TOKEPORTAL

THE CEE CROWD INVEST PORTAL

Privacy Policy

Contents

1.

Based on Act CXII on informational self-determination (hereinafter: **Info Act**) and to ensure the conditions required for compliance with data protection regulations and an adequate level of data processing security in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR), **Tőkeportál Zártkörűen Működő Részvénytársaság** (registered office: H-1095 Budapest, Soroksári út 48., Cg.: 01-10-049519, tax number: 26146951-2-43, hereinafter: **Company** or **Controller**) as data controller accepts to be bound by the content of this Privacy Policy and undertakes an obligation that its data processing relating to its activity complies with the expectations laid down by laws in force.

In all of its data processing activities relating to natural person users in connection with the services provided by the websites operated by the Company www.tokeportal.hu and https://app.tokeportal.hu (hereinafter: "Website") and the user account for accessing the Company's services (hereinafter: "Portal"), the Company acts in accordance with the provisions of this Privacy Policy (hereinafter: Privacy Policy). The data protection guidelines that become relevant in connection with the data processing activities of the Data Controller are continuously available on the website www.tokeportal.hu. By using the Portal and the Website, a person who registers on the Portal accepts to be bound by the provisions of this Privacy Policy.

The Controller is committed to the protection of its clients' and partners' personal data and attaches special importance to respecting the right to informational self-determination. To comply with the data security requirements, the Controller shall ensure the protection and security of the data subjects' data, in particular in the case of unintended or illegal destruction, loss, alteration, unauthorized disclosure of personal data transferred, stored or otherwise processed or access to it based on other statutory provisions.

2. Purpose of the Privacy Policy

The purpose of the Privacy Policy is for the Controller to inform the Data Subjects about how it acts in the course of processing their personal data.

3. Interpretative provisions

Capitalized terms used in this Privacy Policy must be construed to have the meanings specified in this Privacy Policy, which correspond to the terms used in the Info Act and the GDPR.

Controller: The natural person or legal entity or unincorporated organization who/which, independently or together with others, specifies the purpose of data processing, adopts and executes the decisions regarding data processing (including the device used) or commissions a data processor to execute them.

Data processing: Any operation or set of operations executed on the data, regardless of the procedure used, in particular its collection, recording, entry, organization, storage, alteration, use, query, transmission, public disclosure, association or connection, blocking, erasure and destruction, as well as preventing further use of the data, making photo, sound or video records and recording the physical characteristics (e.g. fingerprint or palmprint, DNS sample, iris scan) suitable for identifying the person.

Processor: the natural person or legal entity or unincorporated organization who/which carries out the data processing based on contract, including contracts signed on the basis of legal provisions.

Data processor for the purposes of this Privacy Policy:

1. Dolphio Technologies Kft.

Registered office: H-2016 Leányfalu, Móricz Zs. u. 196
E-mail address: info@dolphio.hu
Website: www.dolphio.hu
Operations performed:

- Operating the Tőkeportál websites
- Implementing developments of the Tőkeportál websites

2. SUM AND SUBSTANCE LIMITED

Registered office: 80 Wood Ln, Central Working White City, London, United Kingdom, W12 0BZ

E-mail address: info@sumsub.com

Website: www.sumsub.com

Operations performed:

- KYC due diligence based on personal identification data and documents
- AML due diligence based on personal identification data and documents

3. Smartsupp.com, s.r.o.

Registered office: Milady Horakove 13, Brno, 602 00, Czech Republic

E-mail address: privacy@smartsupp.com

Website: www.smartsupp.com

Operations performed:

- Provides data in anonymous form for Tokeportal.hu for use of the chat service

4. The Rocket Science Group

Registered office: LLC.675 Ponce de Leon Ave NESuite 5000Atlanta, GA 30308 USA

Operations performed:

- Sending the Controller's newsletters and notification e-mails
- Scope of the transferred data: name, e-mail address.

Data breach: illegal processing of personal data, in particular unauthorized access, alteration, transmission, disclosure, erasure or destruction, or accidental destruction and damage.

Data set: set of data processed in a recording system.

Data transmission: making the data accessible to certain third parties.

Data erasure: making data unrecognizable so that their restoration is no longer possible.

Data subject: a natural person who is or can be identified directly or indirectly based on certain personal data.

