DATA PROCESSING AGREEMENT

Between:

IFAS Consult SRL (trading as **DanubeData**) CUI: RO46614360 Trade Register: J30/870/2022 Registered Office: Satu-Mare, Satu-Mare, Str. Ilarie Chendi no 28 ap 1, Romania Email: privacy@danubedata.ro

(hereinafter referred to as the "**Processor**" or "**DanubeData**")

And:

The Customer who accepts the DanubeData Terms of Service and uses DanubeData cloud infrastructure services

(hereinafter referred to as the "**Controller**" or "**Customer**")

(collectively referred to as the "**Parties**")

RECITALS

WHEREAS:

A. The Controller wishes to use the cloud infrastructure services provided by the Processor, which may involve the processing of personal data;

B. The Parties wish to ensure that personal data is processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, "GDPR") and other applicable data protection laws;

C. This Data Processing Agreement ("DPA") sets out the terms and conditions under which the Processor will process personal data on behalf of the Controller.

NOW, THEREFORE, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

In this DPA, the following terms shall have the meanings set out below:

"Data Protection Laws" means the GDPR, together with any national implementing laws, regulations, and secondary legislation in Romania and the European Union, as amended or updated from time to time.

"Data Subject" means an identified or identifiable natural person whose personal data is processed.

"Personal Data" means any information relating to an identified or identifiable natural person as defined in Article 4(1) of the GDPR.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

"Processing" means any operation or set of operations performed on personal data, as defined in Article 4(2) of the GDPR.

"Services" means the cloud infrastructure services provided by the Processor to the Controller, including but not limited to virtual private servers (VPS), managed databases, cache instances, object storage, and serverless containers.

"Sub-processor" means any third party engaged by the Processor to process personal data on behalf of the Controller.

"Supervisory Authority" means an independent public authority responsible for monitoring the application of Data Protection Laws, including the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP).

1.2 Interpretation

In this DPA:

- References to Articles are to articles of the GDPR unless otherwise stated;
- The terms "Controller," "Processor," "Data Subject," "Personal Data," and "Processing" shall have the meanings given to them in the GDPR;
- Headings are for convenience only and shall not affect interpretation.

2. SCOPE AND PURPOSE OF PROCESSING

2.1 Subject Matter

This DPA applies to the processing of personal data by the Processor on behalf of the Controller in connection with the provision of the Services under the Terms of Service.

2.2 Duration

This DPA shall remain in effect for the duration of the Controller's use of the Services and shall terminate automatically upon termination of all service agreements between the Parties.

2.3 Nature and Purpose of Processing

The Processor processes personal data for the purpose of providing the Services to the Controller, which includes:

- Storage of data on infrastructure managed by the Processor;
- Transmission of data through the Processor's network infrastructure;
- Backup and disaster recovery operations;
- Technical maintenance and support operations;
- Security monitoring and incident response.

2.4 Types of Personal Data

The types of personal data processed are determined solely by the Controller and may include, but are not limited to:

- Contact information (names, email addresses, phone numbers);
- Account credentials and authentication data;
- Financial and transactional data;
- Employment and HR data;
- Customer and user data;
- Any other personal data the Controller chooses to store in the Services.

2.5 Categories of Data Subjects

The categories of data subjects are determined solely by the Controller and may include:

- The Controller's employees, contractors, and agents;
- The Controller's customers and end-users;
- The Controller's suppliers and business partners;
- Any other individuals whose personal data the Controller processes using the Services.

3. CONTROLLER OBLIGATIONS

3.1 Compliance

The Controller shall:

a) Ensure that all personal data provided to or processed by the Processor is collected and processed lawfully, fairly, and in accordance with Data Protection Laws;

b) Ensure that a valid legal basis exists for the processing of personal data by the Processor;

c) Provide clear and documented instructions to the Processor regarding the processing of personal data;

d) Ensure that Data Subjects are informed about the processing of their personal data in accordance with Articles 13 and 14 of the GDPR;

e) Respond to requests from Data Subjects exercising their rights under Data Protection Laws.

