DATA PROCESSING POLICY

COMPANY NAME:	**FrontEndART Szoftver Kft.**
REGISTERED OFFICE:	6721 Szeged, Szilágyi utca 5-2.
TAX NUMBER:	12702644206
COMPANY REGISTRATION NUMBER:	06-09-007548
REPRESENTED BY:	Anita Csillag, company manager
	(hereinafter: Company)

This Policy contains the internal rules of the Company's data processing activities for the purpose of compliance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - (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).

The establishment and amendment of the Policy falls within the competence of the Company's managing director in office at any time.

Dated: Szeged, 01.04.2024

Dr. Tibor Bakota

Managing Director

TABLE OF CONTENTS

CHAPTER XII - FINAL PROVISIONS

ANNEXES

CHAPTER I
GENERAL PROVISIONS

1.§ Introduction

The Company declares that it carries out its data processing activities - by adopting the appropriate internal rules, technical and organisational measures - in such a way that they comply under all circumstances with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - (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: Regulation) – and with the provisions of Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: Info Act).

2. § Purpose of the Policy

1. The purpose of the Policy is to establish internal rules and lay the foundations for measures that ensure that the Company's activity as controller complies with the provisions of the Regulation and the Info Act.

2. A further purpose of the Policy is to serve as proof by the Company of compliance with the Regulation and with the principles concerning the processing of personal data set out therein (Article 5).

3. § Scope of the Policy

(1) The scope of this Policy extends to the processing by the Company of personal data concerning natural persons.

(2) Sole proprietor, sole proprietorship, and primary producer clients, customers and suppliers shall be regarded as natural persons for the purposes of applying this Policy.

(3) The scope of the Policy does not extend to the processing of personal data concerning legal persons, including the name and form of the legal person, as well as data relating to the contact details of the legal person. (GDPR (14))

4. § Definitions

The definitions applicable for the purposes of this Policy are contained in Article 4 of the Regulation. Accordingly, the main terms are highlighted below:

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

2. "processing": any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated or non-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;

3. "restriction of processing": the marking of stored personal data with the aim of limiting their processing in the future;

4. "profiling": 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;

5. "pseudonymisation": the processing of personal data in such a manner that the personal data can no longer be attributed to a specific natural person 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 cannot be attributed to identified or identifiable natural persons;

6. “filing system”: any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. “controller”: the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of processing are determined by Union or Member State law, the controller or the specific criteria for its designation may also be determined by Union or Member State law;

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

9. “recipient”: the natural or legal person, public authority, agency or any other body to whom or with which the personal data are disclosed, whether or not it is a third party. 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 such data by those public authorities must comply with the applicable data protection rules according to the purposes of the processing;

10. “third party”: the natural or legal person, public authority, agency or any other body other than the data subject, controller, processor or persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. “consent of the data subject”: any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them;

12. “personal data breach”: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed.

CHAPTER II

ENSURING THE LAWFULNESS OF DATA PROCESSING

5. § Data processing based on the consent of the data subject

(1) In the case of consent-based data processing, the consent of the data subject to the processing of their personal data must be requested on the data request form according to Annex 1.

(2) Consent is also deemed to have been given if the data subject ticks a relevant box when viewing the Company’s website, applies technical settings to this effect when using information society services, or makes any other statement or action which, in the given context, clearly indicates the data subject’s consent to the intended processing of their personal data. Silence, a pre-ticked box or inactivity therefore does not constitute consent.

(3) Consent covers all processing activities carried out for the same purpose or purposes. Where processing serves several purposes at the same time, consent must be given for all processing purposes.

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

(5) The Company may 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 the contract.

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

(7) Where personal data were collected with the data subject's consent, unless otherwise provided by law, the controller may process the collected data without further separate consent and even after the withdrawal of the data subject's consent for the purpose of fulfilling a legal obligation applicable to the controller.

(8) The Company makes its general privacy notice according to Annex 2 available to data subjects in the footer of its website. The purpose of this notice is to inform data subjects, in this publicly accessible form, clearly and in detail before the start of processing and during processing of all facts relating to the processing of their data, in particular the purpose and legal basis of processing, the person authorised to carry out the processing and data processing, the duration of processing, whether the personal data of the data subject are processed by the controller pursuant to Section 6 (5) of the Info Act, and who may access the data. The information must also cover the rights and legal remedies of the data subject in relation to the processing. This privacy notice must be made accessible by a separate link at each of the most important data processing steps (for example, in the case of registration, before registration, during the registration process, etc.). Data subjects must be informed of the availability of this notice.

(9) Data processing based on the legal ground of fulfilling a legal obligation is independent of the data subject's consent, as the processing is prescribed by law. In this case, before the start of processing, the data subject must be informed that the processing is mandatory, and before the start of processing the data subject must be informed clearly and in detail of all facts relating to the processing of their data, in particular the purpose and legal basis of processing, the person authorised to carry out the processing and data processing, the duration of processing, whether the personal data of the data subject are processed by the controller on the basis of a legal obligation applicable to it, and who may access the data. The information must also cover the rights and legal remedies of the data subject in relation to the processing. In the case of mandatory processing, the information may also be provided by publishing a reference to the statutory provisions containing the above information.

CHAPTER III

DATA PROCESSING RELATED TO EMPLOYMENT

6. § Labour and personnel records

(1) Only such data may be requested from and recorded concerning employees, and only such occupational medical aptitude tests may be carried out, as are necessary for the establishment, maintenance and termination of employment, and for the provision of social and welfare benefits, and which do not infringe the employee's personal rights.

