DATA PROCESSING AGREEMENT

With regard to the provisions of Section 13.5. of the Service Provider's General Terms and Conditions (hereinafter referred to as: **"GTC"** or **"Agreement"**) and the relationship between the User and the Service Provider's legal relationship in relation to the Service in accordance with Article 29 of the GDPR the Parties agree as follows with regard to the processing of data by the Service Provider

1. The Parties establish that, in view of the fact that the Service Provider is the User's data processing partner in the course of the provision of the Service, the Service Provider may also have access to the personal data of third parties as data subjects, and therefore it is necessary for the Parties to enter into a data processing agreement, which obligation the Parties fulfil with the present document, which is attached to the GTC.

2. The Parties acknowledge that they have read and understood the provisions of this Data Processing Agreement and agree to be bound by the provisions contained herein.

3. Accordingly, the Parties agree that if the Service Provider processes data in connection with the provision of the Service in relation to the data processed by the User, the Service Provider undertakes the following:
   - processes data in accordance with the GDPR and other national, European Union or international data protection laws;
   - ensure that all persons who are authorized to process personal data are bound by confidentiality obligations;
   - takes all necessary organizational and technical measures to ensure the security of the data;
   - provide the User with all information necessary to demonstrate compliance with data protection legislation, enable and reasonably consent to audits, including inspections, carried out by the User or an agent acting on its behalf;
   - permanently delete all copies of the User's database in its possession or, by the request of the User, return such data upon termination of this Data Processing Agreement, in accordance with the time limits set out in its Privacy Policy

4. The Parties agree that the Service Provider shall process the personal data made available to it only in connection with the provision of the Service and in accordance with the User's written instructions. The User may give the instruction in a documented electronic form, in relation to which the Parties agree that communication by e-mail shall satisfy this requirement. The Service Provider shall draw the attention of User and to the possible consequences in the event it receives any unprofessional or unlawful instructions from the User.

5. The the scope of the data that may be processed is contained in the Service Provider's Privacy Policy.

6. The Service Provider accepts any instructions at dpa@hungarodo.hu. Only the legal representative of the User or a person whom the Service Provider has reason to believe is entitled to give any instruction. If the Service Provider has doubts as to whether the person giving an instruction on behalf of the User is duly authorized, the Service Provider shall be entitled to suspend the execution of the instruction until it is convicted of the existence of the authorization.

7. In order to fulfil the obligations under Sections 3 to 5, the User shall ensure that the contact details available to the Service Provider are always up to date, so that the Service Provider can notify the User of the relevant circumstances under this Data Processing Agreement in a timely manner.

8. The Parties establish that in all cases related to the provision of the Service, the User shall be the controller of the personal data processed, the sole owners and right holders of which shall be the User's customers, partners, subcontractors or employees. The scope of the data processed by the Service Provider is set out in Annex 1 to this Data Processing Agreement.

9. The Parties establish that in case a third party makes a claim against the Service Provider in connection with the processing of personal data, if the third party's claim is not attributable to the Service Provider, the User shall do everything possible to indemnify the Service Provider from any damages and costs that may arise in connection with the enforcement of the claim. In this case, the Service Provider shall cooperate with the User as the data controller.

10. The Parties agree that in all cases the User is responsible for any question relating to the lawfulness of the processing. In this regard, the Service Provider shall promptly forward to the User any third party request regarding the processing of data. The Service Provider shall be liable for any damage resulting from failure of omitting the latter obligation.

11. The Parties agree that the Service Provider may process the personal data made available by the User only in connection with the GTC, and may not use them for any other purposes, in particular for its own purposes. This shall not apply if the Service Provider is obliged to carry out other data processing under EU law or any other Member State law to which the Service Provider is subject to (e.g. investigations carried out by state authorities or law enforcement agencies). In all cases, the Service Provider shall comply with the applicable Hungarian and EU legislation when processing data.

12. Where the processing involves personal data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data or biometric data revealing the identity of a natural person, health, sex life or sexual orientation, or data concerning criminal convictions or offences (hereinafter as: **"Sensitive Data"**), the Service Provider shall apply special restrictions and/or additional safeguards.

13. The User is responsible for the quality and lawfulness of the collection of customer and other data of data subjects. The User must immediately and to the fullest extent notify the Service Provider if it becomes aware of any errors or irregularities in the data protection provisions or in its instructions during the term of the contractual relationship.

