Airon Consulting Kft., Airon Corporate Services Kft., Airon Trust Bizalmi Vagyonkezelő Kft., Airon Accounting Bt.

JOINT PRIVACY STATEMENT

Effective from 08 June 2021

1. Joint Privacy Statement

Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No. 95/46 (GDPR) Pursuant to Articles 13 and 14. Airon Consulting Kft., Airon Corporate Services Kft., Airon Trust Bizalmi Vagyonkezelő Kft. and Airon Accounting Bt. (Hereinafter: " Data Controllers") provide the following information to the data subjects in connection with the processing of personal data.

2. Data Protection Representative

The listed Data Controllers are considered joint controllers, their appointed joint data controller representative is Airon Consulting Kft. As a result of this joint data controller agreement Airon Consulting Kft. is entitled to act on behalf of all Data Controllers and is responsible for informing and for answering. In such cases, the obligations and responsibilities of each Data Controller shall be clearly settled in the relationship between the Data Controllers.

3. Concepts

The Data Controllers are responsible for the preparation of this Privacy Statement (the " Statement"), for the observance and control of its contents, and for the implementation of the necessary changes. The current version of the Statement is available at the registered office of the Data Controllers and on the website https://airontrust.hu/. The following terms are used in this Statement:

a. " Data management" *means any operation or set of operations on personal data or data files whether automated or non-automated such as collection, recording, systematisation, sorting, storage, transformation or alteration, retrieval, consultation, use, communication, transmission, distribution or other harmonization or interconnection, restriction, deletion or destruction.*
b. " Data processing" *means the management of data of a technical nature without the right to dispose of or decide on the data.*
c. " Personal data" *means any information relating to an identified or identifiable natural person. A natural person may be identified directly or indirectly in particular by an identifier such as a name, number, location, online identifier or identifiable with one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.*
d. " Customer" *means the designation of a natural person customer or a representative of a natural person of a legal person in the case of a contractual relationship between the Data Controllers and the holder of the personal data.*
e. " User" *means the person using the Website.*
f. " Statement" *means this Privacy Statement.*

4. Datas of the Data Controllers

a. Company name: Airon Consulting Kft.
Registered office: 1011 Budapest, Szilágyi Dezső square 1., 2nd floor
Company registration number: 01-09-721127
Tax number: 13149387-2-41
Website: http://airontrust.hu/
Phone: 061 700 4141
E-mail: hello@airon.hu

b. Company name: Airon Corporate Services Kft.
Registered office: 1011 Budapest, Szilágyi Dezső square 1., 2nd floor
Company registration number: 01-09-867077
Tax number: 13668626-2-41
Website: http://airontrust.hu/
Phone: 061 700 4141
E-mail: hello@airon.hu

c. Company name: Airon Trust Bizalmi Vagyonkezelő Kft.
Registered office: 1011 Budapest, Szilágyi Dezső square 1., 2nd floor
Company registration number: 01-09-281682
Tax number: 25550557-4-41
Website: http://airontrust.hu/
Phone: 061 700 4141
E-mail: hello@airon.hu

d. Company name: Airon Accounting Bt.
Registered office: 1011 Budapest, Szilágyi Dezső square 1., 2nd floor
Company registration number: 01-06-747090
Tax number: 22874850-1-41
Website: http://airontrust.hu/
Phone: 061 700 4141
E-mail: hello@airon.hu

5. Datas and contact details of Data Processors

Data Controllers shall only use Data Processors who provide adequate guarantees that the data processing complies with the requirements of the applicable data protection legislation, ensures the protection of the rights of the data subjects and takes appropriate technical and organizational measures to protect personal data.

The following partner(s) act as Data Processors when processing the data:

a. Name: Tárhelypark Kft.

Registered office: 1122 Budapest, Gaál József út 24.
Company registration number: 01-09-322570
Tax number: 23289903-2-43
The purpose of using the data processor is: hosting service.

b. Name: Számlázz.hu

Company name: KBOSS.hu Kft.
Company registration number: 01-09-303201
Tax number: 13421739-2-41
Purpose of using the data processor: online invoicing.

c. Name: Kulcs-Soft Számítástechnika Nyrt.