(2) On the legal basis of the enforcement of the Company's legitimate interests as employer (Article 6(1)(f) of the Regulation), the Company processes the following data of the employee for the purpose of establishing, performing or terminating employment:

1. name
2. birth name,
3. date of birth,
4. mother's name,
5. address,
6. nationality,
7. tax identification number,
8. social security number,
9. telephone number,
10. e-mail address,
11. identity card number,

12. number of the official certificate proving address,
13. bank account number,
14. start and end date of employment,
15. job title,
16. copy of document certifying education and professional qualifications,
17. photograph,
18. curriculum vitae,
19. amount of salary, data relating to salary payment and other benefits,
20. debts to be deducted from the employee's salary on the basis of a final decision or law, or the employee's written consent, and the entitlement thereto,
21. evaluation of the employee's work,
22. manner and reasons for termination of employment,
23. summary of occupational aptitude tests,
24. in the case of private pension fund and voluntary mutual insurance fund membership, the name and identification number of the fund and the employee's membership number,
25. in the case of a foreign employee, passport number; name and number of the document proving entitlement to work,
26. data recorded in protocols concerning accidents suffered by the employee;
27. data recorded by the camera and access control system used at the Company for security and property protection purposes, and by location tracking systems,
28. results and evaluations of the employee's personality, ability and skills assessment tests

(3) Data relating to illness and trade union membership may be processed by the employer only for the purpose of exercising a right or fulfilling an obligation specified in the Labour Code.

(4) Recipients of the personal data: the employer's manager, the person exercising employer's rights, the Company's employees performing labour-related tasks, and processors.

(5) Duration of storage of personal data: 3 years after termination of employment.

(6) Before the start of processing, the data subject must be informed that the processing is based on the Labour Code and on the enforcement of the employer's legitimate interests.

(7) Simultaneously with the conclusion of the employment contract, the employer informs the employee about the processing of their personal data and personal rights by providing the Notice according to Annex 3 of this Policy.

7. § Data processing related to aptitude tests

(1) Only such aptitude test may be applied to an employee as is prescribed by a rule relating to employment, or which is necessary for exercising a right or fulfilling an obligation specified in a rule relating to employment. Before the test, employees must be informed in detail, among other things, of what skill or ability the aptitude test is intended to assess and by what tool or method the test is carried out. If the test is prescribed by law, employees must also be informed of the title of the law and the exact statutory provision. The template privacy notice related to this information is contained in Annex 4 of this Policy.

(2) Test sheets aimed at assessing fitness for work and preparedness may be completed by employees both before the establishment of employment and during the existence of employment.

(3) Scope of personal data that may be processed: the fact of occupational aptitude and the conditions necessary for it.

(4) Legal basis of processing: legitimate interest of the employer.

(5) Purpose of processing personal data: establishment and maintenance of employment, filling a position.

(6) Recipients of personal data, or categories of recipients: the result of the test may be accessed by the examined employee, the specialist conducting the test, the manager entitled to exercise employer's rights, the employee's superior, and the Company's employees performing labour-related tasks.

(7) Duration of processing personal data: 3 years after termination of employment.

8. § Processing of data of employees applying for employment, applications, CVs

(1) Scope of personal data that may be processed: name of the natural person, date and place of birth, mother's name, address, qualification data, photograph, telephone number, e-mail address, curriculum vitae, motivation letter, results and evaluation of completed personality, ability and skills assessment tests, employer's note prepared about the applicant.

(2) Purpose of processing personal data: assessment of application and candidacy, conclusion of an employment contract with the selected person. The data subject must be informed if the employer has not selected them for the given position.

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

(4) Recipients of personal data, or categories of recipients: manager entitled to exercise employer's rights at the Company, employees performing labour-related tasks, processors.

(5) Duration of storage of personal data: until the assessment of the application or candidacy. The personal data of non-selected applicants must be deleted. The data of any person who withdrew their application or candidacy must also be deleted.

(6) The employer may retain applications only on the basis of the data subject's express, unambiguous and voluntary consent, provided that retention is necessary in order to achieve a processing purpose consistent with the law. This consent must be requested from applicants after the recruitment procedure has been closed.

9. § Data processing related to the monitoring of the use of the e-mail account

(1) If the Company provides an e-mail account to the employee, the employee may use this e-mail address and account exclusively for the purposes of their job duties, so that employees may communicate with each other through it or correspond with clients, other persons or organisations on behalf of the employer.

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

(3) The employer is entitled to regularly monitor the entire content and use of the e-mail account – every 3 months - in which case the legal basis of processing is the employer's legitimate interest. The purpose of the monitoring is to check compliance with the employer's provisions on the use of the e-mail account and to check employee obligations (Sections 8 and 52 of the Labour Code).

(4) The employer's manager or the person exercising employer's rights is entitled to carry out the monitoring.

(5) If the circumstances of the monitoring do not exclude this possibility, it must be ensured that the employee may be present during the monitoring.

(6) Before the monitoring, the employee must be informed of the employer interest for which the monitoring is carried out, who may carry out the monitoring on behalf of the employer, under what rules monitoring may take place (observance of the principle of graduality) and what the procedure is, and what rights and legal remedies the employee has in connection with the data processing involved in checking the e-mail account.

(7) During the monitoring, the principle of graduality must be applied; therefore, primarily on the basis of the e-mail address and subject it must be determined whether the e-mail is related 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 instructed to delete the personal data without delay. In the employee's absence or lack of cooperation, the employer deletes the personal data during the monitoring. Due to use of the e-mail account contrary to this Policy, the employer may apply employment law consequences against the employee.

(9) In connection with the data processing involved in checking the e-mail account, the employee may exercise the rights set out in the chapter of this Policy on the rights of the data subject.

10. § Data processing related to the monitoring of computers, laptops, tablets

(1) The computer, laptop or tablet made available by the Company to the employee for work purposes may be used by the employee exclusively for performing their job duties; the Company prohibits private use of these devices, and the employee may not process or store any personal data or correspondence on these devices. The employer may monitor the data stored on these devices. In other respects, the provisions of the above Section 9 apply to the employer's monitoring of these devices and to the legal consequences.

