

VIALTO CONSULTING KFT.

PRIVACY NOTICE

**ON THE RIGHTS OF DATA SUBJECTS IN RELATION TO THE PROCESSING OF THEIR
PERSONAL DATA**

TABLE OF CONTENTS

1. INTRODUCTION	3
2. IDENTIFICATION OF THE DATA CONTROLLER	3
3. USE OF DATA PROCESSORS.....	3
4. DATA PROTECTION SUPERVISORY AUTHORITY	4
5. EMPLOYMENT-RELATED DATA PROCESSING	5
6. PROCESSING OF DATA RELATED TO OFFERS, CONTRACTS AND ORDERS	8
7. PROCESSING OF PERSONAL DATA NECESSARY FOR THE PERFORMANCE OF CONTRACTUAL OBLIGATIONS 10	
8. VISITOR DATA PROCESSING ON THE COMPANY'S WEBSITE	10
9. PHOTOGRAPHS AND VIDEO RECORDINGS MADE AT COMPANY EVENTS	11
10. DATA PROCESSING RULES RELATING TO MARKETING AND DIRECT BUSINESS ACQUISITION ACTIVITIES.....	12
11. SOCIAL MEDIA GUIDELINES AND PROCESSING OF DATA ON THE COMPANY'S FACEBOOK, INSTAGRAM AND LINKEDIN PAGES.....	12
12. PROCESSING OF PERSONAL DATA COMMUNICATED TO THE COMPANY BY OTHER MEANS.....	13
13. DATA PROCESSING BASED ON LEGAL OBLIGATIONS	13
14. PROCESSING OF DOCUMENTS OF PERMANENT VALUE UNDER THE ARCHIVES ACT	14
15. TECHNICAL INFORMATION ON DATA PROCESSING	14
16. INFORMATION ON THE RIGHTS OF DATA SUBJECTS	15
17. SUBMISSION OF DATA SUBJECT'S REQUESTS AND MEASURES	17
18. PROCEDURE IN THE EVENT OF A PERSONAL DATA BREACH.....	17

1. INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as Act CXII of 2011 on Informational Self-Determination and Freedom of Information, require Data Controllers to take appropriate measures to provide Data Subjects with prior information concerning the processing of their personal data, in a concise, transparent and intelligible form, and to facilitate the exercise of their rights.

This Privacy Notice is issued in fulfilment of these statutory obligations. It is effective from 15 September 2026 until withdrawn.

2. IDENTIFICATION OF THE DATA CONTROLLER

Issuer of this Privacy Notice and Data Controller:

Data Controller: Vialto Consulting Kft.
Court registration number: 01-09-706440
Tax number: 12849675-2-42.
Address: 1064 Budapest, Izabella utca 62–64, Building D, III/31. Telephone: +36 1 412 44 55
Names of representatives: Csaba Károly Lengyel, Áron Péter Nemes, Imre Hercegh, managing directors
Email: adatkezeles@vialto.hu
Website: www.vialto.hu
hereinafter: the Company, Data Controller

3. USE OF DATA PROCESSORS

Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller (Article 4(8) of the Regulation).

The prior consent of the Data Subject is not required for engaging a Data Processor; however, the Data Subject must be informed. Accordingly, we provide the following information:

The Data Controller engages a Data Processor for the provision of IT services. Details of the Data Processor: ÜR – IT service provider

SPOExpert Kft.
2086 Tinnye
1 Mátyás Király Street

The Data Controller engages a Data Processor for the provision of cloud services. Details of the Data Processor:
<https://www.microsoft.com/hu-hu/>

Microsoft
1031 Budapest, Building M, Graphisoft Park 3.

The Data Controller engages a Data Processor for website development and hosting services. Details of the Data Processor:

<https://www.mhosting.hu/>

Websupport Magyarország Kft.
1119 Budapest, Fehérvári út 97–99.

The Data Controller engages a Data Processor for domain registration services. Details of the Data Processor: Domain registrar, former web hosting provider:

<https://integrity.hu/>

Integrity Kft.
1132 Budapest, Victor Hugo Street 18–22.