GDPR: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Third party: a natural person or legal entity or unincorporated organization who/which is not the data subject, the data controller or data processor.

Third country: every state which is not an EEA state.

Consent: voluntary and specific, properly informed expression of the data subject's intent by which he grants his unequivocal consent to the processing of his personal data, either as a comprehensive operation or certain operations only

Info Act: Act CXII of 2011 on Informational Self-Determination and the Freedom of Information.

Campaign owner: The person defined in the Company's General Terms and Conditions.

Sensitive data: a) data relating to race, nationality, political opinion or party affiliation, religious or other worldview, union membership, sexual life, b) personal data relating to health, addictions, or criminal history.

The Controller does not request and does not process sensitive data. The Controller shall immediately erase from its system any sensitive data that has been disclosed to it or has come into its possession in any way.

Disclosure: making the data accessible to anyone.

Personal data: data which can be associated with the data subject - in particular their name, identification number, one or several pieces of information about their physical, physiological, mental, economic, cultural or social identity -, or conclusions about the data subject which can be drawn from the data.

Objection: the data subject's statement by which it objects to the processing of its personal data and requests termination of data processing and deletion of the data processed.

Website: webpage available on the website www.tokeportal.hu operated by Tokeportal Ltd.

4. Principles of data processing

The Controller solely processes personal data for a pre-defined purpose, to exercise rights and comply with obligations. It records and processes data in a fair and legal manner. The Controller shall make efforts so that only such and so much personal data is processed as is absolutely necessary for achieving the purpose. The Controller solely processes the personal data to the extent and time necessary. Data processed by the Controller is accurate and up-to-date, and the Controller immediately erases or rectifies any inaccurate personal data. The Controller applies adequate technical and organizational measures that ensure adequate security of the personal data, including protection against unauthorized or unlawful processing and against unintended loss, destruction or damage. Data processing activities that fall within the scope of this Privacy Policy are always related to the service provided by the Controller that is or was used by the Data Subject or for use of which it has made contact with the Controller.

Legal basis of the data processing

Personal data may be processed if:

- the Data Subject has consented;
- processing is necessary for the performance of a contract to which the data subject is party;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;
- ordered by the law or a legal decree or decree of a local municipality under authorization granted by the law within the scope specified therein, for purposes based on public interest (mandatory processing).

In the case of mandatory processing, the types of materials to be processed, the purpose and conditions of processing, access to the data, duration of the processing and the controller's identity are specified by the law or decree of the local municipality. Personal data may be processed also if it is impossible to obtain the data subject's consent or it would cause disproportionate expenses and the processing of personal data is required for compliance with a legal obligation of the Company, or to enforce a legitimate interest of the Company or a third party, and enforcement of such interest is proportionate to the legal restrictions associated with the protection of personal data.

If the data subject consents to the recording of his personal data, the Company may process the recorded data without requiring additional consent from the data subject – unless otherwise specified by law - for compliance with a legal obligation of the Company, or to enforce a legitimate interest of the Company or a third party, and enforcement of such interest is proportionate to the limitation of rights associated with the protection of personal data.

Technical background of the processing

The Company stores personal data electronically. In the case of computer-based data storage, the requirements of the information security policy issued by the Chief Executive Officer must be applied to the protection of personal data.

5. General duration of processing

Data provided on a mandatory basis in the course of registration on the Portal and identification required for establishing investor status is processed starting from the registration and account registration and ending with its erasure. In the case of non-mandatory data, the processing takes place from the date when the data is provided until erasure of the data. Alteration or erasure of the data recorded in the course of preliminary identification may be requested by the data subject at the address support@tokeportal.hu.

The provisions above have no impact on compliance with the retention obligations specified by law (e.g. accounting regulations).

6. Processing performed by the Company

6.1. Website

The Website database stores the Data subject's data for the purpose of performing the free services provided upon registration, and the controller is not entitled to transfer it for any advertising use or other purposes in absence of the Data Subject's express consent.

During visits on the Website, we send one or more cookies – small information packages sent from the server to the browser then from the browser to the server on every request directed to the server – to the Data Subject's computer, through which its browser can be identified uniquely. These cookies operate exclusively to improve user experience, automate the access process and to measure the efficiency of our advertising activity. The Data Subject always has the right to prohibit data processing.