11. § Data processing related to the monitoring of workplace internet use

(1) The employee may only view websites related to their job duties; the employer prohibits workplace internet use for personal purposes.

(2) The Company is the holder of internet registrations carried out in the name of the Company as a job duty; during registration, an identifier and password referring to the Company must be used. If the provision of personal data is also necessary for registration, the Company is obliged to initiate their deletion upon termination of employment.

(3) The employer may monitor the employee's workplace internet use, to which and to the legal consequences of which the provisions of Section 9 apply.

12.§ Data processing related to the monitoring of the use of company mobile phones

(1) The employer does not permit private use of the company mobile phone; the mobile phone may be used only for purposes related to work, and the employer may check the telephone numbers and data of all outgoing calls, as well as the data stored on the mobile phone.

(2) The employee is obliged to notify the employer if they have used the company mobile phone for private purposes. In this case, the monitoring may be carried out by the employer requesting an itemised call statement from the telephone service provider and calling upon the employee to render the called numbers unrecognisable in the document in the case of private calls. The employer may require the employee to bear the costs of private calls.

(3) In other respects, the provisions of Section 9 apply to the monitoring and its legal consequences.

13. § Data processing related to the use of a GPS navigation system

(1) The legal basis for the use of the GPS system is the employer's legitimate interest; its purpose is work organisation, logistics, and monitoring the fulfilment of employee obligations.

(2) Processed data: vehicle registration number, route travelled, distance, time of vehicle use, parking time.

(3) Monitoring may only take place during working hours, and the geographical location of employees may not be monitored outside working hours. In other respects, the provisions of Section 10 apply to employer monitoring and its legal consequences.

14. § Data processing related to workplace entry and exit control

(1) In the case of operating an access control system, information must be displayed on the identity of the controller and the manner of data processing.

(2) Scope of personal data that may be processed: time, place and direction of entry and exit. The Company does not process personal data, as the entry card required for access is not assigned to the employees or other data subjects using it. The Company does not keep records of which entry card is used by whom.

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

(4) Purpose of processing personal data: fire protection, accident prevention and property protection, performance of a contract.

(5) Recipients of personal data, or categories of recipients: manager entitled to exercise employer's rights at the Company, employees of the Company's property protection contractor as processor.

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

15. § Data processing related to workplace camera surveillance

(1) Our Company uses an electronic surveillance system at its registered office, premises and rooms open for customer reception for the protection of human life, physical integrity, personal liberty, business secrets and property protection, which may enable image, sound, or image and sound recording; on this basis, the behaviour of the data subject recorded by the camera is also considered personal data.

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

(3) Notice and information drawing attention to the use of the electronic surveillance system in the given area must be placed in a clearly visible and legible manner, facilitating the information of third persons wishing to appear in the area. The information must be provided with respect to each individual camera. This information includes information on the fact of surveillance carried out by the electronic property protection system, and on the purpose of making and storing image and sound recordings containing personal data recorded by the system, the legal basis of processing, the place of storage of the recording, the duration of storage, the person applying (operating) the system, the scope of persons entitled to access the data, and the provisions concerning the rights of data subjects and the procedure for enforcing them. The template of the information forms Annex 5 of this Policy.

(4) Image and sound recordings of third persons entering the monitored area (clients, visitors, guests) may be made and processed with their consent. Consent may also be given by implied conduct. Implied conduct includes, in particular, where the natural person present enters the monitored area despite the sign and information placed there on the use of the electronic surveillance system.

(5) In the absence of use, recorded footage may be retained for a maximum of 3 (three) working days. Use means where the recorded image, sound, or image and sound recording, as well as other personal data, are intended to be used as evidence in court or other official proceedings.

(6) A person whose right or legitimate interest is affected by the recording of image, sound, or image and sound recording data may, within three working days of the recording of the image, sound, or image and sound recording, request, by proving their right or legitimate interest, that the controller of the data not destroy or delete the data.

(7) An electronic surveillance system may not be used in a room where surveillance may infringe human dignity, especially in changing rooms, showers, lavatories or, for example, in a medical room or the waiting room belonging to it, nor in a room designated for employees to spend their work breaks.

(8) If no one may lawfully stay in the workplace area - in particular outside working hours or on rest days - then the entire workplace area may be monitored (including, for example, changing rooms, lavatories and rooms designated for work breaks).

(9) In addition to those authorised by law, the operating staff, the employer's manager and deputy, and the workplace manager of the monitored area are entitled to view the data recorded by the electronic surveillance system for the purpose of detecting infringements and checking the operation of the system.

CHAPTER IV

DATA PROCESSING RELATED TO CONTRACTS

16. § Processing of contracting partners' data – records of customers and suppliers

(1) On the legal basis of performance of a contract, the Company processes the following data of the natural person contracted with it as customer or supplier for the purpose of concluding, performing and terminating the contract and providing contractual discounts:

1. name,
2. birth name,
3. date of birth,
4. mother's name,
5. address,
6. tax identification number,
7. tax number,
8. sole entrepreneur certificate number,
9. primary producer certificate number,
10. identity card number,
11. address of registered office, premises,
12. telephone number,
13. e-mail address,
14. website address,
15. bank account number,
16. customer number (client number, order number),
17. online identifier (list of customers, suppliers, loyalty lists).

This processing is also considered lawful if the processing is necessary in order to take steps at the request of the data subject prior to the conclusion of the contract. Recipients of the personal data: the Company's employees performing tasks related to customer service, employees performing accounting and taxation tasks, and processors. Duration of storage of personal data: 5 years after termination of the contract.