Registered office: 1016 Budapest, Mészáros utca 13.
Company registration number: 01-10-045531
Tax number: 13812203-2-41
The purpose of using the data processor: to use an accounting program.

d. Name: Microsoft Hungary Ltd.

Registered office: 1031 BudapestGraphisoft Park 3. (Záhony u.)
Phone: +36 1 437 2800
The purpose of using the data processor: correspondence, hosting services.

e. Name: DocuSign

Registered office: 221 Main St., Suite 1550 San Francisco, CA 94105
Purpose of using the data processor: Document authentication, signature in electronic form.

f. Name: PandaDoc

Registered office: 101 California St # 3975, San Francisco, CA 94111
Purpose of using the data processor: Document authentication, signature in electronic form.

g. Name: DO-Q-MENT Digital Document Archiving and Strategy Planning Ltd.

Registered office: H-1134 Budapest, Tüzér u. 30.
Purpose of using the data processor: Document authentication, signature in electronic form.

h. Name: " EVROTRUST TECHNOLOGIES" AD
Registered office: Bulgaria, Sofia, 101 Tsarigradsko shose blvd., Business center AKTIV, fl. 6.
Purpose of using the data processor: Document authentication, signature in electronic form.

i. Name: Adriana Automatik Kft.
Registered office: 1172 Budapest, XIV utca 11.
Tax number: 26383738-2-42
Purpose of using the data processor: automation of accounting.

j. Name: Online ERP Hungary Kft.
Registered office: 1145 Budapest, Szugló utca 9-15.
Tax number: 26752439-2-42
Purpose of using the data processor: use of CRM system and related services.

k. Name: e-Jogsegéd Szolgáltató Korlátolt Felelősségű Társaság
Registered office: 1135 Budapest, Kisgömb utca 6. fszt. 1
Tax number: 22670357-2-41
Purpose of using the data processor: automation of cegkapu.gov.hu.

l. Name: dr. Tornyi Róbert Law Firm
Registered office: 1011 Budapest, Szilágyi Dezső tér 1. II. emelet
Purpose of using the data processor: use of legal services.

m. Name: dr. Bács Márton Law Firm
Registered office: 1126 Budapest, Királyhágó utca 2.
Purpose of using the data processor: use of legal services.

It is mandatory to enter into a written contract between the Data Controllers and the Data Processors which must contain the data provided by the Data Controllers to the Data Processor and the activities of the Data Processor with them.

6. Compliance with legal requirements

In the course of their activities the Data Controllers intend to fully comply with the legal requirements for the processing of personal data in particular Regulation (EU) 2016/679 of the European Parliament and of the Council and process their data in accordance with the principles set out in Article 5 GDPR.

7. Application of these rules

These rules cover the protection of natural persons with regard to the processing of personal data within the scope of the Data Controllers the prevention of unauthorized use of personal data processed by the Data Controllers and the public disclosure of public and public interest data managed by the Data Controllers. The provisions of these regulations shall apply to all data management activities of the Data Controllers.

8. Scope of the Regulations

The scope of the regulations extends to all persons cooperating with the Data Controllers in the framework of any legal relationship in the course of their data processing in particular to the employees and data processors of the Data Controller. The Data Controllers determine the purposes and means of the processing of personal data independently or together with others and as a data processor they process personal data on behalf of the Data Controller. The Data Controllers in their relations with each other as data controllers and data processors respect the privacy of all persons to whom they transfer personal data and are committed to their protection.