6.1.1. Compilation of visitor statistics

The website of the Controller and the information communicated by the Controller can be accessed by any external visitor. During visits on the website, the website's hosting provider records visitor data in order to check website function, prevent abuses and ensure normal operation. The purpose of recording is to collect information about website use, visitor and internet use statistics and analyses. External providers place so-called cookies on the user's computer, which allows them to link the user's current visit to previous visits. The User can block cookie requests any time in the pop-up window on the webpage.

The scope of processed data:

- date of access,
- time of access,
- IP address of the user's computer,
- IP address of page visited,
- IP address of page previously visited,
- data of the user's operating system and browser.

Under Section 5 of the Info Act, the legal basis for processing is the Data subjects' voluntary consent.

6.1.2. Cookies

Cookies collect information about visitors and their devices, they remember the visitors' individual settings that is or may be used for example when using online transactions, which means they do not need to be typed again, they make Website use easier and ensure a high-quality user experience.

To ensure a personalized service, a small data package, a so-called cookie is placed on the User's computer and read during later visits. If the browser returns a previously saved cookie, the service provider that manages the cookie can link the user's current visit with the previous visits, but only in what concerns its own content.

- Mandatory session cookies

The purpose of these cookies is for users to be able to browse the Website fully and smoothly, to use its functions and the services available there. Such cookies are valid until the session (browsing) is ended, and once the browser is closed, cookies of this type are automatically deleted from the computer or other devices used for browsing.

- Third-party (analytics) cookies

The Website uses the cookies of Google Analytics ("Google") as third-party cookies. Using the Google Analytics statistical service, the website uses Google Inc's Google Analytics system to analyze visitor flow. The Google Analytics system stores so-called cookies – simple, short, small text files – on the User's IT device and uses them to analyze visitor flow on our website, thus helping us develop our website to enhance user experience.

Website visit data recorded in the cookie (together with the date of visit and the User's IP address) are transferred and stored on Google Inc.'s servers. Google uses this data to evaluate the User's website visit habits, compile reports about them and to provide other services relating to the website and internet use.

Tokeportal.hu uses the data to develop the website and to improve user experience. These cookies stay on the user's computer or other device used for browsing until they expire or until the visitor deletes them.

Google Inc's Privacy Policy concerning this data can be accessed at https://google.com/intl/h_All/policies/privacy. By using the website, the Website user acknowledges that he or she consents to the processing of his or her data by Google Inc.

Although the installation of cookies can be prevented by appropriate settings of the browser, by doing so some functions of the website may not be entirely functional. By using the website, the User expressly consents that Google may process, as described above, the data generated by website use.

If the User wishes to manage cookie settings or opt-out from the function, he or she can do so in the browser on his or her own IT device. Cookie/tracking function locations depend on the browser tool system, but generally, you can set the tracking functions you allow or opt-out under Tools > Options > Privacy Settings on your IT device.

Users who do not want Google Analytics to include their visit in the reports, can install an extension that opts them out from Google Analytics. This extension instructs the JavaScript scripts of Google Analytics (ga.js, analytics.js, dc.js) not to send visitor information to Google. Additionally, users who have installed the block extension will not participate in content experiments, either.

If a User wants to opt out from the Analytics web activity, he can visit the Google Analytics opt-out page (http://tools.google.com/dlpage/gaoptout), and install the extension on his browser. More information about extension installation and removal can be found in the browser help.

More information about Google cookies is available at the following address: https://www.google.com/policies/technologies/cookies.

6.2. Marketing platform

The Controller uses the MailChimp service of The Rocket Science Group service provider to send newsletters and notification e-mails. The Service Provider is a company registered in the United States of America, and its exact data is as follows: The Rocket Science Group, LLC.675, Ponce de Leon Ave NESuite 5000Atlanta, GA 30308 USA. The Service Provider is a registered member of the EU-US Privacy Shield, as a result of which personal data can be transferred to third countries, on the grounds that the protection level is adequately ensured.

The Service Provider's registration with the United States Department of Commerce can be viewed and checked at the following link: https://www.privacyshield.gov/list.

MailChimp inserts special measurement codes in the letters sent and links included in them, and uses them to measure the status of e-mails and which links have been clicked on. From this information, it can be established whether the e-mails have been successfully delivered and opened and information can be obtained about the User's e-mail use habits. To ensure that full information is provided, the Controller warns the User about legal uncertainties relating to data transfers to the United States, about which more information is provided in a notice by the Hungarian National Authority for Data Protection and Freedom of Information, available at the following link: http://www.naih.hu/files/2015-10-06-Kozlemeny---Safe-harbor.pdf.