The Data Controller engages a Data Processor for accounting and payroll services. Details of the Data Processor:

Separate Inspiráció Kft.
1132 Budapest, Viktor Hugo Street 32, ground floor 2.

The Data Controller may, on an occasional basis, engage a Data Processor for occupational health and fitness-for-work assessment services.

The Company has written agreements with the Data Processors it engages, providing appropriate technical and legal safeguards for the processing of the data transferred.

The Company may also act as a Data Processor in relation to certain services and may engage additional Data Processors authorised by the service recipient. In relation to such services, we always enter into contractual arrangements with service recipients and additional Data Processors in compliance with applicable legislation, defining the relevant legal, technical and organisational safeguards.

4. DATA PROTECTION SUPERVISORY AUTHORITY

The data protection supervisory authority responsible for supervising the Company (hereinafter: the Authority) is the Hungarian National Authority for Data Protection and Freedom of Information (NAIH),

- Address: 1055 Budapest, Falk Miksa Street 9–11.
- Postal address: 1363 Budapest, P.O. Box 9.
- Central telephone number: 1363 Budapest, P.O. Box 9.
- Email address: ugyfelszolgalat@naih.hu

5. EMPLOYMENT-RELATED DATA PROCESSING

5.1 LABOUR AND PERSONNEL RECORDS

- (1) We keep records of our employees and require them to participate only in such fitness-for-work examinations as are necessary for establishing, maintaining or terminating the employment relationship and for providing social and welfare benefits, and which do not infringe the employee's personal rights. Processing in this area is based on the Labour Code and the legitimate interests of the employer.
- (2) For the purposes of establishing, performing or terminating the employment relationship, and on the legal basis of the employer's legitimate interests (Article 6(1)(f) of the Regulation), the Company processes the following employee data:
 - name
 - birth name
 - date of birth
 - mother's name
 - address
 - nationality
 - tax identification number
 - social security identification number (TAJ number)
 - pension identification number (for retired employees)
 - telephone number
 - email address
 - identity card number
 - number of the official address card
 - bank account number
 - online identifier (if applicable)
 - start and end dates of employment
 - position
 - copy of the document certifying educational attainment and professional qualifications
 - copy of the document certifying language skills
 - photograph
 - CV
 - salary amount and data relating to salary payments and other benefits
 - debts to be deducted from the employee's salary on the basis of a final and binding decision, legislation or written consent, and information confirming the entitlement to such deductions
 - employee performance assessment
 - employee's regular working-time report (TR)
 - manner and reasons for termination of employment
 - summary of occupational fitness-for-work examinations and assessments
 - name and identification number of the private pension fund or voluntary mutual insurance fund, and the employee's membership number, where applicable
 - for foreign employees: passport number; name and number of the document certifying the right to work
 - data recorded in reports concerning accidents involving the employee
 - for social purposes, personal data relating to marital status and the names and ages of family members, subject to the employee's consent;
 - for emergency notification purposes, the name and contact details of the person designated by the employee, subject to the employee's consent.

- (3) The Company processes data relating to illness and trade union membership only for the purpose of exercising a right or fulfilling an obligation specified in the Labour Code.
- (4) Recipients of employees' personal data include the head of the employer, who also exercises employer's rights, as well as employees and Data Processors performing labour and personnel-related tasks for the Company.
- (5) In relation to employees' names, professional achievements, CVs, qualifications and language skills, the recipient may also be a legal entity to which the Company submits a business proposal and/or with which it enters into a contract, provided that the request for proposal and/or draft contract, or the proposal itself, contains all conditions ensuring that the personal data transferred are processed by the prospective client and/or contracting partner solely in connection with the relevant transaction and that the data are retained for 5 years following completion of the transaction, unless otherwise provided by law.
- (6) Retention period of personal data: 5 years following termination of employment, unless otherwise provided by law or required by the Company's legitimate interest.