9. Data managed by Data Controllers

In the course of data management the following personal data is processed during the services provided by the Data Controllers:

a. the personal identification data of the natural person such as the data content of the identity card of the holder of the personal data, his/her passport number, the official identity card certifying the address, the official identity card certifying the tax identification mark, the social security mark;
b. depending on the nature of the contractual relationship the bank account number of the holder of the personal data or the name of the financial institution keeping the bank account;
c. contact details of the holder of personal data (telephone number, email address);
d. in the case of a legal person party the surname and first name of the natural person entitled to represent the legal person; office; place and date of birth; mother's birth name; his permanent address, in the absence thereof, his residence address and the data content of his identity card and passport.

9.1. Personal data required by current legislation to prevent money laundering and terrorism. In the identification proccess we need personal datas from natural person customer's or the legal entity customer's natural person representative as follows:

a. surname and first name,
b. birth surname and first name,
c. citizenship,
d. place and date of birth,
e. mother's birth name,
f. address, or failing that, place of residence,
g. the number and type of his identification document.

9.2. In addition to the above the Data Controllers will have the following personal data (both in the case of the Client's employees and their own employees) during their payroll accounting service and will process them:

Personal data	Purpose of data management	Legal basis for data management	Data source	Data transmission
Name, place of birth, time, mother's name, TAJ number, tax identification, date and number of the highest education certificate	*official notification of the establishment of an employee's employment*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*to the payroll accountant, to NAV, to the competent government office during a labor inspection*
Bank account number and bank name	*fulfillment of the obligation to pay wages*	*fulfillment of an obligation arising out of an employment contract or employment contract [Article 6 (1) (b) GDPR]*	*concerned (employee)*	*no*
Data on child(ren)	*provision of additional leave, medical care*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*to payroll*
Name, position, address, social security sign	*job suitability assessment*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*to an occupational physician*
Fact of suitability for the job	*job suitability assessment*	*for preventive occupational health purposes in order to assess the worker's ability to work [Article 9 (2) (h) GDPR]*	*occupational physician*	*no*
Working time record data, (attendance) data on working time and rest time	*payroll accounting*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*employer*	*to a payroll accountant, to the competent government office during a labor inspection*

Private phone number, private email address	*contact in connection with the employment relationship (eg reporting incapacity for work)*	*necessary to pursue the legitimate interests of the employer (or a third party) [Article 6 (1) (f) GDPR]*	*concerned (employee)*	*no*
Business phone number, business email address	*contact in connection with the employment relationship*	*fulfillment of an obligation arising out of an employment contract or employment contract [Article 6 (1) (b) GDPR]*	*concerned (employee)*	*towards business partners*
Name, job title	*occupational safety and fire education*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*in the case of an official procedure, to the authority concerned*
Data on enforcement against the employee (fact of employment, salary, name of the beneficiary, Case number, amount of debt)	*fulfillment of the obligations incumbent on the employer in connection with the enforcement proceedings*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*to payroll, to executive*
Fact and circumstances of an accident at work	*fulfillment of the legal obligations of the employer in connection with the accident at work*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*executor*	*to the labor protection authority, to the payroll accountant*
Name, position, place and time of birth, tax ID, social security sign, contribution periods, fact of enforcement against the employee	*fulfillment of the employer's obligations related to the termination of employment*	*fulfillment of a legal obligation [Article 6 (1) (c) GDPR]*	*concerned (employee)*	*to payroll, to NAV*

10. Website

The Data Controllers implement the following data management on the https://airontrust.hu/ and on the Odoo websites (https://odoo.airon.hu/) operated by them (the "Website"):

a. Registration subpage

In order to fully use the services of the Website, the registration of the person using the Website ("User") is required.

b. When subscribing to the newsletter

On the Website the User has the opportunity to subscribe to the Data Controllers' newsletter on a special interface.

c. Landing page for contacting

The User / Customer has the opportunity to contact the Data Controllers directly on a separate interface using a landing page.

d. Contact subpage

Personal data sent together with a message sent to the email address hello@airon.hu with questions related to the information on the Website.

e. E-commerce / Webshop

The User / Customer has the opportunity to order the given service and settle the fee for the given service online. To do this, it is necessary to provide the personal data required for the order, as well as the bank card data used to pay for the given service.