3.2 Instructions

The Controller hereby instructs the Processor to process personal data as necessary to provide the Services in accordance with this DPA and the Terms of Service.

4. PROCESSOR OBLIGATIONS

4.1 Processing Limitations

The Processor shall:

a) Process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by European Union or Member State law to which the Processor is subject;

b) Immediately inform the Controller if, in the Processor's opinion, an instruction infringes Data Protection Laws;

c) Process personal data only to the extent necessary to provide the Services.

4.2 Confidentiality

The Processor shall ensure that all persons authorized to process personal data:

a) Have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

b) Process personal data only as instructed by the Controller and in accordance with this DPA.

4.3 Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate:

a) The pseudonymization and encryption of personal data;

b) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.

4.4 Specific Security Measures

Without limiting Section 4.3, the Processor implements the following security measures:

Technical Measures:

- Encryption of data in transit using TLS 1.2 or higher;
- Encryption at rest for sensitive data and backups;
- Network security including firewalls, network segmentation, and DDoS protection;
- Intrusion detection and prevention systems;
- Regular security updates and vulnerability patch management;
- Automated backup systems with encrypted offsite storage;
- Multi-factor authentication for administrative access;
- Comprehensive access logging and security monitoring.

Organizational Measures:

- Role-based access control with principle of least privilege;
- Employee background checks and confidentiality agreements;
- Regular security awareness training for all personnel;
- Documented incident response and disaster recovery procedures;

- Business continuity planning and testing;
- Regular security audits and assessments;
- Vendor security assessment procedures.

4.5 Assistance to Controller

The Processor shall assist the Controller in:

a) Responding to requests from Data Subjects exercising their rights under Chapter III of the GDPR, taking into account the nature of the processing;

b) Ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

4.6 Deletion and Return of Data

Upon termination of the Services:

a) The Processor shall, at the choice of the Controller, delete or return all personal data to the Controller within thirty (30) days;

b) The Processor shall delete existing copies of personal data unless European Union or Member State law requires storage of the personal data;

c) Upon request, the Processor shall provide written certification of deletion.

4.7 Audit Rights

The Processor shall:

a) Make available to the Controller all information necessary to demonstrate compliance with this DPA and Article 28 of the GDPR;

b) Allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to reasonable advance notice and confidentiality obligations.

5. SUB-PROCESSORS

5.1 Authorization

The Controller provides general authorization for the Processor to engage Sub-processors to assist in providing the Services, subject to the requirements of this Section 5.

5.2 Current Sub-processors

As of the date of this DPA, the Processor engages the following Sub-processors:

Sub-processor	Purpose	Location
Hetzner Online GmbH	Data center infrastructure	Germany (EU)
Stripe, Inc.	Payment processing	United States (with EU SCCs)
Mailersend, Inc.	Transactional email delivery	United States (with EU SCCs)

5.3 Changes to Sub-processors

a) The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller the opportunity to object to such changes;

b) The Controller may object to the appointment or replacement of a Sub-processor within fourteen (14) days of receiving notice, provided that such objection is based on reasonable grounds relating to data protection;

c) If the Controller objects and the Processor cannot reasonably accommodate the objection, either Party may terminate the affected Services.

5.4 Sub-processor Agreements

The Processor shall:

a) Enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set out in this DPA;

b) Remain fully liable to the Controller for the performance of the Sub-processor's obligations.

6. INTERNATIONAL DATA TRANSFERS

6.1 Data Location

All personal data processed under this DPA is stored and processed within the European Union. The Processor's primary data locations are located in:

- Falkenstein, Germany

6.2 Transfer Mechanisms

In the event that any personal data is transferred outside the European Economic Area, the Processor shall ensure that:

a) The transfer is to a country that has been deemed to provide an adequate level of protection by the European Commission; or

b) Appropriate safeguards are in place, including Standard Contractual Clauses approved by the European Commission; or

c) The transfer is otherwise permitted under Article 49 of the GDPR.

6.3 Additional Safeguards

Where Standard Contractual Clauses are relied upon, the Processor shall implement supplementary measures as necessary to ensure that personal data receives an essentially equivalent level of protection as guaranteed within the EU.