Scope of data transferred: name, e-mail address; - purpose of processing: sending newsletters, e-mails, notifications; - duration of processing: until unsubscribing; - legal basis: the data subject's voluntary consent.

6.3. IT platform

The Portal's IT partner is Dolphio Technologies Kft. (registered office: H-2016 Leányfalu, Móricz Zsigmond út 196., e-mail: info@dolphio.hu, website: www.dolphio.hu).

The IT Partner performs its activity on the basis of the Controller's IT Security Policy and the data processing agreement signed with the Controller.

In the course of IT Audits, while the audit is performed, the auditors can access the Data Subjects' data to the extent required and justified for performing the audit. In the course of audit, justification for the access to the data must be provided before accessing (opening/downloading). Tokeportal.hu logs these instances of data processing, and thus later it can be retrieved who, when, and for what purpose processed the Data Subjects' data.

Purpose of data processing: to ensure the adequacy of the IT system of Tokeportal.hu, to check whether the IT system of Tőkeportál complies with national and international standards in terms of IT and information security.

Legal basis of the data processing: protection of the interests of Tokeportal.hu and the Data Subject.

6.4. Registration

Using the services requires registration via the Portal available on the website and creating a user account.

The person who provides the data shall be exclusively liable for the adequacy of that data. When providing their e-mail address, all Data Subjects accept liability for the fact that solely they will be using the service with the e-mail address provided. Considering this acceptance of liability, all liability whatsoever relating to access with that e-mail address shall be borne by the user who registered that e-mail address.

6.4.1. Login via LinkedIn, Google accounts

A data subject may register on the Portal using his social media account by linking his social media account to his account created on the Portal. In such cases, the privacy terms of the social media provider apply (e.g.: LinkedIn Privacy Policy for services apply to the LinkedIn account (https://www.linkedin.com/legal/privacy-policy; LinkedIn Corporation, 1000 W Maude, Sunnyvale, CA 94085, USA).

For example, when registering with LinkedIn, LinkedIn will first ask the data subject to enter his LinkedIn account data and login or register with LinkedIn. Afterwards, he can link his LinkedIn profile with the Portal, through the LinkedIn application. LinkedIn may transfer any data in the data subject's "public profile" from his LinkedIn account to the Company (e.g. last name, first name, age, profile photo, gender, list of connections, other public information, e-mail address). Of this information, we only import the data subject's e-mail address, last name, and first name to create the account on the Portal.

Via the account registered on the Portal, connected through the LinkedIn account, the data subject can access the Portal without restrictions, by clicking the button "Login via LinkedIn" on the website, which requires being logged in to LinkedIn.

6.4.2. Login via the Portal

Users can register and access the portal without using a social media account, by filling the e-mail address, password and password confirmation fields. After filling the registration form, the user must accept the General Terms and Conditions and the Privacy Policy. Following registration, Tőkeportál sends an e-mail message with the activation URL; the data subject activates his account by opening the activation URL.

6.4.3. General profile data

Following registration, the portal asks users to provide the following data

- Last name
- First name
- Display name
- Citizenship
- Place of birth
- Date of birth
- Mother's maiden name
- Type of ID
- ID number
- Address
- Phone number
- E-mail address

6.5. Investor identification and classification

Data Subjects – as users – must be identified to comply with international KYC, AML, and CTF rules and guidelines. The Company uses its best efforts so that identified and classified users can use the Portal services (e.g. shall not fall on blacklists based on international rules).

Prior to identification, the Data Subject must provide his or her consent to the processing and checking of his or her personal data, under penalty of perjury and for sake of anti-money laundering laws.

Documents to be uploaded for identification purposes:

- the two pages of the personal identity document or copy of driver's license or passport,
- address page of the certificate of domicile,
- providing the securities and bank account number,
- bank account statement and securities account statement (which is required due to the allocation of shares) no older than one month, which include the domicile of the User; the payments and the balance may be occluded
- if the customer has an investor service provider classification, a signed statement to this end.