(2) Before the start of processing, the data subject natural person must be informed that the processing is based on the legal ground of performance of a contract; this information may also be provided in the contract. The data subject must be informed about the transfer of their personal data to a processor. The text of the data processing clause related to a contract concluded with a natural person is contained in Annex 6 of this Policy.

17.§ Contact details of natural person representatives of legal entity clients, customers and suppliers

(1) Scope of personal data that may be processed: name, address, position, telephone number, e-mail address and online identifier of the natural person.

(2) Purpose of processing personal data: performance of the contract concluded with the Company's legal entity partner, business contact; legal basis: consent of the data subject.

(3) Recipients of personal data, or categories of recipients: the Company's employees performing tasks related to customer service.

(4) Duration of storage of personal data: for 5 years after the end of the business relationship or after the data subject's representative status ceases.

(5) The template of the data collection sheet is contained in Annex 7 of this Policy. This declaration must be presented to the data subject by the employee who is in contact with the client, customer or supplier, and the data subject's consent to the processing of their personal data must be requested by having the declaration signed. The declaration must be retained for the duration of the processing.

18.§ Making telephone voice recordings by customer service

The Company does not apply this.

19. § Visitor data processing on the Company's website - Information on the use of cookies

(1) Cookies are short data files placed on the user's computer by the visited website. The purpose of a cookie is to make the given infocommunication or internet service easier and more convenient to use. There are many types, but they can generally be classified into two

large groups. One is the temporary cookie, which the website places on the user's device only during a given session (e.g. during the security identification of internet banking), and the other type is the permanent cookie (e.g. the language setting of a website), which remains on the computer until the user deletes it. Based on the guidelines of the European Commission, cookies [unless they are 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 for the website operators to briefly summarise the essence of the information and refer via a link to the availability of the full 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 associated with the use of cookies begins already when the page is visited. If the use of the cookie is connected to the use of a function specifically requested by the user, the information may also appear in connection with the use of this function. In this case, it is also not necessary for the full text of the cookie notice to appear on the website; a short summary of the essence of the information and a link referring to the availability of the full notice is sufficient.

(4) On the website, the visitor must be informed about the use of cookies in the privacy notice according to Annex 2. With this notice, the Company ensures that the visitor may, before using the information society services of the website and at any time during use, become aware of which types of data the Company processes for which processing purposes, including the processing of data that cannot be directly linked to the user.

20. § Registration on the Company's website

(1) On the website, the registering natural person may give consent to the processing of their personal data by ticking the relevant box. Pre-ticking the box is prohibited.

(2) Scope of personal data that may be processed: the natural person's name (surname, first name), position, telephone number, e-mail address, online identifier.

(3) Purpose of processing personal data:

1. Performance of services provided on the website.
2. Contact by electronic, telephone, SMS and postal inquiry.
3. Providing information on the Company's products, services, contractual terms and conditions, promotions.
4. Sending advertising material electronically.
5. Analysis of website use.

(4) The legal basis of processing is the consent of the data subject.

(5) Recipients of personal data, or categories of recipients: the Company's employees performing tasks related to customer service and marketing activities, and, as processor, employees of the Company's IT service provider performing hosting and operation.

(6) Duration of storage of personal data: until the registration / service exists, or until the withdrawal of the data subject's consent (request for erasure).

21 § Data processing related to newsletter services

(1) On the website, the natural person registering for the newsletter service may give consent to the processing of their personal data by ticking the relevant box. Pre-ticking the box is prohibited. During subscription, the Privacy Notice (Annex 2) must be made available via a link. The data subject may unsubscribe from the newsletter at any time by using the "Unsubscribe" application of the newsletter, or by a written or e-mail statement, which means withdrawal of consent. In such case, all data of the unsubscribing person must be deleted without delay.

(2) Scope of personal data that may be processed: the natural person's name (surname, first name), e-mail address.

(3) Purpose of processing personal data:

1. Sending newsletters concerning the Company's products and services
2. Sending advertising materials

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

(5) Recipients of personal data, or categories of recipients: the Company's employees performing tasks related to customer service and marketing activities, and, as processor, employees of the Company's IT service provider for the purpose of providing hosting and operation.

(6) Duration of storage of personal data: until the newsletter service exists, or until the withdrawal of the data subject's consent (request for erasure).

22. § Community guidelines / Data processing on the Company's Facebook page

(1) The Company maintains a Facebook page for the purpose of introducing and promoting its products and services.

(2) A question asked on the Company's Facebook page shall not be considered an officially submitted complaint.

(3) The Company does not process personal data published by visitors on the Company's Facebook page.

(4) The Facebook Privacy and Terms of Service apply to visitors.

(5) In the case of publication of unlawful or offensive content, the Company may exclude the data subject from members or delete their comment without prior notice.

(6) The Company is not liable for unlawful data content or comments published by Facebook users. The Company is not liable for any error or malfunction arising from the operation of Facebook, or for any problem arising from changes in the operation of the system.

23. § Data processing in the Company's webshop

(1) A purchase made in the webshop operated by the Company constitutes a contract, with regard also to Section 13/A of Act CVIII of 2001 on certain issues of electronic commerce services and information society services, and to Government Decree 45/2014. (II. 26.) on the detailed rules of contracts between consumers and businesses. In the case of a purchase in the webshop, the legal basis of processing is the contract.

(2) The Company, as service provider, may process the natural personal identification data and address necessary for identifying the person registering in or purchasing from the webshop for the purpose of creating the contract for the provision of an information society service, determining its content,

amending it, monitoring its performance, invoicing the fees arising from it, and enforcing related claims, on the legal basis of Section 13/A (1) of Act CVIII of 2001, and may process their telephone number, e-mail address, bank account number and online identifier on the legal basis of consent.

(3) For invoicing purposes, the Company may process the natural personal identification data, address, and data relating to the time, duration and place of use of the service in connection with the use of the information society service, on the legal basis of Section 13/A (2) of Act CVIII of 2001.

