PRIVACY NOTICE

Name and details of the Data Controller

Company name:	TAXATEAM Könyvelő és Adótanácsadó Korlátolt Felelősségű Társaság
Company's abbreviated name:	TAXATEAM Kft.
Registered office:	HU-6723 Szeged, Római körút 23.
Company registration number:	06 09 029209
Tax number:	32416796-2-06
Statistical number:	32416796-6920-113-06
Website:	https://taxateam.hu/
Email address:	taxateam@taxateam.hu
Telephone number:	+36-30-646-0366
Names of representatives:	Gáspár Szurovecz, Ágnes Brigitta Tóth, Boglárka Anna Hedvicsekné Dóda – managing directors (executive officers) Form of representation: individual
Principal activity:	NACE Rev. 2: 6920 – Accounting, bookkeeping and auditing activities; tax consultancy
Data Protection Officer:	NOT APPOINTED

1. Introduction

The Data Controller undertakes to carry out its activities in compliance with the legislation in force at all times, which, at the date of issuance of this Privacy Notice, are as follows:

- ✓ **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 – GDPR) (Text with EEA relevance),
- ✓ **Act CXII of 2011** on the Right of Informational Self-Determination and on Freedom of Information (Infotv),
- ✓ **Act V of 2013** on the Civil Code (Ptk.),
- ✓ **Act C of 2000** on Accounting,
- ✓ **Act I of 2012** on the Labour Code (Mt.),
- ✓ **Act CLV of 1997** on Consumer Protection (Fogy. tv.),
- ✓ **Act LIII of 2017** on Preventing and Combating Money Laundering and Terrorist Financing (Pmt.),
- ✓ **Act CVIII of 2001** on Electronic Commerce and on Information Society Services (Eker. tv.),
- ✓ **Act CLXV of 2013** on Complaints and Public Interest Disclosures (Pktv.),
- ✓ **Act XLVIII of 2008** on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Grtv.)

The Company informs the Data Subject that, with regard to the processing of his or her personal data, it qualifies as the **DATA CONTROLLER**.

The validity (temporal scope) of this Privacy Notice is indicated on each page in the header. The Data Controller reserves the right to amend this Privacy Notice at any time and to publish a new version on its website. Upon the entry into force of a new version, the previous version shall cease to have effect.

With regard to the previous data protection practices of the Member States and the earlier directive-based regulation, the EU Regulation elevates data protection to a higher level. The regulation essentially lays down principles of data processing concerning the implementation of processing, and establishes additional rules elaborating on these principles.

With regard to the processing of personal data of natural persons, the Data Controller shall take appropriate measures to ensure that all information provided to the Data Subject concerning the processing of personal data is concise, transparent, intelligible and easily accessible, formulated in clear and plain language, and furthermore that the DATA CONTROLLER facilitates the exercise of the rights of the Data Subject.

The Data Controller undertakes to apply appropriate technical and organisational measures, covering the full scope of its data processing activities, taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of processing and the varying likelihood and severity of the risks posed to the rights and freedoms of natural persons.

For the purposes of data protection rules, sole traders, sole proprietorships and private individuals engaged in agricultural primary production shall be regarded as natural persons, and therefore the processing of their data in the course of their economic activity also qualifies as the processing of personal data.

The **DATA PROTECTION MANAGEMENT REGULATIONS** contain the rules applicable to the Company's data processing activities, the standard forms and contractual clauses supporting their application, as well as the data security requirements.
Personal data may be accessed by the Company's employees who have access rights related to the specific purpose of data processing, and by persons performing data processing activities for the Company under service agreements, to the extent defined by the Company and to the degree necessary for the performance of their activities.

Purpose limitation of data processing
Personal data may only be processed for a specified purpose, for the exercise of a right and for the fulfilment of an obligation. At every stage of processing, the Data Controller shall ensure compliance with the purpose of processing; the collection and processing of data shall be fair and lawful.
Only such personal data may be processed as is indispensable for the realisation of the purpose of processing and suitable for achieving that purpose. Personal data may be processed only to the extent and for the duration necessary for the realisation of the purpose.

The Company does not knowingly collect or request personal data concerning children.

The detailed DATA PROTECTION MANAGEMENT REGULATIONS are available at the Company's registered office for consultation by any Data Subject.

2. Information on specific data processing activities
The following information presents the principal data processing activities of the Data Controller, categorised according to the purposes of processing.

1. DESIGNATION OF DATA PROCESSORS

1.1. Designation of the accounting, taxation and payroll Data Processor

Company name:	TAXATEAM Könyvelő és Adótanácsadó Korlátolt Felelősségű Társaság
Company's abbreviated name:	TAXATEAM Kft.
Registered office:	HU-6723 Szeged, Római körút 23.
Company registration number:	06 09 029209
Tax number:	32416796-2-06
Statistical number:	32416796-6920-113-06
Website:	https://taxateam.hu/
Email address:	taxateam@taxateam.hu
Telephone number:	+36-30-646-0366
Names of representatives:	Gáspár Szurovecz, Ágnes Brigitta Tóth, Boglárka Anna Hedvicsekné Dóda – managing directors (executive officers) Form of representation: individual
Principal activity:	NACE Rev. 2: 6920 – Accounting, bookkeeping and auditing activities; tax consultancy
Designation of the Data Processing activity:	Provision of accounting services in compliance with the laws on taxation and accounting regulations
Data Protection Officer:	NOT APPOINTED

