Each natural or legal person shall have 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 of the Regulation)*

Right to an effective judicial remedy against a data controller or processor

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

2. Detailed information on the rights of the data subject**Right to be informed prior to data processing**

The data subject shall have the right to receive information regarding the facts and information related to data processing prior to the commencement of data processing through the contact details provided by the data controller.

A) Information to be provided where personal data are collected from the data subject

(1) Where personal data relating to a data subject are collected from the data subject, the data controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- b) the contact details of the data protection officer, where applicable;
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d) where the processing is based on point (f) of Article 6(1) of the Regulation (pursuit of legitimate interests), the legitimate interests pursued by the data controller or by a third party;
- e) the recipients or categories of recipients of the personal data, if any;
- f) where applicable, the fact that the data controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of the Regulation, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the data controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- b) the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- c) where the processing is based on point (a) of Article 6(1) (consent of the data subject) or point (a) of Article 9(2) (consent of the data subject) of the Regulation, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- d) the right to lodge a complaint with a supervisory authority;

- e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
- f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information referred to in paragraph 2.

(4) Paragraphs 1 to 3 shall not apply where and insofar as the data subject already has the information.
(Article 13 of the Regulation)

B) Information to be provided where personal data have not been obtained from the data subject

(1) Where personal data have not been obtained from the data subject, the data controller shall provide the data subject with the following information:

- a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- b) the contact details of the data protection officer, where applicable;
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d) the categories of personal data concerned;
- e) the recipients or categories of recipients of the personal data, if any;
- f) where applicable, that the data controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of the Regulation, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the data controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- b) where the processing is based on point (f) of Article 6(1) of the Regulation (legitimate interest), the legitimate interests pursued by the data controller or by a third party;
- c) the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- d) where the processing is based on point (a) of Article 6(1) (consent of the data subject) or point (a) of Article 9(2) (consent of the data subject) of the Regulation, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- e) the right to lodge a complaint with a supervisory authority;

- f) from what source the personal data originate, and if applicable, whether it came from publicly accessible sources; and
 - g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (3) The data controller shall provide the information referred to in paragraphs 1 and 2:
- a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
 - b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
 - c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.
- (4) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information referred to in paragraph 2.
- (5) Paragraphs 1 through 4 do not apply if and to the extent that:
- a) the data subject already has the information;
 - b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of the Regulation, or insofar as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the data controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
 - c) the obtaining or disclosure is expressly laid down by Union or Member State law to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
 - d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy. (*Article 14 of the Regulation*)

Right of access by the data subject

- (1) The data subject shall have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
- a) the purposes of the processing;
 - b) the categories of personal data concerned;
 - c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the existence of the right to request from the Data Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f) the right to lodge a complaint with a supervisory authority;
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 of the Regulation relating to the transfer.

(3) The Data Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject. The right to obtain a copy shall not adversely affect the rights and freedoms of others. (*Article 15 of the Regulation*)

Right to erasure (“right to be forgotten”)

(1) The data subject has the right to request that the Data Controller erase personal data concerning him or her without undue delay, and the Data Controller is obligated to erase personal data concerning the data subject without undue delay if any of the following grounds apply:

- a) the personal data are no longer necessary for the purpose for which they were collected or otherwise processed;
- b) the data subject withdraws the consent on which the processing is based pursuant to Article 6(1)(a) or Article 9(2)(a) of the Regulation, and there is no other legal basis for the processing;
- c) the data subject objects to the processing of their personal data pursuant to Article 21(1) of the Regulation, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data must be erased to comply with a legal obligation under Union or Member State law to which the Data Controller is subject;
- f) the personal data were collected in connection with the offering of information society services referred to in Article 8(1) of the Regulation.

(2) Where the Data Controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the Data Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

- (3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
- a) for exercising the right of freedom of expression and information;
 - b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Data Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
 - c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the Regulation;
 - d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - e) for the establishment, exercise or defence of legal claims. *(Article 17 of the Regulation)*

Right to restriction of processing

- (1) The data subject shall have the right to obtain from the Data Controller restriction of processing where one of the following applies:
- a) the accuracy of the personal data is contested by the data subject, for a period enabling the Data Controller to verify the accuracy of the personal data;
 - b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - c) the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
 - d) the data subject has objected to processing pursuant to Article 21(1) of the Regulation pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.
- (2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
- (3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the Data Controller before the restriction of processing is lifted. *(Article 18 of the Regulation)*

Right to data portability

- (1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller without hindrance from the Data Controller to which the personal data have been provided, where:
- a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) of the Regulation, or on a contract pursuant to point (b) of Article 6(1); and
 - b) the processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one Data Controller to another, where technically feasible.

(3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

(4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others. (*Article 20 of the Regulation*)

Right to object

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller) or point (f) (processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party) of Article 6(1) of the Regulation, including profiling based on those provisions. The Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(3) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

(4) At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(5) In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object also by automated means using technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the Regulation, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. (*Article 21 of the Regulation*)

Automated decision-making in individual cases, including profiling

(1) The data subject shall have 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.