(4) Recipients of personal data, or categories of recipients: the Company's employees performing tasks related to customer service and marketing activities; as processor, the employees of the enterprise performing the Company's taxation and accounting tasks for the purpose of fulfilling tax and accounting obligations; the employees of the Company's IT service provider for the purpose of providing hosting and operation; the employees of the courier service with respect to delivery data (name, address, telephone number); and the Company's marketing service provider for the purpose of marketing information.

(5) Duration of processing personal data: until the registration / service exists, or until the withdrawal of the data subject's consent (request for erasure), and in the case of a purchase, for 5 years following the year of purchase.

(6) During purchase in the webshop, the Privacy Notice (Annex 2) must be made available via a link.

24. § Data processing related to the organisation of a prize draw

The Company does not apply this.

25. § Data processing for direct marketing purposes

(1) Unless otherwise provided by a separate law, advertising may be communicated to a natural person as the recipient of advertising by the method of direct approach (direct marketing), in particular by electronic mail or other equivalent means of individual communication - with the exception specified in Act XLVIII of 2008 - only if the recipient of the advertising has given prior, clear and express consent.

(2) Scope of personal data that may be processed by the Company for the purpose of approaching advertising recipients: the natural person's name, address, telephone number, e-mail address, online identifier.

(3) The purpose of processing personal data is to carry out direct marketing activities related to the Company's activity, i.e. the regular or periodic sending of advertising publications, newsletters and current offers in printed (postal) or electronic form (e-mail) to the contact details provided during registration.

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

(5) Recipients of personal data, or categories of recipients: the Company's employees performing tasks related to customer service; as processor, the employees of the Company's IT service provider performing server service and operation; in the case of postal delivery, the employees of the Post; and the Company's marketing service provider for the purpose of marketing information.

(6) Duration of storage of personal data: until withdrawal of consent.

(7) The data request form according to Annex 1 of this Policy may be used for consent to data processing for direct marketing purposes.

CHAPTER V
DATA PROCESSING BASED ON LEGAL OBLIGATION

26. § 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 tax and accounting obligations prescribed by law (bookkeeping, taxation), the Company processes the data specified by law of

natural persons entering into a business relationship with it as customers or suppliers. The processed data, pursuant in particular to Sections 169 and 202 of Act CXXVII of 2017 on value added tax, are: tax number, name, address, tax status; pursuant to Section 167 of Act C of 2000 on accounting: name, address, designation of the person or organisation ordering the economic operation, the person authorising and the person certifying execution of the order, and, depending on the organisation, the signature of the controller; on documents of inventory movements and cash management documents, the signature of the recipient, on counter-receipts, the signature of the payer; pursuant to Act CXVII of 1995 on personal income tax: sole entrepreneur certificate number, primary producer certificate number, tax identification number.

(2) The duration of storage of personal data is 8 years after the legal relationship giving rise to the legal basis ceases.

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

27. § Data processing by the payer

(1) On the legal basis of fulfilling a legal obligation, for the purpose of fulfilling tax and contribution obligations prescribed by law (determination of tax, tax advance, contributions, payroll, social security and pension administration), the Company processes the personal data prescribed by tax laws of data subjects – employees, their family members, persons employed, recipients of other benefits – with whom it has a payer relationship (Section 7 § 31 of Act CL of 2017 on the Rules of Taxation (Art.)). The scope of processed data is determined by Section 50 of the Art., highlighting in particular: the natural personal identification data of the natural person (including previous name and title), gender, nationality, the natural person's tax identification number, social security identification number (TAJ number). If tax laws attach a legal consequence to this, the Company may process employees' health data (Section 40 of the Personal Income Tax Act) and data relating to trade union membership (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 duration of storage of personal data is 8 years after the legal relationship giving rise to the legal basis ceases.

(3) Recipients of personal data: the Company's employees and processors performing taxation, payroll and social security (payer) tasks.

28. § Data processing concerning documents of permanent value under the Archives Act

(1) On the legal basis of fulfilling its legal obligation, the Company processes its documents classified as being of permanent value under Act LXVI of 1995 on public records, public archives and the protection of private archival material (Archives Act), for the purpose of ensuring that the part of the Company's records material of permanent value is preserved intact and in usable condition for future generations. Duration of data storage: until transfer to the public archives.

(2) The Archives Act governs the recipients of personal data and other issues of data processing.

29. § 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 of its clients, their representatives and beneficial owners specified in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (Pmt.): a) in the case of a natural person: a) family and given name, b) family and given name at birth, c) nationality, d) place and date of birth, e) mother's name at birth, f) address, failing this, place of residence, g) type and number of identification document; number of the official certificate proving address, copies of the documents presented. (Section 7).

(2) Recipients of personal data: the Company's employees performing tasks related to customer service, the Company's manager and the person designated by the Company under the Pmt.

(3) Duration of storage of personal data: 8 years from the termination of the business relationship or from the performance of the transaction order. (Pmt. Section 56 (2))

CHAPTER VI
DATA SECURITY MEASURES

30. § Data security measures

(1) In relation to all processing carried out by the Company for all purposes and on all legal bases, the Company is obliged, in the interest of the security of personal data, to take the technical and organisational measures and establish the procedural rules necessary for the enforcement of the Regulation and the Info Act.

(2) The Controller protects the data by appropriate measures against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure or unauthorised access.

(3) The Company classifies and treats personal data as confidential data. It prescribes a confidentiality obligation for employees concerning the processing of personal data, for which the clause according to Annex 10 must be applied. The Company restricts access to personal data by assigning authorisation levels.

(4) The Company protects its IT systems with a firewall and provides them with virus protection.

(5) The Company performs electronic data processing and record-keeping by means of a computer program that complies with the requirements of data security. The program ensures that the data may be accessed only in a purpose-bound manner, under controlled circumstances, and only by those persons who need such access in order to perform their tasks.