1.2. Designation of the Data Processor operating the electronic surveillance and security system

Company name:	TAXATEAM Könyvelő és Adótanácsadó Korlátolt Felelősségű Társaság
Company's abbreviated name:	TAXATEAM Kft.
Registered office:	HU-6723 Szeged, Római körút 23.
Company registration number:	06 09 029209
Tax number:	32416796-2-06
Statistical number:	32416796-6920-113-06
Website:	https://taxateam.hu/
Email address:	taxateam@taxateam.hu
Telephone number:	+36-30-646-0366
Names of representatives:	Gáspár Szurovecz, Ágnes Brigitta Tóth, Boglárka Anna Hedvicsekné Dóda – managing directors (executive officers) Form of representation: individual
Principal activity:	NACE Rev. 2: 6920 – Accounting, bookkeeping and auditing activities; tax consultancy
Designation of the Data Processing activity:	Operation of the electronic surveillance and security system, performance of technical operations related to the processing of image recordings
Data Protection Officer:	NOT APPOINTED

1.3. Designation of the billing service Data Processor

Company name:	Billingo Technologies Zártkörűen Működő Részvénytársaság
Registered office:	1133 Budapest, Árbóc utca 6. I. emelet
Company registration number:	01-10-140802
Tax number:	27926309-2-41
Statistical number:	27926309-6210-114-01
Website:	http://billingo.hu
Email address:	hello@billingo.hu
Telephone number:	+36-1-500-9491
Name of representative:	Albert Sárospataki – Chief Executive Officer (executive

	officer) Form of representation: individual
Principal activity:	NACE Rev. 2: 6210 – Computer programming
Designation of the Data Processing activity:	Issuing of invoices
Data Protection Officer:	Dr Zalán Gyetvai – attorney-at-law adatvedelem@billingo.com

1.4. Designation of the IT (hosting and web service) Data Processor

Company name:	Tárhely.Eu Szolgáltató Korlátolt Felelősségű Társaság
Registered office:	HU-1144 Budapest, Ormánság utca 4. X. em. 241.
Company registration number:	01-09-909968
Tax number:	14571332-2-42
Statistical number:	14571332-6310-113-01
Website:	https://tarhely.eu/
Email address:	support@tarhely.eu
Name of representative:	Zoltán László Kárpáti – Managing Director (executive officer) Form of representation: individual
Principal activity:	NACE Rev. 2: 6310 – Data processing, hosting and related activities
Designation of the Data Processing activity:	Hosting service, storage of personal data
Data Protection Officer:	NOT APPOINTED

1.5. Postal services, delivery, parcel delivery

Company name:	Magyar Posta Zrt.
Registered office:	HU-1138 Budapest, Dunavirág utca 2-6.
Company registration number:	01-10-042463
Tax number:	10901232-2-44
Website:	https://www.posta.hu
Email address:	ugyfelszolgalat@posta.hu
Telephone number:	06-1-767-8282
Email address of the Data Protection Officer:	adatvedelem@posta.hu

2. DESIGNATION OF AN INDEPENDENT DATA CONTROLLER (RECIPIENT)

2.1. Designation of the occupational health service provider (doctor) appointed

Company name:	Dr. Balla Beáta egyéni vállalkozó
Registered office:	HU-6772 Deszk, Tempfli tér 4/A.
Place of business:	HU-6772 Deszk, Magyar utca 32.
Statistical number:	45813849-8621-231-06
Registration number:	5640573
Tax number:	45813849-1-26
Website:	not applicable
Email address:	drballa.praxis@gmail.com
Telephone number:	+36-62-631-744, +36-70-341-2449
Designation of the occupational health physician:	Dr Beáta Balla
Name of representative:	Dr Beáta Balla
Principal activity:	Designation according to ÖVTJ ’25: 862101 – General medical practice
Data Protection Officer:	NOT APPOINTED

3. Information on workplace camera surveillance

As Data Controller, the Company ensures the security of the data it processes and takes all measures necessary to enforce data protection requirements.

The Company, at its registered office **[HU-6723 Szeged, Római krt. 23.]**, operates an electronic surveillance system (**CCTV** = Closed-Circuit Television) 24 hours a day, which also enables image recording [no so-called **PTZ** (Pan-Tilt-Zoom) is applied], for the purposes of protecting human life, physical integrity, personal freedom, trade secrets, preventing infringements, detecting infringements, and safeguarding property. On this basis, the image (conduct) of the Data Subject recorded by the camera shall also be considered personal data. The camera surveillance system **records movements only, and does not record audio material**.

Legal basis for this data processing: the enforcement of the employer's legitimate interests.

The demonstration of the existence of the legitimate interest is the legitimate interest of the Data Controller, which has been presented by **carrying out a balancing of interests test** in relation to the operation of the electronic surveillance system, for the processing of data based on legitimate interest pursuant to Article 6(1)(f) of the GDPR.

The operation of the cameras and the recording of their data are the legitimate interests of the Company.

The Company declares that

- ✓ for the protection of human life and physical integrity,
- ✓ for the prevention and detection of infringements, the apprehension of offenders in the act and the proof of infringements for the protection of property,
- ✓ for the identification of persons entering the Company's premises without authorisation and the recording of the fact of entry,
- ✓ for the documentation of the activities of unauthorised persons remaining on the premises,
- ✓ for the investigation and proof of the circumstances of possible work-related or other accidents

no other method is available, and the use of these technical means is indispensable, while not resulting in a disproportionate restriction of the right to informational self-determination.