14. The Service Provider may provide data to authorities or third parties for the purposes of the fulfilment of the GTC, but in other cases it may only provide information on the personal data it processes if it has informed the User in advance, who then provides the consent of the data controller to the disclosure of the data. In the event that the User contacts the Service Provider in order to comply with its statutory obligation to provide any data, the Service Provider shall immediately provide the User with the requested information and, if necessary, shall provide access to the systems and premises where the data processing is carried out.

15. With respect to the above, the Service Provider undertakes to ensure that the owners of the personal data subject to the processing have all rights related to the processing, to comply with the provisions of the GDPR applicable to it, and finally to keep records of its processing activities.

16. If the User informs the Service Provider that it is obliged to delete, restrict or make the data it processes inaccessible, the Service Provider shall comply with the request without delay, except in cases where it is able to prove that it would be contrary to its legitimate interests, in particular

if the reason for refusing to delete the data is to ensure compliance with legal requirements or if the processing of the data is necessary for the proper performance of a contract.

17. The Service Provider undertakes to comply with the confidentiality rules in relation to the processing of data, which obligation shall survive the termination of the Agreement.

18. The Service Provider warrants that it will familiarize its employees and subcontractors involved in data processing with the provisions on data protection prior to the commencement of data processing, and that its employees and subcontractors and sub-processors will also comply with the confidentiality provisions applicable to them.

19. he Service Provider may use additional data processors only with the prior written consent of the User, except for the sub-processors specified in Annex 2 to this Data Processing Agreement and other subcontractors whose activities are closely related to the provision of the Service, as specified in the Service Provider's Privacy Policy. The Service Provider shall ensure compliance with the terms of this Data Processing Agreement in respect of the aforementioned data processors and those specifically authorized by the User.

20. The Service Provider shall enter into a written contract with the sub-processors. This formal requirement is also met if it is in electronic form.

21. The Service Provider shall ensure that the sub-processor(s) in the sub-processing agreement follow the data processing procedures set out in this Data Processing Agreement or a stricter procedure. The Service Provider shall also ensure that the responsibilities between the Service Provider and the sub-processor(s) and other sub-processors are clearly allocated. The Service Provider shall ensure that the User may carry out, or have carried out by a third party acting on its behalf appropriate assessments and audits in relation to sub-processors, unless compliance with the GDPR can be demonstrated by certification or approval.

22. The Service Provider shall notify the User in due time of any request to use a new sub-processor or of any planned changes to replace the previous ones. The User shall have the opportunity to object to these changes within 14 days for good cause. The objection must be made in writing and must state the reasons for the objection. If no approval or objection is given within the 14-day period, the sub-processor concerned shall be deemed to have approved by the User. If the User legitimately objects and the Service Provider is unable to comply with the objection, the Service Provider shall notify the User thereof without delay.

23. If the Service Provider carries out processing in a third country (i.e. outside the EEA), it requires the prior written or electronically documented consent of the User and only if the specific requirements of the GDPR are met. If the Commission decides that a third country ensures an adequate level of data protection, no further consent is required for the transfer of data. The Service Provider informs the User that the data may also be processed in a third country outside the EU if the Service Provider and the recipient of the data enter into an agreement in accordance with the Commission Implementing Regulation (EU) 2021/914 of the European Parliament and of the Council of 29th June 2016 laying down standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (EU) of the European Parliament and of the Council (hereinafter as: **"SCC"**), in which case the written consent of the User is not required pursuant to Article 45 of the GDPR.

24. Transfers within the EEA are governed by the provisions of the GDPR and this Data Processing Agreement.

25. The Service Provider shall take all necessary technical and organizational measures to maintain the required levels of processing throughout the duration of the Agreement in order to ensure that the level of protection and the rights of the data subjects are adequately ensured. The Service Provider shall take into account the objectives of protection, such as confidentiality, integrity and availability of systems and services, in order to minimize the risks during the term of the Agreement, and undertakes to take appropriate technical and organizational measures to assist the User, to the extent possible, to comply with requests related to the exercise of the rights of the data subjects, and to assist the User to comply with the provisions of the GDPR. The precise technical and security measures taken by the Service Provider are set out in Annex 3 to this Data Processing Agreement.

26. The Service Provider undertakes to review its systems on an annual basis to ensure that the technical and organizational solutions it uses maintain the security of data processing.

