DANUBEDATA

Data Processing Agreement

Pursuant to Article 28 of the General Data Protection Regulation (EU) 2016/679

Processor: IFAS Consult SRL (trading as DanubeData)
CUI: RO46614360 | **Trade Register:** J30/870/2022
Address: Str. Ilarie Chendi 28, Ap.1, 440084 Satu Mare, Romania
DPO: dpo@danubedata.ro | **Web:** https://danubedata.ro

Version: 2.1 | **Effective Date:** June 22, 2026

1. Introduction

This Data Processing Agreement ("**DPA**") forms an integral part of the Terms of Service (the "**Agreement**") between IFAS Consult SRL, a company incorporated under the laws of Romania, registered under CUI RO46614360 and Trade Register number J30/870/2022, trading as DanubeData (the "**Processor**", "we", "us", "our"), and the entity or individual accepting these terms (the "**Controller**", "Customer", "you", "your") for the provision of cloud infrastructure and managed application services.

This DPA reflects the parties' agreement with respect to the processing of Personal Data by the Processor on behalf of the Controller, in accordance with the requirements of 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 (the "**GDPR**"), and any other applicable data protection legislation.

In the event of any conflict between this DPA and the Agreement, the provisions of this DPA shall prevail with respect to the processing of Personal Data.

2. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Terms not defined herein shall have the meaning ascribed to them in the GDPR or the Agreement.

"Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'), as defined in Article 4(1) GDPR. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, as defined in Article 4(2) GDPR, including but not limited to collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

"Data Controller" (or "Controller") means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, as defined in Article 4(7) GDPR. For the purposes of this DPA, the Controller is the Customer.

"Data Processor" (or "Processor") means the natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller, as defined in Article 4(8) GDPR. For the purposes of this DPA, the Processor is IFAS Consult SRL (trading as DanubeData).

"Sub-processor" means any third party engaged by the Processor (or by any subsequent Sub-processor) to process Personal Data on behalf of the Controller in connection with the services provided under the Agreement.

"Data Subject" means an identified or identifiable natural person to whom the Personal Data relates, as defined in Article 4(1) GDPR.

"Supervisory Authority" means an independent public authority established by an EU Member State pursuant to Article 51 GDPR. The lead Supervisory Authority for the Processor is the Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP), Romania.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed, as defined in Article 4(12) GDPR.

"Special Categories of Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, as defined in Article 9(1) GDPR.

3. Scope and Purpose of Processing

3.1 Subject Matter

The Processor provides cloud infrastructure and managed application services as described in the Agreement. In the course of providing these services, the Processor may process Personal Data on behalf of the Controller. The services include, but are not limited to:

- **VPS Instances:** Virtual private servers with dedicated and shared CPU allocation options, supporting multiple Linux distributions.
- **Managed Databases:** MySQL, PostgreSQL, and MariaDB database instances with optional read replica support and automated backups.
- **Cache Instances:** Redis, Valkey, and Dragonfly in-memory data stores with optional read replicas and persistent storage.
- **Queue Instances:** Managed RabbitMQ message queues with AMQP 0-9-1, MQTT, STOMP, and WebSocket protocol support.
- **Object Storage:** S3-compatible object storage with versioning, lifecycle rules, and CORS configuration support.
- **Serverless Containers (Rapids):** Scale-to-zero container deployments with automatic TLS and custom domain support.
- **Static Sites:** Static website hosting with automated build pipelines and deployment from Git repositories.
- **Storage Share:** Managed file storage and collaboration platform (Nextcloud-based) with user management.
- **Managed Applications:** Pre-configured application hosting (e.g., n8n, WordPress, Ghost) with automated deployment and updates.
- **Volumes:** Persistent block storage volumes attached to VPS instances for additional storage capacity.
- **Snapshots & Backups:** Automated and on-demand data backup and snapshot services across all applicable resources.

3.2 Nature of Processing

The Processing activities carried out by the Processor include:

- Storage of data on infrastructure managed and operated by the Processor;
- Transmission of data through the Processor's network infrastructure;
- Backup and recovery operations, including automated snapshots and offsite backups;
- Building and deploying application containers and static assets from source code;
- Message queuing and brokering through managed message queue services;
- Execution of managed application workloads on behalf of the Controller;
- Monitoring, logging, and technical operations necessary to maintain the availability, integrity, and security of the services.

3.3 Categories of Data Subjects

The categories of Data Subjects whose Personal Data may be processed are determined entirely by the Controller and may include, without limitation, the Controller's employees, contractors, customers, suppliers, partners, end users, or any other individuals whose Personal Data the Controller stores, transmits, or otherwise processes using the services.