The data processing complies with the principle of purpose limitation and fair processing, and does not involve any violation of human dignity.

To facilitate the provision of information to employees and other persons wishing to enter the premises (registered office) (hereinafter: Data Subjects), the Company has placed clearly visible and legible **informative warning signs** in prominent locations, indicating that an electronic surveillance system is in operation in the given area, which also allows for direct monitoring and image recording.
By entering the areas subject to surveillance, clients, visitors and guests acknowledge and accept the fact of camera surveillance.
The Company **displays an annex (Information Notice)**, which forms an integral part of its current Data Protection Management Regulations, in order to ensure that entrants are informed of the use of cameras before entering the area under surveillance.
The field of view of the cameras is not directed at the monitoring or observation of the private activities or behaviour of employees, visitors or clients.

Information has been provided in respect of each individual camera.

In the absence of use, the Company stores and retains the recorded footage for a maximum of **3 (three)** working days.
Use shall be deemed to occur where the recorded image, as well as other personal data, is intended to be used as evidence in court or other official proceedings.

Any person whose right or legitimate interest is affected by the recording of image data may, within three working days from the recording, request – by substantiating his or her right or legitimate interest – that the data not be destroyed or deleted by the Data Controller.
In addition to those authorised by law, the data recorded by the electronic surveillance system may be accessed, for the purpose of detecting infringements and verifying the operation of the system, by the managing directors of the Company or by a person duly authorised by the managing directors.
A record shall be made of any access to the recorded footage (an electronic register containing such data in a verifiable manner shall also qualify as a record), which shall include the date and time of access, the names of the persons accessing the data, and the reason for access. To ensure the security of personal data, the stored data are protected by individual usernames and passwords, and data processing events are logged.

Criteria of proportionality and necessity
The above data processing is made necessary by the legitimate economic interest of the employer and by the protection of employees and guests. The use of workplace cameras is a generally accepted and widespread means of employer monitoring, for which the employer has no other reliable technical alternative.
The use of the workplace electronic surveillance system restricts the employee's rights to privacy, to confidentiality and the protection of personal data, and to his or her image.
Balancing these interests, the employer has decided in favour of the restriction of the employee's personality rights, having regard to the employer's interests in the protection of human life, personal freedom, physical integrity, trade secrets and property.
In favour of the restriction of personality rights is also the fact that the employer's right of direction and monitoring over the employee is regulated by the Labour Code (Mt.) (Section 42(2); Section 11/A(1)), and consequently the employee must in any case expect the fact of monitoring in the workplace (including the use of technical means of monitoring) and the partial restriction of his or her personality rights resulting therefrom.
The proportionality of the restriction of personality rights is ensured by the following measures and requirements of the Data Controller, which must be observed in the course of applying electronic workplace camera surveillance.
The Company does not operate an electronic surveillance system in any premises where monitoring could violate human dignity (such as changing rooms, showers, toilets, or premises designated for employees to spend their breaks).

4. Key definitions set out in the Data Protection Management Regulations

The definitions applicable to the implementation of the Regulations and this Privacy Notice are contained in Article 4 of the referenced EU Regulation.
Accordingly, the key definitions are highlighted as follows:
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, 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;
2) **processing:** 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;
3) **controller:** 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) **processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

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

6) **personal data breach:** 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;

7) **Right to be informed:** The Data Subject shall have the right to be informed of the facts and information relating to data processing prior to the commencement of the processing;

8) **Right of access:** 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 to the related information specified in the Regulation;

9) **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;

10) **Right to erasure ("right to be forgotten"):** 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 set out in the Regulation applies;

11) **Right to data portability:** Under the conditions set out 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 shall 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;

12) **Communication of a personal data breach to the Data Subject:** Where 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;

13) **Right to lodge a complaint with a supervisory authority (right to an 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.

Definitions set out in Section 3 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, as applied in Hungarian legal practice:

1) **data subject:** a natural person identified or identifiable on the basis of any information;

2) **identifiable natural person:** a natural person 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) **personal data:** any information relating to the data subject;

4) **special data:** any data belonging to the special categories of personal data, that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,

or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, and personal data concerning a natural person's sex life or sexual orientation;

5) **criminal personal data:** personal data which arise in connection with a criminal offence or criminal proceedings, either during or prior to such proceedings, at bodies authorised to conduct criminal proceedings or to detect criminal offences, as well as at the penitentiary service, which can be linked to the data subject, together with personal data relating to a criminal record;

6) **data public on grounds of public interest:** any data not falling within the definition of public interest data, the disclosure, accessibility or availability of which is ordered by law on grounds of public interest;

7) **data transfer:** making data available to a specified third party;

8) **disclosure to the public:** making data available to anyone;

9) **data erasure:** rendering data unrecognisable in such a way that their restoration is no longer possible;

10) **data set:** all data processed in a single register;

11) **EEA state:** a Member State of the European Union and any other state party to the Agreement on the European Economic Area, as well as any state whose nationals, under an international treaty concluded between the European Union and its Member States and a state not party to the Agreement on the European Economic Area, enjoy the same legal status as nationals of a state party to the Agreement on the European Economic Area;

12) **third country:** any state that is not an EEA state.

5. Processing of special categories of personal data

The Data Controller does not request or process data belonging to the special categories of personal data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic and biometric data for the purpose of uniquely identifying a natural person, health data, and personal data concerning a natural person's sex life or sexual orientation), except for certain data prescribed by law in the case of an employment relationship.