f. Career subpage

When apply for the job advertisement to the email address hello@airon.hu (or on the Website or through an other service providers website) your motivation letter or professional CV will containe the follows personal datas:

Personal data	Purpose of data management	Legal basis for data management	Data source	Data transmission
Name, place of birth and time, address,	*determining the application material of the applicant*	*consent of the person concerned*	*concerned (employee)*	*no*

date and number of the highest diploma	*participating in the recruitment and the suitability of the applicant*			
Private phone number, private email address	*contact in connection with the employment relationship (eg reporting incapacity for work)*	*necessary to enforce the legitimate interests of the employer (or a third party) [GDPR Article 6 (1) (f)]*	*concerned (employee)*	*no*

10.1. The Data Controllers will only transfer the data of the data subject to other person(s) if the data transfer is required by law (statistical data collection; obligation to provide data imposed on the employer) or the data transfer is addressed to the Data Controllers by a court authority or other body.

10.2. If the recruitment is unsuccessful or the owner of the personal data does not accept the offer of the Data Controllers, the Data Controllers will immediately delete the application material of the data subject and his/her personal datas from all its records. If the recruitment is successful, the Data Controllers with the consent of the owner of the personal data make the part of their personal data that the Data Controllers may keep and manage in their possession part of the register of data processed about the employee. Data Controllers are not entitled to obtain personal data from sources other than the application material unless it becomes necessary to enforce the legitimate interests of the Data Controllers.

11. Guaranteeing data security

The Data Controllers shall take appropriate technical and organizational measures, taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data processing and the varying probability and severity of the risk to individuals' rights and freedoms, in order to: guarantee a level of data security commensurate with the level of risk.

12. Actions of data controllers

The Data Controllers shall take measures to ensure that natural persons with access to personal data acting under the control of the Data Controllers or the Processor may process such data only in accordance with the instructions of the Data Controllers, unless otherwise required by Union or Member State law.

13. Provision of information

The Data Controllers undertake and guarantee to provide the Customer with all information necessary to verify the fulfillment of the obligations, as well as to enable and facilitate audits performed by the Customer or another

auditor appointed by the Customer including on-site inspections. The Data Controllers undertake to immediately inform the Customer if they believe that any of its instructions violates the GDPR Regulation or other legislation.

14. Deleting and returning data

The Data Controllers undertake and guarantee that upon termination of the provision of the service under this Statement, all personal data will be deleted or returned to the Customer at the discretion of the Customer and the existing copies will be deleted unless the storage of personal data is required by law.

15. Legislation applicable to data controllers

The Parties agree that the Data Controllers may process the personal data provided by the Customer (the personal data of the Customer's employees required for payroll accounting and official reporting) only on the basis of the Customer's written instructions. For the purposes of this Statement, this Statement shall also constitute a written instruction. The Data Controllers may deviate from this only if the data processing is prescribed by the legislation applicable to the Data Controllers. In this case, the Data Controllers shall notify the Customer of this legal requirement prior to the data processing unless the notification of the Customer is prohibited by the relevant legislation in the important public interest.

16. Data Protection Officer

Data Controllers are not obliged under Article 37 of the GDPR to appoint a Data Protection Officer.

17. Data transmission

By accepting this Privacy Statement the Costumer taking into account our data protection principles, expressly consents to the Data Controllers transferring data to the service providers in a direct contractual relationship with them (credit institutions and financial companies in case of opening a bank account) in relation to the provided data. All data subjects may use the data only for the performance of the contractual task retain them for further use or pass them on to third parties in any form. The purpose of data transfer: to provide personalized service to the Costumers, to optimize the services provided to them by the Data Controllers' partners, and to fulfill the contractual tasks of the Data Controllers. We do not make the stored data available to other third parties except in cases specified by law (in the framework of criminal proceedings) or in the performance of the contractual tasks of the Data Controllers.