27. The Service Provider is obliged to notify the User within 72 hours if it detects a personal data breach, and to fully cooperate with the User and provide the necessary information to the User in order to let the User comply with its legal obligations related to the notification of the personal data breach.

28. The Service Provider's notification under Section 27 above must include:

    a) the description of the nature of the data breach (including, where possible, the categories and approximate number of data subjects and data);
    b) details of the contact point where further information about the data breach can be obtained;
    c) its likely consequences and the measures taken or planned to address the data breach, including mitigation of any adverse effects.

    Where it is not possible to provide all the above information at the same time, the first notification shall contain the information available at the time and further information, as it becomes available, shall be provided subsequently without undue delay.

29. The Service Provider is also required to take reasonable steps to contain, investigate and mitigate the effects of the data breach. Notification of or response to the User about a data breach in accordance with this Section shall not be construed as an admission of fault or liability by the Service Provider in connection with the data breach.

30. It is the User's obligation to notify the authorities about the personal data breach, unless the User instructs the Service Provider to make the notification on its behalf.

31. Prior to the commencing and during the data processing the User shall have the right to verify that the data processing activities of the Service Provider, in particular the technical and organizational measures, are in compliance with the obligations and legal requirements imposed on the Service Provider in this Data Processing Agreement, in the framework of which the Service Provider shall provide the User with all requested information.

32. The Parties agree that the Service Provider shall not be entitled to request data from the User's systems, to process data made available to it in connection with the performance of the Agreement, or to store such data, as of the termination of the Agreement, and shall therefore be obliged to return the processed data to the User in accordance with the User's instructions or to irretrievably delete them after the termination of the Agreement. Exceptions to the latter shall be

such personal data in connection with which further processing is necessary to comply with a legal obligation applicable to the Service Provider or which the Service Provider processes on the grounds of its own legitimate interests.

33. This Data Processing Agreement shall enter into force upon the establishment of a contractual relationship between the Parties.

34. This Data Processing Agreement may not be terminated independently of the GTC.

35. Upon termination of the legal relationship under the GTC, this Data Processing Agreement shall automatically terminate without any further legal declaration.

36. The Parties agree that this Data Processing Agreement is the only agreement between the Parties relating to the processing of data in connection with the Services and supersedes and replaces any previously data processing agreements they may have entered into.

37. Any modification, amendment or termination of this Data Processing Agreement must be in writing or in documented electronic form. This also applies to any modification or termination of the requirement of written form.

38. For matters not covered by this Data Processing Agreement, the provisions of the GDPR and other applicable European Union or Hungarian data protection laws shall prevail. For all disputes arising out of this Data Processing Agreement, the parties agree to submit to the jurisdiction of the courts of Hungary and to the exclusive the competence of courts according to the place of establishment of the Service Provider.

39. If any provision of this Data Processing Agreement is or becomes invalid, void, or deficient, the remaining provisions shall not be affected. The Parties agree to replace the invalid provision with a legally permissible provision that most closely matches the intent and best meets the requirements of the invalid provision.

Annex no. 1.
Data affected by processing

User Databases: if the User uses the Service and creates his/her/its own database, any information or content that he/she/it records or uploads to his/her/its database becomes subject to the Service Provider's processing.

These data often contain personal data, such as: a list of the User's employees, contacts and customers, messages, images, videos, etc. These data are collected by the Service Provider on behalf of the User, but are owned and controlled by the User in all cases.

Annex no. 2.
Sub-processors

1) **Digitalocean**

Company name: **Digitalocean LLC**
Registered seat: **101 6th Avenue, New York, NY 10013, USA**
Registration number: **5182649**
Represented by: **Yancey L. Spruill igazgató**
E-mail: **privacy@digitalocean.com**
Phone: **+1 212 226 2794**
(hereinafter as: **„Digitalocean”**)

The Service runs on servers provided by Digitalocean at Digitalocean's data centers located in Frankfurt, Germany and Amsterdam, the Netherlands i.e. within the European Union.