The Data Controller shall not record any such data that is disclosed to or comes to the knowledge of the Data Controller by any means. If such data enters any system of the Data Controller without its knowledge, it shall be erased from the system without undue delay upon detection.

6. Assessment of the lawfulness of data processing

1) The Data Controller examines the lawfulness of data processing at every stage of its activities and processes only such data, and only for such time, as the purpose and legal basis of which can be demonstrated.

Where the condition for a legal basis ceases to exist, data processing may only continue if the Data Controller can demonstrate an appropriate alternative legal basis.

2) **The legal bases of data processing**, in the order determined by the Data Controller:

a) the processing is necessary for the performance of a contract to which the Data Subject is party; [Article 6(1)(b)]

b) the processing is necessary for compliance with a legal obligation to which the Data Controller is subject; [Article 6(1)(c)]

c) the processing is necessary for the purposes of the legitimate interests pursued by the Data Controller – supported by a balancing of interests; [Article 6(1)(f)]

d) the Data Subject has given consent to the processing of his or her personal data; [Article 6(1)(a)]

3) As a general rule, the method of demonstrating legal bases is in writing; even in the case of a legal basis established by implied conduct, it must be examined whether it can be clearly demonstrated afterwards. In case of doubt, due regard shall be given to considerations of reasonableness and cost-effectiveness, and efforts shall be made to obtain written confirmation of data processing established by implied conduct.

4) With regard to a contracting party to a valid contract, the Data Controller shall, pursuant to Article 6(1)(b) of the Regulation, continue to process the data of the contracting party after the entry into force of the Regulation until the termination of the contract.
5) Following the termination of the contract, the Data Controller shall process data for the purpose of compliance with its legal obligations or for the enforcement of its legitimate interest, for as long as the existence of such obligations or interests can be demonstrated.

7. Data processing activities necessary for the performance of contractual obligations

This section sets out the conditions for data processing necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into such a contract. [Regulation, Article 6(1)(b)]

7.1. Processing of data of a natural person as a contracting party

1) **Purpose of processing:** to provide the Data Subject with appropriate information and support, and to maintain contact for the preparation (e.g. request for quotation, provision of quotation, consultation on the basis of the quotation, acceptance of the quotation), maintenance, performance and proper termination of the contract.
2) **Legal basis of processing:** Where the request for information relates to the conclusion of a contract, a question concerning its maintenance, its amendment or the preparation of its termination, the legal basis of processing is the contract. Where the request for information concerns a purpose outside the contract, the processing is based on voluntary consent.
3) **Recipients of personal data,** categories of recipients: employees of the Data Controller engaged in providing information, preparing contracts and performing contracts.
4) **Scope and purpose of processed data:** name – identification; email address – contact, clarification of request, provision of information; telephone number – contact, clarification of request, provision of information; content of question/request – input data for providing a response.
5) **Categories of data subjects:** all natural persons who contact the Data Controller and request contract-related information/quotation from the Data Controller by providing their personal data.
6) **Duration of processing:** until the contract remains in force, and following its termination, until the expiry of rights arising from the contract on the basis of the legitimate interest of the Data Controller, as well as until the end of the document retention period prescribed by accounting regulations.
7) **Process of data processing:**
a) the Data Subject contacts the Data Controller for the purpose of requesting information/quotation, in a manner of his or her choice (in person, by telephone, by email, or in another form);
b) the Data Controller clarifies the request or requirement with the Data Subject as necessary;
c) the Data Controller provides the requested information/quotation in the manner in which the request was received, or as agreed with the Data Subject;
d) by acceptance of the quotation or by conclusion of a contract established in writing or by implied conduct.

8. Data processing activities necessary for compliance with legal obligations

8.1. Data processing related to the fulfilment of tax and accounting obligations

1) **Purpose of processing:** the processing of documents (invoices, delivery notes, etc.) containing the personal data of natural persons and of the natural person representatives of legal persons who come into contact with the Data Controller as customers or suppliers, on the basis of the relevant and applicable legislation in force at all times. At the time of entry into force of the Regulations, this includes in particular:

a) Act CL of 2017 on the Rules of Taxation (Art.), in particular Section 50;
b) Act CXXVII of 2007 on Value Added Tax (ÁFA tv.), in particular Section 169;
c) Act C of 2000 on Accounting (Szt.), in particular Section 167.

2) **Legal basis of processing:** compliance with a legal obligation to which the Data Controller is subject.
3) **Recipients of personal data, categories of recipients:** employees of the Data Controller performing taxation and accounting administration, and/or Data Processors providing such

services; the employer's executive authorising payments; and the employee or Data Processor carrying out the related verification.
4) **Scope and purpose of processed data:** the data content prescribed by law and the data contained in the documents and reporting forms mandatory for compliance with such obligations, for the purpose of fulfilling the legal obligation.
5) **Categories of data subjects:** all customers and suppliers who come into contact with the Data Controller.
6) **Duration of processing:** 8 years following the economic event.