3.4 Types of Personal Data

The types of Personal Data processed are determined by the Controller based on the Controller's use of the services. The Processor does not control or determine the types of Personal Data that the Controller chooses to store or process. The Controller shall ensure that no Special Categories of Data are processed unless the Controller has established a valid legal basis and appropriate safeguards for such processing.

4. Processor Obligations

In accordance with Article 28 GDPR, the Processor shall:

- Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by European Union or Member State law to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement before Processing, unless prohibited by law on important grounds of public interest;
- Ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of Processing, as required by Article 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons;
- Respect the conditions referred to in Section 7 of this DPA for engaging Sub-processors, and obtain the Controller's prior general written authorisation before engaging any Sub-processor;
- Taking into account the nature of the Processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR;
- Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of Processing and the information available to the Processor;
- At the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless European Union or Member State law requires storage of the Personal Data;
- Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;
- Immediately inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes the GDPR or other European Union or Member State data protection provisions.

5. Controller Obligations

The Controller shall:

- Provide the Processor with documented instructions regarding the Processing of Personal Data, and ensure that all instructions comply with applicable data protection laws;
- Ensure that it has established a valid legal basis for the Processing of Personal Data in accordance with Articles 6 and, where applicable, Article 9 of the GDPR;
- Be solely responsible for the accuracy, quality, and legality of Personal Data and the means by which it acquires Personal Data;
- Respond to and fulfil Data Subject requests in accordance with Chapter III of the GDPR, with the assistance of the Processor where necessary;
- Carry out Data Protection Impact Assessments (DPIAs) where required by Article 35 GDPR, and consult with the relevant Supervisory Authority pursuant to Article 36 GDPR where applicable;
- Notify the Processor without undue delay of any changes to applicable data protection laws that may affect the Processor's obligations under this DPA.

6. Security Measures

Pursuant to Article 32 GDPR, the Processor implements and maintains the following technical and organisational measures to ensure a level of security appropriate to the risk. A detailed description of these measures is provided in Annex C.

6.1 Technical Measures

- Encryption of data in transit using TLS 1.2 or higher, with TLS 1.3 preferred for all communications;
- Encryption of data at rest using AES-256 encryption for object storage, volumes, and backup media;
- Network security through firewalls, Cilium network policies for tenant isolation, and intrusion detection systems;
- Regular security updates and systematic patch management across all infrastructure components;
- Automated backup systems with encrypted storage, including daily snapshots and offsite backups;
- Comprehensive access logging and monitoring via Prometheus metrics, Loki log aggregation, and Bugsnag error tracking;
- Centralised key management using HashiCorp Vault with Shamir seal (3-of-5 threshold);
- Multi-tenant isolation through dedicated Kubernetes namespaces with enforced network policies per tenant.

6.2 Organisational Measures

- Role-based access control (RBAC) with the principle of least privilege enforced across all systems;
- Mandatory confidentiality agreements for all employees and contractors with access to Personal Data;
- Regular security awareness training for all personnel handling Personal Data;

- Documented incident response procedures with defined escalation paths and communication protocols;
- Business continuity and disaster recovery planning, tested annually with quarterly backup verification;
- Annual penetration testing conducted by qualified security professionals;
- Quarterly access reviews to verify that access rights remain appropriate.

7. Sub-processors

7.1 General Authorisation

The Controller hereby grants the Processor general written authorisation to engage Sub-processors for the performance of specific Processing activities on behalf of the Controller. The current list of authorised Sub-processors is set out in Annex B to this DPA and is maintained at https://danubedata.ro/sub-processors.

7.2 Notification of Changes

The Processor shall notify the Controller at least thirty (30) days in advance of any intended changes concerning the addition or replacement of Sub-processors, by email to the Controller's registered account email address, thereby giving the Controller the opportunity to object to such changes.

7.3 Objection Right

The Controller may object to the appointment or replacement of a Sub-processor within thirty (30) days of receiving notification. If the Controller raises a reasonable objection, the Processor shall use commercially reasonable efforts to make available to the Controller a change in the services or recommend a commercially reasonable change to the Controller's use of the services to avoid Processing of Personal Data by the objected-to Sub-processor. If no such alternative is reasonably available, either party may terminate the affected portion of the services without penalty.

7.4 Sub-processor Obligations

The Processor shall ensure that each Sub-processor is bound by a written agreement that imposes data protection obligations no less protective than those set out in this DPA. The Processor shall remain fully liable to the Controller for the performance of any Sub-processor's obligations under such agreements.