5.2 DATA PROCESSING RELATED TO APTITUDE TESTS

- (1) We will only apply an aptitude test to an employee if it is required by the employment rule or is necessary for the exercise of a right or the performance of an obligation set out in the employment rule. Prior to the examination, the employee will be informed in detail about, among other things, the skills and abilities to be assessed and the means and methods of the examination. If the examination is required by law, employees will be informed of the title of the law and the exact place of legislation.
- (2) The employer may ask employees to fill out test forms for fitness and readiness for work, both before the establishment of employment and during the employment relationship.
- (3) The scope of the personal data that may be processed: the fact of suitability for the job and the conditions required for this.
- (4) Legal basis for processing: legal compliance and/or legitimate interest of the employer.
- (5) Purpose of processing: establishing and maintaining the employment relationship and filling the position.
- (6) Recipients of personal data and categories of recipients:
 - The employees examined and the professional conducting the assessment may access the results of the assessment.
 - The employer receives only information as to whether the person examined is fit for the work and what conditions need to be ensured. The employer may not access the details of the assessment or its complete documentation.
- (7) Retention period of personal data: 5 years following termination of employment.

5.3 PROCESSING OF DATA RELATING TO EMPLOYEE CAREER DEVELOPMENT ASSESSMENTS

- (1) The employer operates a competency assessment system for the regular evaluation of employee career progression, consultant classification and the setting of personal development objectives. The competency assessment covers the employee's professional, consulting, project management and business development competencies, as well as the employee's individual contribution to the Company's operations. The assessment is conducted using an assessment template accessible to all employees, based on the assessed employee's consent and following an explanation of the assessment process.
- (2) Categories of personal data processed: the employee's professional, consulting, project management and business development competencies, individual contribution to the Company's operations, appropriate development directions, and the classification determined on the basis of the assessment.

- (3) Legal basis for processing: compliance with legal requirements, the employee's interests, and the legitimate interest of the employer.
- (4) Purpose of processing: determining the employee's career progression and personal development directions, and determining the employee's opportunities to participate in consulting projects.
- (5) Recipients of personal data and categories of recipients:
 - With regard to detailed assessment data: participants in the assessment (colleagues working with the assessed employee and the employee's mentor), the manager exercising employer's rights, and employees performing HR and personnel-related tasks.
 - With regard to aggregated assessment results: project lead employees; with regard to the classification level achieved: all employees of the Company.
- (6) Retention period of personal data: 5 years following termination of employment.

5.4 PROCESSING OF PERSONAL DATA GENERATED THROUGH AUDIO RECORDINGS DURING WORK

- (1) During electronic or hybrid work meetings, audio recordings may be made for the purpose of preparing accurate minutes based on the recording of essential information, decisions, etc., provided that the following conditions are strictly met.
- (2) Categories of personal data processed: audio recordings of participants' verbal statements and contributions exclusively insofar as they relate to the subject of the work meeting.
- (3) Legal basis for processing: in the case of employees and subcontractors involved in the work, the legitimate interest of the employer or principal. In the case of an external participant, the participant's explicit consent given before recording begins. In addition, the verbal consent of all participants must be obtained before recording starts. Participants must also be given the opportunity to stop or pause the recording during the meeting, including at the request of a single participant.
- (4) Purpose of processing: preparing accurate minutes of the work meeting in a resource-efficient manner. If the recording and preparation of minutes are performed using an artificial intelligence-based system, only a system that provides the required data and information security may be used, does not transfer the recordings to third parties, does not use them for machine learning, processes data within the EEA or in a country covered by an EU Commission adequacy decision (or provides adequate protection based on a completed TIA), and for which the necessary contractual safeguards are in place.
- (5) Audio recordings made during work meetings may not be used for profiling, emotion recognition, biometric identification, employee assessment or any other purpose other than the purpose specified in paragraph (4).
- (6) Secret audio recording is prohibited, whether made by the employer, an employee or an external participant.
- (7) Recipients of the recordings: until the minutes are prepared, the employee preparing the minutes and/or the artificial intelligence-based system; until the minutes are approved, the meeting chair and the person approving the minutes. Thereafter, the audio recording may not be processed, except for the mandatory deletion within 30 days of making the recording.
- (8) Retention period of personal data: after approval of the minutes, the recording must be deleted immediately, but no later than within 30 days after the recording was made.