9. Data processing activities necessary for the enforcement of legitimate interests

9.1. Data processing relating to the natural person representatives of legal person clients

1) **Purpose of processing:** cooperation with the persons designated by the Data Controller's legal person partner, and general business contact with them.
2) **Legal basis of processing:** performance of obligations arising from the contract between the parties.
3) **Recipients of personal data, categories of recipients:** employees of the Data Controller involved in the performance of the contract.
4) **Scope and purpose of processed data:** name – identification; email address – contact; telephone number – contact.
5) **Categories of data subjects:** all natural persons designated as representatives, contact persons or acting persons for the performance of the contract by the legal person contracting with the Data Controller.
6) **Duration of processing:** 5 years following the termination of the contract or the business relationship.
7) **Process of data processing:**
a) the parties specify in the contract the persons designated on both sides as representatives, contact persons or persons acting in the performance;
b) the Data Subjects carry out the tasks imposed on them by the contract, cooperating in these as necessary;
c) they document the events of their cooperation as necessary (memoranda, notes, records, etc.), and archive documents relevant to the performance of the contract.

9.2. Processing of applicants' data in recruitment and selection

1) **Purpose of processing:** the selection of the successful candidate from among the natural persons applying for a job advertisement published by the Data Controller as employer, the notification of both successful and unsuccessful candidates, and the necessary communication related thereto.
2) **Legal basis of processing:** the application is based on voluntary consent, but during the selection process the Data Controller as employer is bound by Act CXXV of 2003 on Equal Treatment and the Promotion of Equal Opportunities (Ebktv.), under which the employer must observe the principle of equal treatment in access to employment, in particular in public job advertisements, recruitment and conditions of employment.
3) **Recipients of personal data, categories of recipients:** employees of the Data Controller engaged in recruitment and selection, and/or a recruitment or headhunting company occasionally commissioned for this purpose, acting as a Data Processor in such capacity, as well as the employer's representative exercising employer's rights on behalf of the Data Controller.
4) **Scope and purpose of processed data:** name – identification; curriculum vitae (including the personal data contained therein) – identification, content evaluated during selection; telephone number – contact; interview records – identification, content evaluated during selection; tests – content evaluated during selection.
5) **Categories of data subjects:** all natural persons who apply for a job advertisement by submitting their curriculum vitae and cover letter.
6) **Duration of processing:** the Data Controller processes the documents related to the application and selection for 3 years from their creation, in view of Section 17 of the applicable and effective Act CXXV of 2003 on Equal Treatment and the Promotion of Equal Opportunities (Ebktv.), which provides that proceedings to examine compliance with the requirement of equal

treatment may be initiated within one year from becoming aware of the infringement and within three years from the occurrence of the infringement. The employer can prove compliance with the requirement of equal treatment in proceedings initiated within this period only if the necessary documents are in its possession. After the expiry of 3 years, the documents are destroyed by the employer.

7) **Process of data processing:**

a) the Data Subject submits his or her application to the Data Controller as employer in the manner specified in the job advertisement;

b) those involved in selection carry out the selection in accordance with the applicable protocol;

c) the manager exercising employer's rights decides on the selected person;

d) the employer informs both the selected and the rejected applicants about the closure of the selection and the outcome relevant to them;

e) if the employer wishes to continue processing the data of a rejected applicant for the purpose of possible future employment, the Data Subject must be invited to make a declaration to that effect. On the basis of such a declaration the Data Subject may be contacted at a later date; in the absence of such a declaration, the applicant may only be considered in the course of a new application submitted in response to a new job advertisement;

f) those conducting the selection archive the documents created during the selection process;

g) in the event of a request from the Equal Treatment Authority, the manager exercising employer's rights and/or the legal representative retrieves the relevant documents from the archive and uses them in the proceedings;

h) after 3 years the employee designated by the employer destroys the documents.

10. Data processing activities based on the consent of the Data Subject

10.1. Customer service activities in person, by telephone and by email

1) The Data Controller carries out customer service activities in person, by telephone and by email. Where the Data Subject receives an appropriate service in person or during the telephone conversation in relation to all of his or her questions, and no personal data of the Data Subject are recorded, no data processing takes place. Where the service can only be provided by calling the Data Subject back or by providing information by email, and the data provided by the Data Subject are recorded by the Data Controller on paper or in electronic form (hereinafter: Call Log), data processing takes place, which is carried out by the Data Controller in accordance with this section.

2) **Purpose of processing:** providing information to Data Subjects in person, by telephone and by email.

3) **Legal basis of processing:** the consent of the Data Subject. Consent shall be deemed to have been given where the Data Subject provides the Data Controller with the data necessary for a call-back, as well as where the Data Subject contacts the Data Controller by email.

4) **Recipients of personal data, categories of recipients:** employees of the Data Controller engaged in providing information.

5) **Scope of processed data:** name – identification; telephone number – contact; email address – contact; date, hour, minute – identification.

6) **Categories of data subjects:** all natural persons who contact the employees of the Data Controller engaged in customer service activities by telephone or by email.

7) **Duration of processing:** the Data Controller deletes emails received at the email address indicated by it, together with the sender's name and email address and any other voluntarily provided personal data, within a maximum of 1 year from the conclusion of the matter.

8) **Process of data processing:**

a) the Data Subject contacts the Data Controller in person, by telephone or by email;

b) the employee of the Data Controller engaged in customer service listens to the Data Subject or interprets the email received;

c) the request or requirement is clarified with the Data Subject as necessary;

d) either a response is provided immediately, or the Data Subject is offered a call-back after obtaining information on the matter, in which case the optimal time for the call-back is agreed, or in the case of email, the expected time for the reply is indicated;

e) where a question or call cannot be answered immediately, the Data Subject's data are recorded in the designated Call Log;

f) the employee engaged in customer service deletes from the register the data recorded in the Call Log in cases closed without a complaint by the Data Subject, within a maximum of 1 year.