(6) During automated processing of personal data, the controller and the processor ensure by further measures:

a) the prevention of unauthorised data entry;

b) the prevention of the use of automated data processing systems by unauthorised persons by means of data transmission equipment;

c) the possibility to check and establish to which bodies personal data have been or may be transmitted using data transmission equipment;

d) the possibility to check and establish which personal data were entered into automated data processing systems, when and by whom;

e) the restorability of installed systems in the event of malfunction; and

f) that a report is prepared on errors occurring during automated processing.

(6) In order to protect personal data, the Company ensures the monitoring of incoming and outgoing electronic communications.

(7) Only the competent administrators may access documents under ongoing work or processing; personnel, payroll and labour documents and other documents containing personal data must be kept securely locked away.

(8) Appropriate physical protection of the data and the devices and documents carrying them must be ensured.

CHAPTER VII

THE COMPANY'S DATA PROCESSOR ACTIVITY

31.§ Data processor activities

The Company performs data processing in respect of the following activities:

5829 - Other software publishing

6201 - Computer programming

6202 - Information technology consultancy

6209 - Other information technology service activities

6311 - Data processing, web hosting service

8559 - Other education n.e.c.

7490 - Other professional, scientific and technical activities n.e.c.

6820 - Rental and operating of own or leased real estate

32. § Provision of guarantees by the data processor

(1) As processor, the Company guarantees – in particular with regard to expertise, reliability and resources – that it implements technical and organisational measures ensuring compliance with the requirements of the Regulation, including the security of processing.

(2) In the course of its activity, the Processor ensures that persons authorised to access the personal data concerned – unless they are otherwise subject to an appropriate confidentiality obligation based on law – undertake a confidentiality obligation with respect to the personal data of which they become aware. The text of the applicable Confidentiality Declaration is contained in Annex 8 of this Policy.

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

(4) The Company has the legal and technical conditions for electronic communication with state bodies.

(5) The Company undertakes to make available to the principal controller all information necessary to demonstrate compliance with the legal provisions relating to the use of a processor.

33. § Obligations and rights of the principal controller

(1) The controller is entitled to check the performance of the contractual activity at the processor.

(2) The controller is responsible for the lawfulness of its instructions relating to the tasks specified in the contract; however, the processor is obliged to notify the controller without delay if an instruction of the controller or its execution would violate the law.

(3) The controller is obliged to inform the data subject natural persons of the processing under this contract and, where required by law, to obtain their consent.

34. § Obligations and rights of our Company as processor

(1) Right of instruction: In the course of its activity, the processor acts exclusively on the basis of the written instructions of the controller.

(2) Confidentiality: In the course of its activity, the processor ensures that persons authorised to access the personal data concerned – unless they are otherwise subject to an appropriate confidentiality obligation based on law – undertake a confidentiality obligation with respect to the personal data of which they become aware.

(3) Data security: Taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons, the processor implements appropriate

technical and organisational measures to guarantee a level of data security appropriate to the degree of risk. The processor takes measures to ensure that natural persons acting under its authority and having access to personal data process such data only in accordance with the controller's instructions, unless Union or Member State law requires them to deviate from this. The processor ensures that only authorised persons may access the stored data through an internal system or by direct access, and only in connection with the purpose of processing. The processor ensures the necessary regular maintenance and development of the devices used. The device storing the data is placed in a closed room with appropriate physical protection, and its physical protection is also ensured. The processor is obliged to use persons with appropriate knowledge and experience in order to perform the tasks specified in the contract. It is also obliged to ensure that the persons it uses are prepared with regard to the data protection legal provisions to be observed, the obligations set out in this contract, and the purpose and manner of data collection.

(4) Use of an additional processor: The processor undertakes to use an additional processor only subject to fulfilment of the conditions specified in the Regulation and the Info Act. In the contract, the controller gives the processor general authorisation to use an additional processor (subcontractor). Before using an additional processor, the processor informs the controller of the identity of the additional processor and of the planned tasks to be performed by the additional processor. If, on the basis of this information, the controller objects to the use of the additional processor, the processor is entitled to use the additional processor only if the conditions specified in the objection are fulfilled. If the processor uses the services of an additional processor for certain specific processing activities carried out on behalf of the controller, it is obliged to conclude a written contract for this purpose and impose on the additional processor the same data protection obligations as those set out in the contract concluded between the controller and the processor, in particular by requiring the additional processor to provide appropriate guarantees for the implementation of appropriate technical and organisational measures and thereby ensuring that the processing complies with the requirements of the Regulation. If the additional processor fails to fulfil its data protection obligations, the processor engaging it shall be fully liable to the controller for the performance of the additional processor's obligations.

(5) Cooperation with the controller:

a) In the course of its activity, our Company as processor assists the controller by all appropriate means in facilitating the exercise of the rights of data subjects and in fulfilling its related obligations.

b) Our Company as processor assists the controller in fulfilling the obligations under Articles 32–36 of the Regulation (Data security, Data Protection Impact Assessment and prior consultation), taking into account the nature of the processing and the information available to the processor.

c) Our Company as processor makes available to the controller all information necessary to demonstrate fulfilment of the obligations specified in Article 28 of the Regulation (Processor), and enables and facilitates audits, including on-site inspections, carried out by the controller or by another auditor mandated by it. In connection with this point, the processor informs the controller without delay if it considers that any instruction of the controller violates the Regulation or Member State or Union data protection provisions.

35.§ General contractual terms and conditions of the Company's data processing activity

(1) The Company concludes a written contract with the principal controller for the data processing activity.

(2) The general contractual terms and conditions of the Company's data processing activity are contained in Annex 9 of this Policy.