Data to be provided for identification purposes:

- On the data entry screen, mark investor status according to Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities

6.6. Third parties

In the case of occasional data reporting, the legal basis for processing must be ascertained in each case. Personal data may solely be transferred if the legal basis for this is clear, and the purpose and the identity of the recipient of data transferred are clearly defined. Data transfers must be documented in each case, in such a way that the course and legality of the transfer should be possible to demonstrate. For documentation purposes, primarily the properly managed documents requesting data reporting and those ordering compliance with them are used.

When using the Portal, if there is an express and targeted consent of the User when participating in a specific campaign, the User's name and invested amount provided by it can be accessed by the Campaign Owners and validated Users. If the User does not consent to this, only the invested amount and the investor classification can be accessed by campaign owners and validated Users, which is by no means suitable for identifying the User.

6.7. Newsletters and other notifications

If the Data Subject has provided consent when registering or subscribing to the newsletter, the Company may send newsletters and other notifications about its services and promotions to the Data Subject. Scope of data processed for the consent and subscription: name, e-mail address, areas of interest of the Company's services.

The Data Subject provides consent to the processing of the data indicated above following prior learning of this Privacy Policy, by express acceptance – ticking the relevant checkbox – and by using the Website, by registering, and voluntarily providing the relevant data. Regarding newsletters, the Data Subject provides express and voluntary consent, by ticking the relevant checkbox, that the Controller send Website-related news and information to the e-mail address provided by the Data Subject in the course of registration.

The controller uses the electronic addresses (e-mail addresses) provided during registration as follows: the e-mail addresses are processed in order to identify the Data Subject, for contact during use of the services, and for sending the newsletter to the Data Subject.

The Controller sends information about its services to the Data Subject in electronic form, by e-mail.

The Controller only sends newsletters to its clients who have provided their express consent to this in the menu point used for this purpose.

The Data Subject may unsubscribe from the newsletter service any time, free of charge and without reason. Unsubscribing is possible with a one-step click on the link included in the newsletter or by e-mail sent to the Controller. In this case, the Controller will immediately erase the Data Subject's data from its records.

Legal basis of the data processing: the Data Subject's consent.

6.8. Social media presence, external websites

When using social media sites, data processing takes place on the social media sites, therefore the duration and form of processing, the possibilities of erasing and changing data shall be governed by the regulations of the relevant social media site.

The Website may contain links to other websites, for the purposes of the data subject's convenience and information. These websites may be operated independently from the Company's Website. The referenced websites may have their own data protection statements or policies in place, therefore it is strongly recommended to review them if the data subject visits such websites. If the referenced websites visited are not part of the Company's Website, the Company accepts no liability for their content, use, and data protection practices.

Processing related to the Controller's profile on social media sites is based on voluntary consent. The purpose of processing is to share the content located on the Controller's website on social media sites, to draw attention to it, and marketing.

Scope of data processed:

- name – identification
- photo used – identification
- comments – expressing opinion and comments
- rating – expressing opinion and sentiment
- content of question/request – reply input data

All natural persons who visit or follow the Controller's social media pages, like/dislike any content placed on them, partially or fully share them with their own friends. The data is processed until unsubscribing.

6.9. Contact with clients

Purpose of data processing: To improve User experience and manage complaints, the Company provides a possibility on its Website for its future partners to contact the Company's employees who are designated for contact. Contact can be initiated by e-mail to support@tokeportal.hu and hello@tokeportal.hu. Additionally, the User can directly access customer service via the Smartsupp chat application.

The Smartsupp application complies with the data processing rules stated in this Privacy Policy. Other information relating to data protection is available on the website https://www.smartsupp.com/help/privacy/. Scope of data processed: name, e-mail address

Legal basis of the data processing: Section 5 of the Info Act. The partners' data processing is classified as data within the scope of regulation, therefore it is not notified to the records of the data protection authority.

Duration of the data processing: until withdrawal of the Data Subject's consent.

The detailed rules of complaint management are laid down in the Complaint Management Policy.

6.10. Processing for direct business marketing and research purposes

The Controller may use the Data Subjects' personal data based on the Data Subjects' consent for the following purposes:

- sending advertisements by direct marketing, by e-mail or automated tools by phone;
- inquiry by e-mail or automated tools by phone, for market research and public opinion polling purposes;
- inquiry by e-mail or automated tools by phone, for data subject satisfaction measurement and service development purposes

The Data Subject's consent is a prerequisite to the use of the data as above. In each case consent is voluntary, and the Controller has no right to set it as a prerequisite to the signing of the contract.