5.5 PROCESSING OF DATA OF POTENTIAL EMPLOYEES APPLYING FOR A POSITION

- (1) Categories of personal data processed:
 - name
 - date and place of birth
 - mother's name
 - address
 - qualification data

- photograph
 - telephone number
 - email address
 - previous employers
 - CV
 - any references from previous employers
 - information provided by the recruitment (head-hunting) company, provided that the head-hunter has an appropriate personal data processing policy
 - results of interviews, practical exercises and tests related to the intended position during the recruitment process
 - for positions involving higher expectations – subject to the candidate’s explicit consent – the outcome of a psychological assessment: the fact of personal suitability, any risks identified and the employer conditions required to manage such risks.
 - subject to the candidate’s explicit consent, audio or video recordings made during the recruitment interview(s)
 - if the Company also uses an artificial intelligence system in the recruitment process, it shall use only a system and procedure fully compliant with the relevant provisions of the AI Act concerning high-risk systems; the applicant shall always be informed in advance, and the decision shall in all cases be made by the person(s) authorised to make it.
- (2) Purpose of processing: application, assessment of the application, and conclusion of an employment contract with the selected candidate.
 - (3) Legal basis for processing: the Data Subject’s voluntary consent.
 - (4) Recipients of personal data: the manager authorised to exercise employer’s rights at the Company, and employees performing personnel and recruitment tasks.
 - (5) Personal data are retained until the application has been assessed, after which the personal data of unsuccessful applicants are deleted. The Company retains applicants’ personal data beyond this period only on the basis of the applicant’s clear and voluntary consent, for the purpose of potentially contacting the applicant again in the future.

6. PROCESSING OF DATA RELATED TO OFFERS, CONTRACTS AND ORDERS

6.1 DATA PROCESSING OF CONTRACTING PARTNERS – RECORDS OF NATURAL PERSON CUSTOMERS AND SUPPLIERS

For the purposes of concluding, performing and terminating contracts, granting contractual discounts and maintaining business relations, the Company processes the personal data of natural persons who have entered into a contract with the Company as customers or suppliers, on the legal basis of performance of a contract.

- (1) Categories of personal data processed:
 - name
 - birth name
 - date and place of birth
 - mother’s name
 - address
 - tax identification number and/or tax number

- number of entrepreneur's or agricultural producer's certificate
 - identity card number
 - telephone number
 - email address
 - bank account number
 - online identifier
 - in the case of subcontractors intended to be or actually involved in project work:
 - subcontractor's professional CV
 - subcontractor's time records
- (2) The Company stores data of potential subcontractor partners in a database subject to the Data Subject's explicit consent. In order to keep the database up to date, the Company regularly contacts persons included in the database to update their data and professional CVs. To support the selection of a subcontractor for a specific assignment, the Company may use an artificial intelligence system; however, this does not perform profiling within the meaning of the GDPR, but examines the professional experience required for the assignment in the relevant CVs and lists potential subcontractors with the appropriate experience for the decision-maker responsible for the selection. This procedure complies with the relevant provisions of the AI Act.
 - (3) Recipients of personal data are employees performing customer service, supplier partner selection and partner relationship management tasks, as well as employees and Data Processors performing accounting and tax-related tasks for the Company.
 - (4) Retention period of personal data: 5 years following termination of the contract or the Data Subject's explicit consent to inclusion in the potential subcontractor database, unless otherwise provided by law or the Data Subject extends their intention to participate.
 - (5) The legal basis for inclusion in the database is the Data Subject's consent; in all other cases, processing is based on performance of the contract. Such processing is also lawful where it is necessary to take steps at the request of the Data Subject prior to entering into a contract.

6.2 PROCESSING OF DATA OF CONTRACTING PARTNERS – RECORDS OF LEGAL ENTITY CUSTOMERS AND SUPPLIERS

For the purposes of concluding, performing and terminating contracts, granting contractual discounts and maintaining business relations, the Company processes the contact details of natural-person representatives of legal-person clients, customers and suppliers contracted with the Company, on the legal basis of performance of a contract.