10.2. Presence on social media platforms

For the purpose of presenting and promoting its services, the Company **does not maintain** a Facebook, Twitter, LinkedIn, Instagram or any other social media page.

10.3. Complaint handling

1) The purpose of processing is to enable the submission of complaints, to identify the Data Subject and the complaint, to record the data required by law to be mandatorily registered, and to maintain the contact necessary for the investigation and resolution of the complaint.
2) **Legal basis of processing:** the lodging of a complaint is based on voluntary consent, but once a complaint has been made, the processing of the related data is mandatory under Act CLV of 1997 on Consumer Protection (Fgytv.).
3) **Recipients of personal data, categories of recipients:** employees of the Data Controller engaged in complaint handling.
4) **Scope and purpose of processed data:**

- complaint identifier – identification; name – identification;
- date of receipt of the complaint – identification; telephone number – contact;
- time of the call – identification;
- personal data provided during the conversation – identification;
- billing / postal / email address – contact;
- complained product/service/conduct – investigation of the complaint;
- attached documents – investigation of the complaint;
- reason for the complaint – investigation of the complaint;

5) **Categories of data subjects:** all natural persons who wish to submit a complaint, orally or in writing, concerning an ordered or used service/product and/or the conduct, activity or omission of the Data Controller.
6) **Duration of processing:** the Data Controller processes the record of the complaint and the copy of the response **for 3 years** from their recording, as required by Section 17/A (7) of the applicable and effective Act CLV of 1997 on Consumer Protection (Fgytv.).
7) Complaints may be submitted to the Data Controller:

a) by email to taxateam@taxateam.hu, preferably with the word *PANASZ* (complaint) indicated in the subject line; or;
b) by post to **TAXATEAM Kft., HU-6723 Szeged, Római krt. 23.**

A record must be made of complaints submitted orally in person.
8) In accordance with the provisions of the Fgytv., the Data Controller is obliged to provide a substantive written response to a written complaint within thirty (30) days of its receipt, or within any shorter period prescribed by law, and to take measures to communicate it. The Data Controller is obliged to give reasons for its position rejecting the complaint.
9) **Process of data processing:**
a) the Data Subject submits his or her complaint to the Data Controller in a manner of his or her choice;
b) in the case of an oral complaint, the Data Controller records the complaint in writing;
c) the Data Controller examines all the circumstances of the complaint and, on this basis, responds within the time limit;
d) the Data Controller endeavours to resolve the complaint in a manner satisfactory to the complainant.

11. Information for website visitors on the use of cookies

The Data Controller ensures that data processing on the website is technically compliant with these rules. Name of the website concerned:
https://taxateam.hu/
Definitions
Visitor: a natural person who enters the website during browsing.

User: a natural person who contacts the Company via one of the contact details indicated on the website, provides his or her personal data, or uses the services of the website.
The contents published on the Data Controller's website and accessible to anyone may be viewed without providing personal data.
The Data Controller informs visitors to the website that **the website uses cookies**, as they are necessary for its operation.
Further information on the management of cookies can be found on the cookie information page**.**

The privacy policy provides information on what data are collected, for what purpose, and how the Data Subject can update, manage, export and delete his or her data. The Data Controller provides information that its data processing does not extend to the processing carried out by service providers or websites to which links on the Website lead.

12. Access to data

1) The personal data provided by the Data Subject may be accessed by the Data Controller and by the Data Processors identified in Section 2 and in the descriptions of individual processing activities, for the purpose of carrying out their tasks. Personal data are in principle processed by the Data Controller, or, in the case of outsourced activities, by the Data Processors. In such cases, the Data Controller transfers data to the Data Processors, or the latter may access data by the nature of their activities. The Data Controller is responsible for the activities of the Data Processors.
2) The lawyer representing the Data Controller may also have access to the personal data of the Data Subject if court proceedings are initiated on the basis of the Data Subject's submission.
3) The Data Controller transfers personal data to other state authorities only in exceptional cases, namely where,
a) pursuant to legislation on archiving, the Data Controller transfers a case containing the personal data of the Data Subject to the Archives;
b) court proceedings are initiated concerning the Data Subject and the transfer of documents containing the personal data of the Data Subject to the competent court is necessary;
c) the police contact the Authority and request the transfer of documents containing the personal data of the Data Subject for the purposes of an investigation.

13. Data processing activities carried out for another Data Controller

The Company declares that, by virtue of its scope of activities, it performs data processing activities.
The Company's data processing activities must be recorded in writing in a contract relating to data processing.
The content of the contract must be made available to the other party prior to its conclusion and must be accepted by the other party.

14. Data security measures implemented

1) The Data Controller stores the personal data provided by the Data Subject primarily on the servers of the Data Processor(s) specified at the beginning of this Privacy Notice, which are equipped with standard protection systems, and partly on its own IT equipment, and, in the case of paper-based data carriers, securely locked at its registered office. The Data Controller does not use the services of any other third party for the storage of personal data.
2) The Data Controller takes appropriate measures to protect personal data, in particular against unauthorised access or unauthorised alteration.
3) To ensure the security of access to data stored electronically in files or in the cloud, the Data Controller implements strong password protection providing adequate security and updates it at appropriate intervals.
4) The Data Controller ensures that access to its systems is logged and regularly analyses the log data. In the event of any indication of an anomaly, the Data Controller takes the necessary preventive or incident management measures.
5) The Data Controller ensures that passwords are linked to individual users in the course of using the tools and systems in operation, and regularly monitors their use in accordance with the