17.1. Data transmitted is personal data required by current legislation to prevent money laundering and terrorism. In the identification proccess we need personal datas from natural person customer's or the legal entity customer's natural person representative as follows:

a. surname and first name,
b. birth surname and first name,
c. citizenship,
d. place and date of birth,

e. mother's birth name,
f. address, or, failing that, place of residence,
g. the number and type of the identification document,
h. the data content of the official tax certificate certifying the foreign tax number, tax identification mark,
i. social security sign.

18. Foreign data transfer

Data Controllers may transfer personal data to a Data Controller conducting data processing in a third country or to a data processor processing data in a third country if the data subject has expressly consented thereto or the data processing legislation in force in the third country is complied with and an adequate level of protection of personal data is ensured during its processing. In order to implement the international agreement on international legal assistance, exchange of tax information and avoidance of double taxation the Data Controllers shall transfer personal data to a third country for the purpose under the conditions and within the scope of data specified in the international agreement. The transfer of data to an EEA state shall be deemed to take place within the territory of Hungary.

19. Data management purposes:

Data Controllers process data in accordance with the law for the following purposes:

a. performance of a contractual relationship, exercise of rights arising from a contractual relationship and performance of obligations through data processing based on the consent of the data subject;
b. fulfillment of the legal obligations of the Data Controllers and
c. enforcing the legitimate interests of the Data Controllers.

19.1. In connection with the operation of the Data Controllers and in the case of the Website operated by them, they process data for the following purposes:

a. contact, the primary purpose of which is to properly inform the Customers and Users, to deal with any technical problems that may arise efficiently and quickly, to send system messages in connection with the service;
b. registration;
c. newsletter;
d. transfer of information related to the individual services, performance of information tasks, implementation of legal regulations;
e. applying for job vacancies advertised by the Data Controllers and, in the case of further consent, retaining the data for inquiries regarding future job opportunities.

20. Data controllers process personal data during the purpose of data management such as registration, contact, newsletter sending, contacting on the landing page or applying for the indicated job

advertisement on the career sub-page or until the User's request to delete his/her datas or withdraw his/her consent.

21. By registering for the full use of the Website or by finalizing the Registration by accepting this Statement, the Users consent to the Data Controllers processing their personal data. The processing of personal data is based on the User's voluntary consent given in the knowledge of this information.

22. By subscribing to the newsletter, the User expressly and unambiguously gives his/her prior consent to the sending of marketing-related letters by the Data Controllers and in this respect to the processing of the personal data provided. The User may unsubscribe from the newsletter at any time as described in the newsletter. Newsletters may contain advertising messages.

23. By applying for a job advertisement or making inquiries sent through the contact details indicated on the contact sub-page, the Users consent to the Data Controllers processing their personal data. The processing of personal data is based on the User's voluntary consent given in the knowledge of this information.

24. In some cases, the handling, storage and transmission of a set of provided data is obliged by law, a fact which the Data Controllers shall notify the data subjects separately in each case.

25. Users may only enter their own personal data on the Website. If they do not provide their own personal data, they are obliged to obtain the data subject's consent.

26. Legal basis for data management:

a. GDPR Article 6 (1) (a): consent of the data subject;
b. GDPR Article 6 (1) (b): necessary for the performance of the contract;
c. GDPR Article 6 (1) (c): necessary to fulfill a legal obligation;
d. GDPR Article 6 (1) (a): legitimate interest, balance of interests always required.

27. If the Customer or the User contacts the Data Controllers directly by electronic or traditional letter, telephone, voice or video call and the electronic or traditional letter, telephone, voice or video call also contains the personal data indicated in the Statement in accordance with Article 6 (1) (a) of the GDPR, the Data Controllers shall consider the consent of the Customer or the User to the processing of the personal data of the data subject in accordance with the relevant legislation.

28. The Customer or the User is responsible for the fact that the third party included in the conversation by the Customer or the User during the electronic correspondence, telephone, voice or video call between him and the Data Controllers maybe find out personal datas.