- (1) Categories of personal data processed:
 - name of the natural person
 - address
 - telephone number
 - email address
 - position
 - online identifier
- (2) Recipients of personal data are employees and Data Processors performing customer service and supplier partner relationship management tasks for the Company.
- (3) Retention period of personal data: 5 years following termination of the contract, unless otherwise provided by law or required by the Company's legitimate interest (maintaining references and a business partner register).
- (4) Processing of personal data is based on performance of the contract. Such processing is also lawful where it is necessary to take steps at the request of the Data Subject prior to entering into a contract.

- (5) The legal basis for storing reference statements and maintaining records of past, current and potential business partners is the Company's legitimate interest related to its business operations and business development.

7. PROCESSING OF PERSONAL DATA NECESSARY FOR THE PERFORMANCE OF CONTRACTUAL OBLIGATIONS

The Company's core service is providing business management consulting to clients. In the course of this consulting, the Company's employees and subcontractors enter into direct working relationships with the employees of contracting partners. For effective work and communication, the Company processes the contact details of employees of contracting partners.

- (1) Categories of personal data processed:
 - name of the natural person
 - address
 - telephone number
 - email address
 - project role, position
- (2) Recipients of personal data are the Company's employees and subcontractors.
- (3) Retention period of personal data: 5 years following termination of the contract, unless otherwise provided by law or required by the Company's legitimate interest (maintaining references and a business partner register).
- (4) Processing of personal data is based on performance of the contract.
- (5) The legal basis for storing reference statements and maintaining records of past, current and potential business partners is the Company's legitimate interest related to its business operations and business development.

8. VISITOR DATA PROCESSING ON THE COMPANY'S WEBSITE

Information on the use of cookies

In accordance with common internet practice, the Company also uses cookies on its website. Cookies enable the website to recognise the visitor's browser. Cookies may store user preferences (e.g. selected language) and other information. Among other things, they collect information about the visitor and their device and remember the visitor's individual settings.

The cookies used on the Company's website are technically essential session cookies.

The retention period of data processed through these cookies is limited exclusively to the visitor's current visit; at the end of the session or when the browser is closed, this type of cookie is automatically deleted from the visitor's computer.

The legal basis for this processing is Section 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elkertv.).

Purpose of processing: ensuring the proper functioning of the website.

Content requiring registration

- (1) The Company requires registration to access certain professional content on its website. Such content may include, in particular, analyses, studies, research and webinar recordings.
- (2) Categories of data processed in connection with registration:
 - name of the person wishing to access the content (mandatory)
 - occupation of the person wishing to access the content (mandatory)
 - employer of the person wishing to access the content
 - position/job title of the person wishing to access the content
 - work email address of the person wishing to access the content (mandatory)
- (3) The legal basis for processing personal data is the Data Subject's consent, expressly indicated by registration, as well as Vialto Consulting's legitimate interest in identifying persons interested in the relevant professional content and obtaining their contact details.
- (4) Purpose of processing personal data: enabling professional contact; providing information/invitations concerning related content and events; and business development.
- (5) Recipients of personal data: Vialto employees working in the relevant professional area and the marketing team. Vialto Consulting does not use the personal data processed for any other purpose and does not disclose them to other organisations.
- (6) Retention period of personal data: 5 years following registration, unless otherwise provided by law.
- (7) Information on the Data Subject's rights relating to processing is provided in Chapter 14.

9. PHOTOGRAPHS AND VIDEO RECORDINGS MADE AT COMPANY EVENTS

Internal events

The Company organises various internal events to develop its professional and corporate operations. Photographs and/or video recordings may occasionally be made at these events. The Company publishes such recordings on its internal intranet for internal company-building purposes and/or on its publicly accessible website and LinkedIn and/or Facebook and Instagram pages for brand-building purposes.