(2) Paragraph 1 shall not apply if the decision:

- a) is necessary for entering into, or performance of, a contract between the data subject and a Data Controller;
- b) is authorised by Union or Member State law to which the Data Controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- c) is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the Data Controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Data Controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1) of the Regulation, unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. (*Article 22 of the Regulation*)

Restrictions

(1) Union or Member State law to which the Data Controller or processor is subject may restrict by way of legislative measures the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions are in harmony to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- a) national security;
- b) defence;
- c) public security;
- d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- o) the protection of judicial independence and judicial proceedings;
- g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- i) the protection of the data subject or the rights and freedoms of others;
- j) the enforcement of civil law claims.

(2) Any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- a) the purposes of the processing or categories of processing;
- b) the categories of personal data;
- c) the scope of the restrictions introduced;
- d) the safeguards to prevent abuse or unlawful access or transfer;
- e) the specification of the controller or categories of controllers;
- f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- g) the risks to the rights and freedoms of data subjects; and
- h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

(Article 23 of the Regulation)

Communication of a personal data breach to the data subject

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

(2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3) of the Regulation.

(3) The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- a) the Data Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- b) the Data Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the Data Controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met. *(Article 34 of the Regulation)*

Right to lodge a complaint with a supervisory authority

(1) Without prejudice to any other administrative or non-judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her

habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

(2) The supervisory authority to which the complaint was submitted is required to inform the customer of developments in the proceedings related to the complaint and of its outcome, including the fact that, pursuant to Article 78 of the Regulation, the customer is entitled to seek judicial remedy. (Article 77 of the Regulation)

Right to an effective judicial remedy against a supervisory authority

(1) Without prejudice to other administrative or non-judicial remedies, every natural and legal person is entitled to an effective judicial remedy against a legally binding decision of the supervisory authority that applies to them.

(2) Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority competent pursuant to Article 55 or 56 of the Regulation does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

(4) Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court. (*Article 78 of the Regulation*)

Right to an effective judicial remedy against a data controller or processor

(1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77 of the Regulation, each data subject shall have the right to an effective judicial remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

(2) Proceedings against a Data Controller or a processor shall be brought before the courts of the Member State where the Data Controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the Data Controller or processor is a public authority of a Member State acting in the exercise of its public powers. (*Article 79 of the Regulation*)

CHAPTER IX

SUBMISSION OF REQUESTS BY THE DATA SUBJECT, MEASURES BY THE DATA CONTROLLER

1. Measures based on the request of the data subject

(1) Our Company, as data controller, shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. Where the data subject objects to the processing of their own data, the Company is obliged to examine the request, make a decision, and inform the applicant in writing within a maximum of 25 (twenty-five) days from the submission of the request, in accordance with the provisions of domestic legislation (Info Act).

(2) That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

(3) Where the data subject makes the request by electronic form, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the Data Controller does not take action on the request of the data subject, the Data Controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

(5) Our Company, as Data Controller, shall provide information under Articles 13 and 14 of the Regulation and any communication and any actions taken regarding the rights of the data subject (Articles 15 to 22 and 34 of the Regulation) free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Data Controller may, taking into account the administrative costs of providing the information or communication or taking the action requested:

- a) charge a reasonable fee, or
- b) refuse to act on the request.

(6) Where the Data Controller has reasonable doubts concerning the identity of the natural person making the request, the Data Controller may request the provision of additional information necessary to confirm the identity of the data subject – the Data Controller is entitled to refrain from taking action until its reasonable doubts are credibly and satisfactorily resolved.

CHAPTER X CLOSING PROVISIONS

1. Establishment and amendment of the regulations

The Board of Directors of the Company is entitled to establish and amend this Regulation.

2. Measures regarding the awareness of the regulation

The provisions of this Regulation must be made known to all employees (engaged persons) of the Company, and employment contracts must dictate that compliance and enforcement constitute an

essential job obligation for every employee (engaged person). The template for the employment contract clause is included in Annex 6 of this Regulation.

ANNEXES

- Annex 1:** Data collection sheet - Personal data sheet - for the processing of personal data based on a legal obligation necessary for establishing an employment relationship / Data collection sheet - Personal data sheet - for the processing of personal data based on a legal obligation necessary for establishing an contractual relationship
- Annex 2:** Data Privacy Policy regarding the processing of personal data of natural persons
- Annex 3:** Notice of NoBoMed Zrt. for employees / contracted persons regarding their fitness-for-duty examination
- Annex 4:** Data protection clause for contracts concluded with natural persons
- Annex 5:** Consent declaration for the processing of contact details of natural person representatives of legal entity contracting partners
- Annex 6:** Provision related to the employment contract regarding familiarity with and compliance with the privacy policy and the obligation of confidentiality / For the establishment of a contractual relationship

NoBoMed Private Company Limited by Shares