29. Personal data sent by the Customer or the User by electronic or traditional mail, telephone, voice or video call, which have not been requested by the Data Controllers and are not necessary for the purposes of data processing, the Data Controllers shall delete them immediately and inform the Customer or the User.

30. If the Customer or the User unreasonably attaches or transmits several e-mails, telephone, voice or video calls to the employees of the Data Controllers without request, the Data Controllers shall state the state of science and technology and the costs of implementation, and seeks to avoid the deletion of all such personal data, taking into account the nature, scope, circumstances and purposes of the data processing and the rights and freedoms of natural persons, but it is the responsibility of the Customer or the User to act with caution in this matter.

31. In case of processing the personal data of the data subject on the basis of a legitimate interest,we perform a balance of interests, during which:

a. identify and record a legitimate interest,
b. identify and record the interests and rights of the data subject,
c. necessity and proportionality, consideration based on the principles of purpose, data saving, limited storage,
d. we inform the data subject of the balance of interests.

32. Duration of data processing:

a. The duration of the contract or otherwise provided by law, the duration of the law.
b. Invoices are kept for at least 8 years due to a legal obligation.
c. The retention period of the documents on which the invoice is based is 8 years.
d. Retention period of documents on which the employment relationship is based: 50 years.
e. The retention period of the data provided for the purpose of contact is 1 year after the termination of the connection.
f. Retention of data related to the performance of the contract: 5 years.

33. Rights of the person concerned:

In connection with his personal data, the data subject has the rights specified by law:

a. the right to information [Articles 13 and 14 GDPR];
b. right of access (knowledge of data, fact of data processing) [Article 15 GDPR];
c. if a data is out of date or incorrect, adjust it [Articles 16 and 19 GDPR];
d. deletion (only for data processing based on consent) [Articles 17 and 19 GDPR];
e. restrictions on data processing [Articles 18 and 19 GDPR];
f. prohibiting the use of personal data for direct marketing purposes;

g. transfer or prohibit the transfer of your personal data to a third party service provider;
h. request a copy of any personal data processed by the Data Controllers;
i. protest against the use of personal data [Article 21 GDPR];
j. making a complaint to the authority;
k. court redress.

34. At the request of the User or the Customer, data controllers shall provide information on the personal data they manage, their source, the purpose, legal basis, duration of the data processing and - in case of transfer of the data subject's personal data - the legal basis and recipient of the data transfer. The information can be requested by e-mail: at the e-mail address hello@airon.hu or by post to the following postal address: Airon Consulting Kft. 1011 Budapest, Szilágyi Dezső square 1st, 2nd floor, in both cases with proof of identity and by entering a mailing address. Data controllers shall respond in writing no later than 30 (thirty) days from the receipt of the request.

35. The User or the Customer is entitled to request the correction of his/her personal data (indicating the correct data) also at the e-mail address hello@airon.hu or by post to the following postal address: Airon Consulting Kft. 1011 Budapest, Szilágyi Dezső square 1st, 2nd floor, in both cases with proof of identity and postal address. Data controllers shall immediately make the correction in their records and notify the data subject in writing.

36. In addition to the above, the User or the Customer may at any time request the deletion of his data or the restriction of his handling by sending an e-mail to hello@airon.hu and by post to the following postal address: Airon Consulting Kft. 1011 Budapest, Szilágyi Dezső square 1st, 2nd floor at a postal address free of charge, without justification, with proof of identity and postal address. Upon receipt of the request for deletion the data controllers shall immediately ensure the termination of the data processing and delete the User or the Customer from its register.

37. Instead of deleting, the Data Controllers restrict the processing of personal data if the User or the Customer so requests. Where data processing is restricted, such personal data may be processed, with the exception of storage, only with the consent of the data subject or for the purpose of bringing, enforcing or protecting legal claims or protecting the rights of another natural or legal person or in the important public interest of the Union or a Member State.