- (1) Categories of personal data processed:
- (2) individual, small-group or large-group photographs and videos of participating employees
- (3) The legal basis for processing personal data is the Data Subject's written consent given before the recording is made. In the case of individual and small-group recordings, the Data Subject's consent is additionally required before the photograph/recording is published internally or made public.
- (4) Purpose of processing personal data: company building, brand building, event documentation
- (5) Recipients of personal data: the Company's employees and/or the public
- (6) Retention period of personal data: where made public, 1 year from the date the recording was made. Thereafter, archival storage may be possible for the purpose of documenting the Company's history, for the duration of the Company's operations.

Events involving external participants

The Company organises various events involving external participants to develop its professional and corporate operations and to support the development of its partners. Photographs and/or video recordings may occasionally be made at these events. The Company publishes such recordings on its internal intranet and/or, for brand-building purposes, on its publicly accessible website and LinkedIn and/or Facebook pages.

- (7) Categories of personal data processed: individual, small-group or large-group photographs and videos of participants

- (8) The legal basis for processing personal data is the Data Subject's written consent given before the recording is made. In the case of individual and small-group recordings, the Data Subject's consent is additionally required before the photograph/recording is published internally or made public.
- (9) Purpose of processing personal data: brand building, event documentation
- (10) Recipients of personal data: the Company's employees and/or the public
- (11) Retention period of personal data: where made public, 1 year from the date the recording was made. Thereafter, archival storage may be possible for the purpose of documenting the Company's history, for the duration of the Company's operations.

10. DATA PROCESSING RULES RELATING TO MARKETING AND DIRECT BUSINESS ACQUISITION ACTIVITIES

- (1) The Company regularly informs existing and potential business partners about its professional research, conferences presenting research results, events and professional activities. The target groups of such professional information and marketing communications, notifications and invitations are the relevant groups of persons registered on our website, the relevant groups of our LinkedIn partners, and persons included in our Partner database. Our Partner database (HubSpot) can also send automated email messages to selected recipients. To measure email effectiveness (e.g. opens and link clicks) and optimise content, the system may use technical identifiers such as tracking pixels.
- (2) Categories of personal data processed: the Data Subject's email address, the fact that a message has been opened and the fact that a link in the message has been clicked. If the unsubscribe link is clicked, the Data Subject is removed from the group of persons who may be contacted for marketing purposes.
- (3) The legal basis for processing is the Data Subject's consent and the Company's legitimate interest in developing its business communications. The Data Subject has the right to object to such processing at any time via the unsubscribe link at the bottom of the emails or through the individual settings of their email system.
- (4) Retention period of personal data: for as long as the Data Subject remains in the partner database.
- (5) Recipients of personal data: the Company's marketing employees.

11. SOCIAL MEDIA GUIDELINES AND PROCESSING OF DATA ON THE COMPANY'S FACEBOOK, INSTAGRAM AND LINKEDIN PAGES

- (1) The Company maintains Facebook, LinkedIn and Instagram pages for the purpose of introducing and promoting its products and services.
- (2) The Company does not process personal data posted by visitors on its Facebook, LinkedIn and Instagram pages.
- (3) Visitors are subject to the Privacy Policies and Terms of Service of Facebook, Instagram and LinkedIn.

12. PROCESSING OF PERSONAL DATA COMMUNICATED TO THE COMPANY BY OTHER MEANS

- (1) In the course of any other contact, any person may provide the Company with any of their own personal data.
- (2) The purpose of processing is to fulfill the purpose of the contact. The legal basis for processing is the Data Subject's voluntary consent.
- (3) In the case of a minor under 16, data may be provided with the approval of their legal representative. With regard to such approval, we rely on the presumption of the Data Subject's lawful conduct.
- (4) We draw the attention of persons providing data to us that, if they provide personal data other than their own, it is their responsibility to obtain the Data Subject's consent.
- (5) Data are stored until the purpose has been fulfilled or until the Data Subject withdraws their consent (requests deletion), unless legislation requires further retention.
- (6) Recipients of personal data are employees of the Company performing customer service-related tasks.