prescribed requirements. In particular, this includes the prohibition of passwords being used by multiple users, the storage of passwords in a way that makes them inaccessible to others, and the technical prevention, or in the absence thereof, the prohibition of disabling password protection.
6) For electronic data transferred to its Data Processor (e.g. Excel spreadsheets, Word documents, databases stored in the cloud, etc.), the Data Controller also uses the password protection solutions available for the given document, thereby ensuring that the data in the document cannot be accessed by unauthorised persons even if the document should come into their possession.
7) For data stored in analogue form on paper, physical security must also be ensured by providing lockable storage facilities and the secure keeping of keys.
8) In the course of activities, reasonable measures must also be taken to ensure that data stored on paper are not accessible to others (e.g. by using a folder, folding the document, etc.).
9) At the end of daily activities, the Data Controller must allow sufficient time for documents created during the day to be placed in secure storage, inaccessible to unauthorised persons. The Data Controller regularly monitors compliance with this requirement.
10) The Data Controller ensures, through regular training, that the human factor necessary for establishing and maintaining data security is kept at a high level. The training must cover the maintenance of a high level of user responsibility and, through the development of best practices, must make data security an integral part of daily routines (e.g. laptops or telephones containing personal data must not be left in a vehicle or unattended, etc.).
11) The user is obliged to report to the Data Controller any sign, however minor, of abnormal operation.
12) In the course of cooperation with the Data Processor, the Data Controller and the Data Processor mutually ensure that appropriately trained and authorised persons, who are familiar with each other's contact details, are available to take measures relating to data security, to prevent data protection incidents, and, in the event of their occurrence, to take effective measures to mitigate their effects.

15. Measures taken in the event of a data protection incident

15.1. Obligations relating to the prevention of data protection incidents

1) A data protection incident *(a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed)* must be prevented by all reasonable and available means.
2) In the event of an indication of a data protection incident, the Data Controller shall, without undue delay after becoming aware of it, investigate and determine whether a data protection incident has in fact occurred.
3) Even where the case does not qualify as a data protection incident, if conclusions can be drawn from it in the interest of safer future operation, the events must be documented and the Data Controller shall take the necessary measures on that basis.

15.2. Notification of a data protection incident to the supervisory authority

1) The Data Controller shall notify the competent supervisory authority pursuant to Article 55 of any personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2) The Data Processor shall notify the Data Controller of any personal data breach without undue delay after becoming aware of it.
3) The notification of a personal data breach shall, at a minimum, include:
a) a description of 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 data records concerned;
b) the name and contact details of the data protection officer, or other contact point where further information can be obtained;
c) a description of the likely consequences of the personal data breach;

d) a description of the measures taken or proposed by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4) Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided subsequently in phases without undue delay.
5) The Data Controller shall document personal data breaches, indicating the facts relating to the personal data breach, its effects and the remedial measures taken. Such documentation shall enable the supervisory authority to verify compliance with the requirements of this Article.

15.3. Information to the Data Subject about the personal data breach

1) Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the Data Subject of the personal data breach without undue delay.
2) The communication to the Data Subject concerning the personal data breach shall clearly and in plain language describe:
a) 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 data records concerned;
b) the name and contact details of the data protection officer, or other contact point where further information can be obtained;
c) the likely consequences of the personal data breach;
d) the measures taken or proposed by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
3) The Data Subject need not be informed where 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 measures such as encryption, which render the data unintelligible to any person not authorised to access it;
b) the Data Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialise;
c) communication would involve disproportionate effort. In such a case, a public communication shall be made, or a similar measure shall be taken whereby the Data Subjects are informed in an equally effective manner.
4) Where the Data Controller has not yet informed the Data Subject of the personal data breach, the supervisory authority, having considered whether the personal data breach is likely to result in a high risk, may require the Data Subject to be informed or may determine that one of the conditions for exemption from notification has been met.

16. Rights of the Data Subject

Rights relating to data processing
a) Right of access (Article 15 of the EU Regulation)
b) Right to rectification (Article 16 of the EU Regulation)
c) Withdrawal of consent (Article 7(3) of the EU Regulation)
d) Right to erasure (Article 17 of the EU Regulation)
e) Right to restriction of processing (Article 18 of the EU Regulation)
f) Right to data portability (Article 20 of the EU Regulation)
g) Right to object (Article 21 of the EU Regulation)

Detailed information on the rights of Data Subjects can be found on the website of the NAIH (National Authority for Data Protection and Freedom of Information):
https://naih.hu/data-protection/rights-of-data-subjects

16.1. General rules of procedure for the exercise of Data Subjects' rights

1) The Data Controller shall provide the Data Subject with information on the processing of personal data and each communication relating thereto by means of this Privacy Notice, prepared on the basis of its Data Protection and Management Policy, or on the basis thereof, striving to

ensure that it is delivered in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any extract must refer to the full Privacy Notice (attached or made available by means of a link).
2) Information relating to the Data Subject may be provided exclusively to the Data Subject. Where the person requesting the information cannot be identified beyond any reasonable doubt as the Data Subject, the request for information must be refused. In such cases, the person acting on behalf of the Data Controller is obliged to draw up a record accurately documenting the facts, which may serve as a basic document in the handling of a possible complaint.
3) Identification must also be carried out in accordance with the principles set out in Article 5 of the Regulation (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability), and must be performed in accordance with the principle of necessity and sufficiency. (For example, where a request is received from the email address of the Data Subject processed by the Data Controller, no further identification is required.)
4) Where the Data Subject has submitted the request by electronic means, the information shall be provided by electronic means where possible, unless the Data Subject requests otherwise.
5) At the request of the Data Subject, information may also be provided orally, provided that his or her identity has been duly verified.
6) The Data Controller shall inform the Data Subject of the measures taken on the basis of the request without undue delay and at the latest **within one month** of receipt of the request. Where necessary, taking into account the complexity of the request and the number of requests, that period may be extended by a further two months. 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.
7) Where 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 of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
8) The Data Controller shall communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. At the request of the Data Subject, the Data Controller shall inform the Data Subject about those recipients.