The Data Subject may withdraw his or her consent to the data processing under this section any time without reason.

In every inquiry, the Controller will provide information about the fact that the Data Subject may withdraw his or her consent, and that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

6.11. Internal records about the Company's data processing and data transfers

The Company keeps a data processing and data transfer register of the data processing activities and related data transfer processes under Section 15 of Act CXII of 2011 on Informational Self-Determination and the Freedom of Information.

The documentation of the data processing and data transfer register is included in an annex to the data security and data protection policy.

7. Use of a data processor

Primarily the Controller and the Controller's internal staff have the right to access the data; however, they shall not disclose it, and, taking section 6.6 into account, they shall not transfer it to any third parties besides the data processors.

The Company may transfer data to data processor companies for the performance of system operation tasks and identification tasks. The processor shall make no decisions concerning the data processing without the controller's consent, and shall perform no processing for other purposes except as instructed by the controller, and shall perform its tasks solely on the basis of the controller's instructions. The Processor has an obligation to ensure the physical and software protection of the data to be processed, based on the rules laid down in the Company's data protection and data security notice.

8. Rights of the Data Subject

At the data subject's request, the Company shall provide information about the data subject's data it is processing, the purpose, legal basis, duration of data processing, and the persons who may receive or have received the data and the purpose for which they have received it. The Company shall provide the requested information within 15 days from submission of the request, in writing.

9. General legal remedies

The data subject may send any processing-related inquiries or comments to the Controller's personnel and may obtain information about the processing of his or her data, and may request rectification, erasure or blocking of his or her personal data, via support@tokeportal.hu and hello@tokeportal.hu.

The Controller erases the personal data if:

- it is processed illegally,
- it is incomplete or erroneous, and this situation cannot be remedied legally,
- the data subject requests so,
- the purpose of data processing has ceased or the statutory term for storing data has expired,
- it is ordered by court or by an authority.

Of the legally processed data, the Controller may transfer those which are required for the purpose of data processing:

- for settlement of legal disputes, to bodies authorized to this based on law,
- for national security, homeland defense, and protection of public security and
- for prosecuting publicly prosecutable crimes, to the authority that has jurisdiction in such cases,
- based on other legal provisions.

If the data subject does not agree with the data controller's decision or information relating to the processing of his or her personal data, or if the data controller misses the statutory deadline for sending a reply, the data subject may take the matter to court, or may contact the Hungarian National Authority for Data Protection and Freedom of Information, within 30 days from communication of the decision or missed deadline. Trial of the case falls within the jurisdiction of regional courts. If the court admits the petition, it may compel the data controller to provide the information, to rectify, block or erase the data, to annul the decision made by automatic data processing, to observe the data subject's right to objection, or to release the data.

Managing data breaches

The Company acknowledges that a data breach, in absence of adequate and timely action, may cause material and non-material damage to natural persons. To manage data breaches, it keeps a log of data breaches, in which the data protection officer records the circumstances of data breaches within no more than 72 hours from the reporting of the breach.

10. Technical background

The data controller shall select the IT devices used for providing the services for personal data processing and shall operate them in such way as:

- the processed data is accessible to the authorized parties (availability);
- authenticity and validation of the processed data are ensured (authenticity of data processing);
- it can be certified that no change has been made to the data processed (data integrity);
- the processed data is protected against unauthorized access (data confidentiality).

The Controller protects the data through adequate measures against illegal access, alteration, transmission, disclosure, erasure or destruction, or accidental destruction.

The Controller shall employ technical, management and organizational measures to ensure the protection of the security of data processing, that offer an adequate level of protection corresponding to the risks arising in connection with the data processing.

11. Other provisions

In each case where the Company intends to use the data supplied for a different purpose than that for which it was originally collected, it shall inform the user and obtain his or her prior express consent and provide him or her the possibility to prohibit such use.

The Company undertakes an obligation to ensure the security of the data, and shall take the technical measures that ensure that the data collected, stored, and processed is protected, and shall use its best efforts to prevent its destruction, unauthorized use and unauthorized alteration. It also undertakes an obligation to instruct every third party to which it may transfer or transmit the data to comply with such obligations.