13. DATA PROCESSING BASED ON LEGAL OBLIGATIONS

Processing of data for the purpose of fulfilling tax and accounting obligations

- (1) On the legal basis of compliance with a legal obligation, the Company processes, for the purpose of fulfilling statutory tax and accounting obligations (accounting and taxation), the data prescribed by law of natural persons who enter into a business relationship with the Company as customers or suppliers. The data processed are, in particular, under Sections 169 and 202 of Act CXXVII of 2017 on Value Added Tax: tax number, name, address and tax status; under Section 167 of Act C of 2000 on Accounting: name, address, identification of the person or organisation ordering the business transaction, the person authorising payment and the person certifying execution of the instruction, and, depending on the organisation, the auditor's signature; on inventory movement documents and cash-handling documents, the signature of the recipient, and on counter-receipts, the signature of the payer; and under Act CXVII of 1995 on Personal Income Tax: entrepreneur's certificate number, agricultural producer's certificate number and tax identification number.
- (2) Retention period of personal data: 8 years following termination of the legal relationship forming the basis for the processing.
- (3) Recipients of personal data: employees and Data Processors performing the Company's tax, accounting, payroll and social security tasks.

Processing in the capacity of a payer

- (4) On the legal basis of compliance with a legal obligation, the Company processes the personal data prescribed by tax legislation of Data Subjects – employees, their family members, persons engaged by the Company and other persons receiving benefits – with whom it has a payer relationship (Section 7(31) of Act CL of 2017 on the Rules of Taxation (Art.)), for the purpose of fulfilling statutory tax and contribution obligations (determining tax, tax advances and contributions, payroll, social security and pension administration). The categories of data processed are specified by Section 50 of the Art., in particular the natural person's natural identification data (including former name and title), sex, nationality, tax identification number and social security identification number (TAJ number). Where tax legislation attaches legal consequences to such data, the Company may process employees' health data (Section 40 of the PIT Act) and data concerning trade union membership (Section 47(2)(b) of the PIT Act) for the purpose of fulfilling tax and contribution obligations (payroll and social security administration).
- (5) Retention period of personal data: 8 years following termination of the legal relationship forming the basis for the processing.

- (6) Recipients of personal data: employees and Data Processors performing the Company's tax, payroll and social security (payer) tasks.

14. PROCESSING OF DOCUMENTS OF PERMANENT VALUE UNDER THE ARCHIVES ACT

- (1) On the legal basis of compliance with a legal obligation, the Company processes its records classified as having permanent value under Act LXVI of 1995 on Public Records, Public Archives and the Protection of Private Archival Materials (Archives Act), for the purpose of ensuring that the permanent-value part of the Company's archival material is preserved intact and in usable condition for future generations. Retention period: until transfer to the public archive.
- (2) The Archives Act governs the recipients of personal data and other matters relating to processing.

15. TECHNICAL INFORMATION ON DATA PROCESSING

- (1) When processing personal data, the Company selects and operates the IT tools used in providing its services in such a way that the processed data are:
- accessible to authorised persons (availability);
 - authentic and appropriately authenticated (authenticity);
 - demonstrably unchanged (data integrity);
 - protected against unauthorised access (confidentiality).
- (2) The Company protects data through appropriate measures against unauthorised access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction.
- (3) The Company ensures the security of processing through appropriate technical and organisational measures providing a level of protection commensurate with the risks arising in connection with processing.
- (4) In the course of processing, the Company
- maintains
 - confidentiality: protects information so that only persons authorised to access it can do so;
 - integrity: protects the accuracy and completeness of the information and the processing methods;
 - ensures availability: ensures that, when an authorised user needs the information, they can actually access the required information and that the related resources are available.
- (5) Data are stored and processed partly using a cloud-based database server.
- (6) Passwords for user accounts are assigned by an authorised employee, who handles them confidentially as required by their employment contract.
- (7) Both the server storing the data and the communication channel between the server and client are protected at multiple levels against unauthorised intrusion. In addition, the server is protected by a strong firewall and software installed to protect against malicious viruses.
- (8) Backups of the data are made at the frequency specified in the agreement with the cloud service provider and are stored by the Company's cloud service provider.