7. PERSONAL DATA BREACH

7.1 Notification

In the event of a Personal Data Breach affecting personal data processed on behalf of the Controller, the Processor shall:

a) Notify the Controller without undue delay and in any event within twenty-four (24) hours of becoming aware of the breach;

b) Provide the Controller with sufficient information to enable the Controller to meet any obligations to notify Supervisory Authorities and/or Data Subjects.

7.2 Information to be Provided

The notification shall include, to the extent known:

a) A description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

b) The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

c) A description of the likely consequences of the Personal Data Breach;

d) A description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

7.3 Assistance

The Processor shall:

a) Cooperate with the Controller and take such reasonable steps as directed by the Controller to assist in the investigation, mitigation, and remediation of the Personal Data Breach;

b) Not inform any third party of the Personal Data Breach without first obtaining the Controller's prior written consent, except where required by law.

8. DATA PROTECTION IMPACT ASSESSMENTS

Where required under Article 35 of the GDPR, the Processor shall provide reasonable assistance to the Controller in conducting data protection impact assessments and, where necessary, prior consultations with Supervisory Authorities, taking into account the nature of the processing and the information available to the Processor.

9. LIABILITY

9.1 Allocation of Liability

Each Party's liability arising out of or related to this DPA shall be subject to the limitations of liability set forth in the Terms of Service.

9.2 Processor Liability

The Processor shall be liable for damages caused by processing that does not comply with the GDPR or this DPA, or where it has acted outside of or contrary to the Controller's lawful instructions.

9.3 Indemnification

Each Party agrees to indemnify and hold harmless the other Party from and against any claims, damages, losses, costs, and expenses arising from any breach of this DPA by the indemnifying Party.

10. TERM AND TERMINATION

10.1 Term

This DPA shall come into effect upon the Controller's acceptance of the Terms of Service and shall remain in effect until the termination of all service agreements between the Parties.

10.2 Survival

The obligations of the Parties under this DPA with respect to personal data processed during the term shall survive the termination of this DPA until such personal data is deleted or returned in accordance with Section 4.6.

11. GENERAL PROVISIONS

11.1 Governing Law

This DPA shall be governed by and construed in accordance with the laws of Romania, without regard to its conflict of laws provisions. The Parties submit to the exclusive jurisdiction of the courts of Satu-Mare, Romania.

11.2 Entire Agreement

This DPA, together with the Terms of Service, constitutes the entire agreement between the Parties with respect to the processing of personal data and supersedes all prior agreements and understandings.

11.3 Amendments

This DPA may only be amended in writing, signed by both Parties, except that the Processor may update this DPA from time to time to reflect changes in Data Protection Laws, provided that such updates do not materially reduce the level of protection afforded to personal data.

11.4 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

11.5 No Waiver

No failure or delay by either Party in exercising any right under this DPA shall constitute a waiver of that right.

11.6 Third-Party Rights

This DPA does not confer any rights on any person or party other than the Parties and their respective successors and permitted assigns.

12. CONTACT INFORMATION

Data Protection Officer: Email: dpo@danubedata.ro

Privacy Inquiries: Email: privacy@danubedata.ro

General Support: Email: support@danubedata.ro Website: https://danubedata.ro

SIGNATURES

This Data Processing Agreement is entered into and becomes effective as of the date of electronic acceptance.

For the Processor:

IFAS Consult SRL (DanubeData)

Signature: Digitally signed by Adrian-Flaviu-Ionut Silaghi
Date: 2026.01.05 16:26:06 +02'00'

Name: Silaghi Adrian Flaviu Ionut

Title: Founder, CEO

Date: 05.01.2025

For the Controller:

By using DanubeData services and accepting the Terms of Service, the Controller agrees to be bound by this Data Processing Agreement.

Document Information:

- Version: 1.0
- Effective Date: January 5, 2025
- Last Updated: January 5, 2025

This Data Processing Agreement is provided in accordance with Article 28 of the General Data Protection Regulation (EU) 2016/679.