Although the Service Provider use the servers of Digitalocean located within the territory of the European Union, namely in Frankfurt, Germany and Amsterdam, the Netherlands, Digitalocean is a service provider located outside the EU in the United States and it may occur that certain data is transferred outside the EU. Despite the latter personal data is still secure and protected by the provisions of the GDPR, as Digitalocean's data processing outside the European Union is in line with the rules of the SCC regarding which more information may be found at https://www-static.cdn.prismic.io/www-static/4578633e-ba6b-4c45-845c-1e69848c6e3b_DigitalOcean+SCC+Template.pdf

Digitalocean ensures the protection of data on multiple levels, physically protecting data storage servers, its infrastructure through uninterruptible power supplies and other advanced tools, limiting access to data, continuous monitoring of its system, encryption, and finally, environmentally selecting data center locations, because Digitalocean set up its data centers in places where it is not exposed to nature, such as seismic activity. More information about Digitalocean's security solutions is available at https://www-static.cdn.prismic.io/www-static/62aae0a4-619c-4b87-9e91-deca34e0c07c_DigitalOcean+-+2021+Type+2+SOC+3+-+Report.pdf

Digitalocean has the following security and privacy certificates: https://www.digitalocean.com/trust/certification-reports

Digitalocean’s general privacy policy can be reached at: https://www.digitalocean.com/legal/privacy-policy/

Annex no. 3.
Organizational and technical measures

The Service Provider uses the following organizational and technical measures to ensure the security of personal data:

1. Confidentiality

a. Access control to premises and facilities

Unauthorized access (in the physical sense) must be prevented.

Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

Realized measures by the Processor:

☒ Access control system
ID reader, magnetic card, chip card
☐ (Issue of) keys
☐ Door locking (electric door openers etc.)
☒ Security staff, janitors
☒ Surveillance facilities
Alarm system, video/CCTV monitor
☒ others: infrastructure in DO private cloud, access is given only to authorized individuals, infrastructure access only possible in multi level security steps

b. Access control to systems

Unauthorized access to IT systems must be prevented.

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

Realized measures by the Processor:

☒ Password procedures (incl. special characters, minimum length, change of password)
☐ Automatic blocking (e.g. password or timeout)
☒ Creation of one master record per user
☒ Two-factor authentication
☐ Encryption of data media
☒ others: Users has passphrase protected minimum 2048 bit encoded SSH keys, with_____

c. Access control to data

Activities in IT systems not covered by the allocated access rights must be prevented.

Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

Realized measures by the Processor:

☒ Differentiated access rights (profiles, roles, transactions and objects)
☐ Reports
☒ Access
☐ Change
☐ Deletion
☒ Rights authorization concept
☒ Need-based rights of access
☐ Logging of system access events
☐ others: _____

d. Disclosure control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

Realized measures by the Processor:

☒ Encryption/tunneling (VPN = Virtual Private Network)
☐ Electronic signature
☒ Logging
☒ Transport security
☐ others: _____

e. Segregation control

Data collected for different purposes must also be processed separately.

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

Realized measures by the Processor:

☐ "Internal client" concept / limitation of use
☒ Segregation of functions (production/testing)
☒ others: only storage

f. Pseudonymization and Encryption

The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

Realized measures by the Processor:

☒ others: every customer has separate database and Linux user for the file system access

2. Integrity

a. Disclosure control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

Realized measures by the Processor:

See 1.b

b. Input control

Full documentation of data management and maintenance must be maintained.

Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Realized measures by the Processor:

☐ Logging and reporting systems
☐ Document Management
☐ others: _____

3. Availability and Resilience

a. Availability control

The data must be protected against accidental destruction or loss.

Measures to assure data security (physical/logical):

Realized measures by the Processor:

☒ Backup procedures
☒ Mirroring of hard disks, e.g. RAID technology
☒ Uninterruptible power supply (UPS)
☒ Remote storage
☒ Anti-virus/firewall systems
☐ Reporting procedures and contingency planning
☒ Disaster recovery plan
☐ others: security measures provided by DO like multi A-Z database

b. Resilience of the Systems

Realized measures by the Processor:

☒ ongoing Monitoring of the parameter of the data center and the uses of applications
☒ usage of fault tolerant systems
☒ contingency plan

☐ others: _____

c. Rapid Recovery

Realized measures by the Processor:

☒ recovery
☒ control of contingency plan
☒ recovery testing
☐ others: _____

4. Procedures for regular testing, assessment and evaluation

Realized measures by the Processor:

☐ certified Data Management System according to ISO 27001
☐ ISO 27001 Certification
☒ Data Protection Management
☒ Incident Response Management
☐ Data Protection Officer
☒ Training of employees
☐ Data Protection by Design and Default (Article 25 Paragraph 2 GDPR)
☐ Order or Contract Control (Article 28 GDPR)
☐ others: _____