38. If the Data Controllers do not comply with the request of the User or the Customer for rectification, restriction of processing or deletion, they shall communicate in writing the factual and legal reasons for rejecting the request for rectification, restriction of processing or deletion within 30 days of receipt of the request. In the event of a rejection of a request for rectification, erasure or restriction of handling,

the Data Controllers shall inform the User or the Customer of the possibility of legal redress and recourse to the National Data Protection and Freedom of Information Authority.

39. The User or the Customer may object to the processing of his/her personal data,

a. if the processing or transfer of personal data is necessary only for the fulfillment of a legal obligation to the Data Controllers or to enforce the legitimate interests of the Data Controllers, the data recipient or a third party, except in the case of mandatory data processing;

b. if the use or transfer of personal data is for the purpose of direct business acquisition, public opinion polling or scientific research; and

c. in other cases specified by law.

40. The Data Controllers shall examine the protest as soon as possible but not later than within 15 days from the submission of the request, make a decision on the merits thereof and inform the applicant of its decision in writing. If the User or the Customer does not agree with the decision of the Data Controllers, or if the Data Controllers fail to comply with the above deadline, the User or the Customer may apply to a court within 30 days from the notification of the decision or the last day of the deadline.

41. Data collected while using the Website

If the User does not explicitly provide personal data or information on the Website the Data Controllers will not collect or process any personal data relating to the User in a manner that would allow the User to be personally identified.

41.1. By visiting the Website, all Users or Clients consent to the Data Controllers recording the data and information written in this part of the Prospectus, as well as placing the cookies necessary for the recording.

41.2. Such data is the data of the User's or the Customer's login computer, which is generated during the use of the Website and which is recorded by the Data Controllers' system as an automatic result of the technical processes. The automatically recorded data is automatically logged by the system - without a separate statement or action of the User or the Customer - when visiting or exiting the Website.

41.3. This data is not linked to other personal user data, the User or the Customer cannot be identified on the basis of this data. Such data can only be accessed by the Data Controllers. This data can be collected using various technologies such as cookies, web beacons and log files.

41.4. Such data shall include the following information:

a. Cookies: Cookies are short text files that a website sends to an user's computer hard drive that contain information about the user.

b. Log files: the Internet browser automatically transmits certain other data to the website, such as the IP address of the User's computer (192.168.2.1), the operating system or browser type used by the User or the Customer, the domain name from which the user sub-pages visited on the website, as well as sub-pages visited by the user within the website, content viewed on the website.

41.5. Data Controllers, like other service providers operating the Website, analyze this data to determine which areas of the Website are more popular than others. Furthermore, like other major service providers, this data is also used by Data Controllers to tailor the website experience to the needs of the user.

42. Use of Data Collected While Using the Website

The data collected by the above-mentioned technologies may not be used to identify the User or the Customer, nor shall the Data Controllers link this data with any other data that may be identifiable.

42.1. The primary purpose of the use of such data is to enable the Data Controllers to operate the Website properly, which requires in particular the monitoring of data on visits to the Website and the prevention of possible abuses related to the use of the Website. The data specified in this Statement may also be used for the personal preferences of the Data Controllers (the most frequently viewed content on the Website).

42.2. In addition to the above, Data Controllers may use this information to analyze usage trends and to improve and improve the functions of the Website, as well as to obtain comprehensive traffic data on the full use of the Website.

43. Disable cookies:

If you do not want the Data Controllers to collect the information described above about you in connection with your use of the Website, you may disable the use of cookies in part or in full in your Internet browser settings or otherwise change the settings for cookie messages.

43.1. In such a case, however, you agree that the content displayed on the Website will not be displayed in a selective manner according to your preferences, certain services will not be available or in the way that would otherwise be enabled by cookies and the Website user experience will not be the same to a large extent.

44. Links

The Data Controllers are not responsible for the content, data and information protection practices of external websites available as a jumping point from the Website. If the Data Controller becomes aware that the site or

linking to it infringes the rights of third parties or applicable law, the link will be removed from the Website immediately and further action will be taken.