(3) The content of the general contractual term must be made known to the other party before conclusion of the contract, and the other party must accept it.

CHAPTER VIII

MANAGEMENT OF DATA PROTECTION INCIDENTS

36. § Definition of a data protection incident

(1) Data protection incident: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed. (Article 4(12) of the Regulation)

(2) The most commonly reported incidents may include, for example: loss of a laptop or mobile phone, insecure storage of personal data (e.g. payslips thrown into the bin), insecure transmission of data, unauthorised copying or transmission of customer and buyer partner lists, server attacks, hacking of the website.

37. § Handling and remedying data protection incidents

(1) Preventing and handling data protection incidents and complying with the relevant legal requirements are the tasks of the Company's manager and the data protection officer.

(2) Accesses and access attempts must be logged on IT systems and continuously analysed.

(3) If the Company's employees authorised to carry out checks detect a data protection incident while performing their tasks, they must notify the Company's manager and the data protection officer without delay.

(4) The Company's employees are obliged to report to the Company's manager and the data protection officer if they detect a data protection incident or an event indicating such incident.

(5) A data protection incident may be reported at the Company's central e-mail address or telephone number, through which employees, contracting partners and data subjects can report the underlying events and security weaknesses.

(6) In the event of a report of a data protection incident, the Company's manager and the data protection officer – involving the IT, financial and operations manager – examine the report without delay; during this, the incident must be identified and it must be decided whether it is a real incident or a false alarm. The following must be examined and established:

a. the time and place of occurrence of the incident,

b. the description, circumstances and effects of the incident,

c. the scope and quantity of data compromised during the incident,

d. the scope of persons affected by the compromised data,

e. description of the measures taken to eliminate the incident,

f. description of the measures taken to prevent, eliminate or mitigate damage.

(7) In the event of a data protection incident, the affected systems, persons and data must be delimited and isolated, and the collection and preservation of evidence supporting the occurrence of the incident must be ensured. Thereafter, restoration of damage and restoration of lawful operation may begin.

38. § Register of data protection incidents

(1) A register must be kept of data protection incidents, containing:

a) the scope of personal data concerned,

b) the scope and number of persons affected by the data protection incident,

c) the time of the data protection incident,

d) the circumstances and effects of the data protection incident,

e) the measures taken to remedy the data protection incident,

f) other data specified in the law prescribing the processing.

(2) Data relating to data protection incidents included in the register must be retained for 5 years.

CHAPTER IX
RIGHTS OF THE DATA SUBJECT

39.§ Summary information on the rights of the data subject

For the sake of clarity and transparency, this point briefly summarises the rights of the data subject, with detailed information on exercising these rights provided in the following chapter.

Right to prior information

The data subject has the right to receive information on the facts and information related to processing before the start of processing. (Articles 13-14 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right of access by the data subject

The data subject has the right to obtain confirmation from the controller as to whether personal data concerning them are being processed and, where such processing is ongoing, the right to access the personal data and related information specified in the Regulation. (Article 15 of the Regulation).

Information on the detailed rules is provided in the following chapter.

Right to rectification

The data subject has the right to have inaccurate personal data concerning them rectified by the controller without undue delay at their request. Taking into account the purpose of processing, the data subject has the right to request the completion of incomplete personal data, including by means of a supplementary statement. (Article 16 of the Regulation).

Right to erasure ("right to be forgotten")

The data subject has the right to have personal data concerning them erased by the controller without undue delay at their request, and the controller is obliged to erase personal data concerning the data subject without undue delay where one of the grounds specified in the Regulation applies. (Article 17 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right to restriction of processing

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

Information on the detailed rules is provided in the following chapter.

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

The controller informs every recipient to whom or with which the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves disproportionate effort. At the data subject's request, the controller informs the data subject of these recipients. (Article 19 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right to data portability

Under the conditions set out in the Regulation, the data subject has the right to receive the personal data concerning them which they have 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 whom the personal data were provided. (Article 20 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right to object

The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on point e) of Article 6(1) of the Regulation (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 point f) (processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party). (Article 21 of the Regulation)

Information on the detailed rules is provided in the following chapter.

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 would produce legal effects concerning them or similarly significantly affect them. (Article 22 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Restrictions

Union or Member State law applicable to the controller or processor may, by legislative measures, restrict the scope of the rights and obligations provided for in Articles 12–22 and Article 34, as well as the rights and obligations provided for in Article 5 insofar as its provisions correspond to the rights and obligations set out in Articles 12–22. (Article 23 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Information to the data subject about a data protection incident

Where the data protection incident is likely to result in a high risk to the rights and freedoms of natural persons, the controller informs the data subject of the data protection incident without undue delay. (Article 34 of the Regulation)

Information on the detailed rules is provided in the following chapter.

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

The data subject has the right to lodge a complaint with a supervisory authority – in particular in the Member State of their habitual residence, place of work or place of the alleged infringement – if the data subject considers that the processing of personal data relating to them infringes the Regulation. (Article 77 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right to an effective judicial remedy against a supervisory authority

Every natural and 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 of the procedural progress or outcome of the complaint lodged. (Article 78 of the Regulation)

Information on the detailed rules is provided in the following chapter.

Right to an effective judicial remedy against the controller or processor

Every data subject has the right to an effective judicial remedy where they consider that their rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with the Regulation. (Article 79 of the Regulation)

Information on the detailed rules is provided in the following chapter.

40.§ Detailed information on the rights of the data subject

Right to prior information

The data subject has the right to receive information on the facts and information related to processing before the start of processing.