16.2. Right to prior information

1) At the time of obtaining the Data Subject's personal data, the Data Controller shall make available to the Data Subject this **Privacy Notice**, which contains the information required under Articles 13 and 14 of the Regulation.
2) The Data Controller shall place the **Privacy Notice** in the header/footer of its website in a form that can be downloaded electronically, and shall also display it at its registered office on paper in a location accessible to Data Subjects.

16.3. Right of access

1) The Data Subject may, in writing and through the contact details of the Data Controller, request information from the Data Controller as to whether it processes his or her personal data and, if so, to be informed of:
a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed;
d) the envisaged period for which the personal data will be stored;
e) where the personal data were not collected from the Data Subject, any available information as to their source;
f) whether the personal data have been transferred to a third country or to an international organisation, and, where this is the case, the appropriate safeguards pursuant to Article 46.
2) The information shall also include notice of the Data Subject's right to request from the Data Controller the rectification or erasure of personal data or restriction of processing concerning him

or her, and to object to such processing, as well as the right to lodge a complaint with a supervisory authority.
3) The Data Controller shall provide the Data Subject with 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.

16.4. 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.

16.5. Right to erasure ("right to be forgotten")

1. The Data Subject may, in writing and through the contact details provided by the Data Controller, request the erasure of his or her personal data where:
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, and there is no other legal ground for the processing;
c) the Data Subject objects to the processing 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) of the Regulation;
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 Data 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) of the Regulation.
2. Where the Data Controller has made the personal data public and is obliged to erase them, it shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform other 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. The Data Controller may refuse erasure where the processing is necessary for the establishment, exercise or defence of legal claims, or in the other cases specified in Article 17(3) of the Regulation.

16.6. 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; in this case, processing shall be restricted pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.
2. Where processing has been restricted pursuant to 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 Data Controller shall inform the Data Subject who has obtained restriction of processing pursuant to paragraph (1) before the restriction of processing is lifted.

16.7. 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 shall 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 the Data Subject's consent or on a contract to which the Data Subject and the Data Controller are parties; and
b) the processing is carried out by automated means.
2. In exercising his or her right to data portability, the Data Subject shall have the right to request, where technically feasible, that the personal data be transmitted directly from one Data Controller to another.
3. The exercise of the right to data portability shall not prejudice the provisions of the Regulation relating to the "Right to erasure." This right shall not apply where the 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.
4. The right to data portability shall not adversely affect the rights and freedoms of others.

16.8. 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 the processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1) of the Regulation, including profiling based on those provisions. In such a case, 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 the 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. The right to object shall be explicitly brought to the attention of the Data Subject at the latest at the time of the first communication, 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 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.

16.9. 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 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 the 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, freedoms and legitimate interests, including 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), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests are in place.

16.10. Restrictions

Union or Member State law to which the Data Controller or Data Processor is subject may, by way of a legislative measure, restrict the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as corresponding provisions in Article 5, in so far as 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 the objectives set out in Article 23 of the Regulation.

17. In the course of processing, we ensure

a) **availability**: we ensure that authorised users have access to the required information and related tools when needed;
b) **confidentiality**: we protect the information so that only those who are authorised may access it;
c) **integrity**: we protect the accuracy and completeness of the information and the methods of its processing.

18. Designation of the Data Protection Officer (DPO)

The Company shall designate a Data Protection Officer in the cases specified in Article 37 of the Regulation. In view of this, the Company is currently not required to designate a Data Protection Officer. The designation of the Data Protection Officer falls within the competence of the managing directors.

19. Remedies available in relation to data processing

If you have submitted a request to the Data Controller for rectification, erasure or restriction of processing, or if you have objected to the processing of your personal data, and we have not complied with your request, you have the right to lodge a complaint with the supervisory authority. If you encounter any problems or believe that your rights have been infringed, you may also contact the Data Controller at the above e-mail address or by telephone. You may initiate proceedings before the National Authority for Data Protection and Freedom of Information (**NAIH**) if you experience a breach of data protection law.

Contact details of the supervisory authority:

National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság – NAIH)
Registered office**:** HU-1055 Budapest, Falk Miksa utca 9–11.
✉ Postal address: HU-1363 Budapest, Pf. 9.
Email: ugyfelszolgalat@naih.hu
Website: https://naih.hu
Telephone: +36 (1) 391-1400
Fax: +36 (1) 391-1410

20. Exercise of rights in relation to data processing

In the event of unlawful data processing experienced by the Data Subject, he or she may bring a civil action against the Data Controller. Such proceedings fall within the jurisdiction of the court. The action may also be brought, at the Data Subject's choice, before the court with jurisdiction over his or her place of residence. The list and contact details of the courts may be consulted via the following link:
https://birosag.hu/en/judicial-system

TAXATEAM Könyvelő és Adótanácsadó Korlátolt Felelősségű Társaság
DATA CONTROLLER