45. Data security

The Data Controllers undertake to ensure the security of the data, to take the technical and organizational measures and to establish the procedural rules to ensure that the recorded, stored and processed data are protected and to prevent their destruction and unauthorized use and unauthorized alteration. They also undertake to call on all third parties to whom the data is transmitted or transferred with the consent of the Users or the Clients to comply with the data security requirement.

46. Disclosure of personal data

Only Data Controllers have the right to access personal data directly. Data Controllers will take all technically reasonable steps to securely store Users and Customers and their data. The Data Controllers shall treat the information generated during the provision of the data specified in the above points with the utmost care and in strict confidence. Administrators of Data Controllers have different rights in the management of data: some administrators have full rights, others have only limited access and rights.

47. Privacy Incident

Data controllers shall ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorized persons. The processed data may only be accessed by the employees of the Data Controllers, they shall not be transferred by the Data Controllers to a third party who is not entitled to access the data.

47.1. Data controllers will do their best to ensure that the data is not accidentally damaged or destroyed. The above commitment is also required by Data Controllers for their employees involved in data management activities.

47.2. Under no circumstances shall data controllers collect specific data, ie data relating to racial origin, membership of a national or ethnic minority, political opinion or party affiliation, religious or other worldview, membership of an advocacy organization, health status, pathological passion, sex life, and a criminal record.

47.3. In the event of a data protection incident, the Data Controllers shall, without undue delay and no later than 72 hours after becoming aware of the data protection incident, notify the supervisory authority, unless the data protection incident is not likely to jeopardize the rights and freedoms of natural persons. In the unexpected case, if the notification is not made within 72 hours, the Data Controllers shall also attach to the notification the reasons for the delay.

47.4. If the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons, the Data Controllers shall inform the data subject of the data protection incident without undue delay.

47.5. When informing data subjects about a data protection incident that is likely to involve a high risk, the Data Controllers shall:

a. the nature of the data protection incident is clearly and intelligibly described;
b. provide information on the names and contact details of other contact persons for further information;
c. describe the likely consequences of the data protection incident;
d. describe the measures taken or planned by the Data Controllers to remedy the data protection incident, including, where appropriate, measures to mitigate any adverse consequences arising from the data protection incident.

48. Remedies information

In Hungary, the data protection supervisory authority is the National Data Protection and Freedom of Information Authority (hereinafter: NAIH, address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C, e-mail address: ugyfelszolgalat@naih.hu). The data subject may submit a complaint to the NAIH if, in his or her opinion, the processing of personal data concerning him or her does not comply with the legal obligations. A judicial review may be initiated against the decision of the NAIH.

49. Information on records:

The Data Controllers manage and process the data in a lawful, transparent and verifiable manner for the purposes of which they keep the following records:

a. records of data processing,
b. records of data transfers,
c. records of cessation of data management,
d. record of data protection incidents,
e. records of stakeholder and official requests and responses,
f. Registration of "lost" data, inquiries,
g. record of prior data protection impact assessment.

49.1. Data Controllers shall take appropriate measures to provide the data subject with all information and any information relating to the processing of personal data in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner.

49.2. If the processing is carried out by another person on behalf of the Data Controllers, the Data Controllers may only use data controllers who provide adequate guarantees to implement appropriate

technical and organizational measures to ensure that the data processing complies with the requirements of this Regulation and protects the rights of data subjects.

50. Final provisions

These Regulations are effective from 08 June 2021. The Regulations shall apply to legal relationships arising after its entry into force or to existing legal relationships in which data processing takes place after 08 June 2021.

50.1. Data controllers reserve the right to unilaterally amend this Privacy Statement at any time with prior notice to those concerned.

50.2. The Data Controllers are obliged to draw the attention of all their Clients or natural persons establishing other legal relations with the Data Controllers to the entry into force of these Regulations and their application, and they are obliged to make these Regulations available to them.

Date: Budapest, 08 June 2021