16. INFORMATION ON THE RIGHTS OF DATA SUBJECTS

Right to prior information

The Data Subject has the right to receive information on the facts and circumstances relating to processing before the processing begins. (Articles 13–14 of the Regulation)

Right of access

The Data Subject has the right to obtain confirmation from the Company as to whether personal data concerning them are being processed and, where such processing is taking place, to obtain access to the personal data and the related information specified in the Regulation.

(Article 15 of the Regulation)

Right to rectification

The Data Subject has the right to have the Company rectify inaccurate personal data concerning them without undue delay upon request. Taking into account the purposes of processing, the Data Subject has the right to request completion of incomplete personal data, including by means of providing a supplementary statement.

(Article 16 of the Regulation)

Right to erasure ('right to be forgotten')

The Data Subject has the right to have the Company erase personal data concerning them without undue delay upon request where one of the grounds specified in the Regulation applies.

(Article 17 of the Regulation)

Right to restriction of processing

The Data Subject has the right to request that the Company restrict processing where the conditions specified in the Regulation are met.

(Article 18 of the Regulation)

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

The Company shall inform every recipient to whom 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 Company shall inform them about those recipients.

(Article 19 of the Regulation)

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 the Company in a structured, commonly used and machine-readable format, and has the right to transmit those data to another Data Controller.

(Article 20 of the Regulation)

Right to object

The Data Subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them 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 Data Controller) or point (f) (processing necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party), 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 which relate to the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Data Subject has the right to object at any time to processing of personal data concerning them for such marketing, including profiling to the extent that it is related to direct marketing.

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 has the right to object, on grounds relating to their particular situation, 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 – the Company does not carry out such processing

The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

(Article 22 of the Regulation)

Restrictions

The Data Subject has the right to request that the Data Controller restrict processing where the conditions specified by law are met.

(Article 23 of the Regulation)

Information of the Data Subject about a personal data breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall inform the Data Subject of the personal data breach without undue delay.

(Article 34 of the Regulation)

Right to lodge a complaint with a supervisory authority (right to an 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 they consider that the processing of personal data concerning them infringes the Regulation.

(Article 77 of the Regulation)

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 deal with the complaint or does not inform the Data Subject within three months of the progress or outcome of the complaint.

(Article 78 of the Regulation)

Right to an effective judicial remedy against a Data Controller or Data 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 processing of their personal data in breach of the Regulation.

(Article 79 of the Regulation)

17. SUBMISSION OF DATA SUBJECT'S REQUESTS AND MEASURES

Data Subjects may submit their requests

- in writing to the Company at 1064 Budapest, Izabella utca 62–64, Building D, III/31.
- info@vialto.hu electronically by sending them to our email address: info@vialto.hu.

The Company shall inform the Data Subject of the measures taken following a request to exercise their rights without undue delay and in any event within one month of receipt of the request. Where necessary, taking into account the complexity and number of requests, this period may be extended by a further two months.

If the Company has reasonable doubts concerning the identity of the natural person making the request, it may request additional information necessary to confirm the identity of the Data Subject.

If the Data Controller refuses to comply with the request, the information on the refusal shall include the grounds for the refusal and the Data Subject's available remedies.

The Data Controller shall inform every recipient to whom the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves disproportionate effort.

The Data Subject may lodge a complaint concerning processing with the authority designated by the legislator or with the court having jurisdiction according to their place of residence or habitual residence.

18. PROCEDURE IN THE EVENT OF A PERSONAL DATA BREACH

In the event of a personal data breach, the person detecting the incident shall immediately notify the Company's data protection officer, who shall immediately take measures to minimise the risks of the

incident. Personal data breaches likely to result in a risk to the rights and freedoms of natural persons shall be notified by the Data Controller to the competent supervisory authority pursuant to Article 33(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: GDPR).

The personal data breach shall be notified to the competent supervisory authority without undue delay and, where feasible, no later than 72 hours after the Company becomes aware of the breach.

The Company shall report the personal data breach by completing and submitting the notification form provided by the Authority.

Information of the Data Subject about the personal data breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall inform the Data Subject of the personal data breach without undue delay.

(Article 34 of the Regulation)