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

1. Where personal data relating to the data subject are collected from the data subject, the controller provides the data subject, at the time the personal data are obtained, with all of the following information:

a) the identity and contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purpose of the intended processing of personal data and the legal basis of the processing;

d) in the case of processing based on point f) of Article 6(1) of the Regulation (enforcement of legitimate interest), the legitimate interests pursued by the controller or by a third party;

e) where applicable, the recipients or categories of recipients of the personal data;

f) where applicable, the fact that the 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 transfer referred to in Article 46, Article 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 point 1, the controller, at the time when the personal data are obtained, informs the data subject of the following additional 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 right of the data subject to request from the controller access to and rectification or erasure of personal data concerning them or restriction of processing and to object to such processing, as well as the data subject's right to data portability;

c) where processing is based on point a) of Article 6(1) of the Regulation (consent of the data subject) or point a) of Article 9(2) (consent of the data subject), 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 based on a legal or contractual obligation or is a precondition for entering into a contract, and whether the data subject is obliged to provide the personal data, as well as the possible consequences of failure to provide such data;

f) the existence of automated decision-making referred to in Article 22(1) and (4) of the Regulation, including profiling, and, at least in such 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 controller intends to further process the personal data for a purpose other than that for which the data were collected, prior to that further processing the controller shall inform the data subject of that other purpose and of all relevant additional information referred to in paragraph (2).

4. Paragraphs 1–3 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 the personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
   a) the identity and contact details of the controller and, where applicable, of the controller's representative;
   b) the contact details of the data protection officer, where applicable;
   c) the purpose of the intended processing of the personal data and 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, the fact that the controller intends to transfer personal data to a recipient in a third country or to an international organisation, and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers referred to in Articles 46, 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 point 1, the controller shall provide the data subject with the following additional 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) where processing is based on point f) of Article 6(1) (legitimate interest), the legitimate interests pursued by the controller or by a third party;
   c) the right of the data subject to request from the 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 processing is based on point a) of Article 6(1) (consent of the data subject) or point a) of Article 9(2), 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) the source of the personal data and, where applicable, whether they originate from publicly accessible sources; and
   g) the existence of automated decision-making referred to in Article 22(1) and (4), including profiling, 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 controller shall provide the information referred to in points 1 and 2 as follows:
   a) within a reasonable period after obtaining the personal data, but at the latest within one month, taking into account the specific circumstances of the processing;
   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; or
   c) if disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, prior to that further processing the controller shall inform the data subject of that other purpose and of all relevant additional information referred to in point 2.

5. Paragraphs 1–4 shall not apply where and insofar as:
   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 is likely to

render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides for 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 controller confirmation as to whether or not personal data concerning them 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 right to request from the controller rectification or erasure of personal data or restriction of processing 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 referred to in Article 22(1) and (4), including profiling, 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 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the 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. 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 shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point a) of Article 6(1) or point a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) 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 have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers processing the personal data that the data subject has requested the erasure 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 requiring processing by Union or Member State law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with points h) and i) of Article 9(2) and Article 9(3);

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), 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 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 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 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), pending the verification whether the legitimate grounds of the 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. The controller shall inform the data subject who has obtained restriction of processing pursuant to paragraph 1 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 them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right

to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the processing is based on consent pursuant to point a) of Article 6(1) or point a) of Article 9(2), 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 the right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of this right 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 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 their particular situation, at any time to processing of personal data concerning them which is based on point e) or f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

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 them 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 their right to object 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), the data subject, on grounds relating to their particular situation, shall have the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

(Article 21 of the Regulation)

Automated individual decision-making, 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 them or similarly significantly affects them.

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 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 controller shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their 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), 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 controller or processor is subject may restrict, by way of legislative measures, the scope of the obligations and rights provided for in Articles 12–22 and Article 34, as well as Article 5, in so far as its provisions correspond to the rights and obligations provided for in Articles 12–22, where 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 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;

f) 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, with the exercise of official authority in 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 measures 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) safeguards to prevent abuse or unlawful access or transfer;

e) the specification of the controller or categories of controllers;

f) the storage periods and 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)

Information to the data subject about a data protection incident

1. Where a data protection incident is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the data protection incident to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the data protection incident and shall 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 controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the data protection incident,

in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the 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. Where the controller has not already communicated the data protection incident to the data subject, the supervisory authority, having considered the likelihood of the data protection incident 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 judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to them infringes the Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

(Article 77 of the Regulation)

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, every natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, every data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 or 56 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 decision of the Board within 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 the 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, every data subject shall have the right to an effective judicial remedy where they consider that their rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with the Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has their habitual residence, unless the 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 X

SUBMISSION OF THE DATA SUBJECT'S REQUEST,

MEASURES OF THE CONTROLLER

41. § Measures based on the data subject's request

(1) The Company, as controller, shall inform the data subject without undue delay, but in any case within one month of receipt of the request, of the measures taken following a request relating to the exercise of their rights.

(2) If necessary, taking into account the complexity and number of requests, this period may be extended by a further two months. The 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 means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay, but 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) The Company, as controller, shall provide the information referred to in Articles 13 and 14 of the Regulation and any communication and action taken under Articles 15–22 and 34 free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may, taking into account the administrative costs of providing the information or communication or taking the action requested:

a) charge a fee of HUF 10,000; or

b) refuse to act on the request.

The burden of demonstrating the manifestly unfounded or excessive character of the request shall lie with the controller.

(6) Where the Company, as controller, has reasonable doubts concerning the identity of the natural person making the request, it may request the provision of additional information necessary to confirm the identity of the data subject.

CHAPTER XI

DATA PROTECTION OFFICER

Not applicable.

CHAPTER XII
FINAL PROVISIONS

45. § Establishment and amendment of the Policy

The managing director of the Company is entitled to establish and amend this Policy.

46. § Measures to ensure awareness of the Policy

The provisions of this Policy must be made known to all employees (staff) of the Company, and employment contracts must stipulate that compliance with and enforcement of it is an essential duty of all employees (staff). A template of the relevant employment contract clause is contained in Annex 10 of this Policy.