8. International Data Transfers

8.1 All Personal Data processed by the Processor is stored and processed within the European Economic Area (EEA). The Processor's primary infrastructure is hosted in data centres located in Germany (Falkenstein and Nuremberg), operated by Hetzner Online GmbH, which holds ISO 27001 and SOC 1/2 Type II certifications.

8.2 Where the use of Sub-processors involves the transfer of Personal Data outside the EEA (as detailed in Annex B), the Processor ensures that appropriate safeguards are in place in accordance with Chapter V of the GDPR, including but not limited to:

- EU Standard Contractual Clauses (SCCs) as adopted by the European Commission;
- Adequacy decisions pursuant to Article 45 GDPR;
- Binding Corporate Rules pursuant to Article 47 GDPR;
- Any other transfer mechanism approved under applicable data protection law.

8.3 The Processor shall promptly inform the Controller of any changes to the legal framework governing international data transfers that may materially affect the safeguards in place.

8.4 Where Personal Data is transferred to a Sub-processor located outside the EEA, the Processor maintains a Transfer Impact Assessment documenting the considerations required under Chapter V GDPR and applicable supervisory authority guidance, including the legal regime of the destination country, the safeguards relied upon, and any supplementary technical, contractual, or organisational measures. The Processor shall make a summary of the relevant Transfer Impact Assessment available to the Controller on reasonable written request.

9. Personal Data Breach Notification

In the event of a Personal Data Breach, the Processor shall:

- Notify the Controller without undue delay, and in any event within twenty-four (24) hours of becoming aware of the Personal Data Breach;
- Provide the Controller with sufficient information to enable the Controller to comply with its obligations under Articles 33 and 34 GDPR, including: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; (c) 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;
- Cooperate with the Controller and provide all reasonable assistance in the Controller's efforts to notify the relevant Supervisory Authority within seventy-two (72) hours and, where applicable, the affected Data Subjects;
- Document the Personal Data Breach, including the facts relating to the breach, its effects, and the remedial actions taken, in accordance with Article 33(5) GDPR;
- Take all reasonable steps to contain and remediate the Personal Data Breach and to prevent recurrence.

10. Data Subject Rights

10.1 The Processor shall, taking into account the nature of the Processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR, including:

- Right of access (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure / right to be forgotten (Article 17 GDPR);
- Right to restriction of processing (Article 18 GDPR);
- Notification obligation regarding rectification, erasure, or restriction (Article 19 GDPR);
- Right to data portability (Article 20 GDPR);
- Right to object (Article 21 GDPR);
- Rights in relation to automated decision-making and profiling (Article 22 GDPR).

10.2 If the Processor receives a request from a Data Subject directly, the Processor shall promptly notify the Controller and shall not respond to the Data Subject directly without the Controller's prior written instructions, unless required by applicable law.

11. Data Protection Impact Assessment

11.1 The Processor shall provide reasonable assistance to the Controller in conducting Data Protection Impact Assessments pursuant to Article 35 GDPR, where the type of Processing is likely to result in a high risk to the rights and freedoms of natural persons.

11.2 The Processor shall provide the Controller with all information reasonably necessary to carry out such assessments, including information about the Processing operations, technical and organisational measures in place, and any relevant Sub-processor arrangements.

11.3 Where required, the Processor shall assist the Controller in prior consultation with the relevant Supervisory Authority pursuant to Article 36 GDPR.

12. Audits and Inspections

12.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and Article 28 GDPR.

12.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an independent auditor mandated by the Controller, subject to the following conditions:

- The Controller shall provide the Processor with at least thirty (30) days' prior written notice of any audit or inspection;
- Audits shall be conducted during normal business hours and in a manner that minimises disruption to the Processor's operations;
- The Controller shall bear the costs of any audit or inspection, unless the audit reveals material non-compliance by the Processor;
- All information obtained during the audit shall be treated as confidential by the Controller and the auditor;
- The scope of the audit shall be limited to the Processor's compliance with this DPA and shall not extend to the data or infrastructure of other customers of the Processor;
- Where the Processor has obtained relevant certifications or audit reports (e.g., ISO 27001, SOC 2), these may be offered as supplementary evidence of compliance, without prejudice to the Controller's right to conduct a direct audit.

13. Duration and Termination

13.1 This DPA shall come into effect on the date it is executed by both parties and shall remain in effect for the duration of the Agreement. This DPA shall automatically terminate upon the expiration or termination of the Agreement.

13.2 Upon termination or expiry of this DPA, the Processor shall, at the choice of the Controller:

- Delete all Personal Data processed on behalf of the Controller within thirty (30) calendar days, including all copies in the Processor's systems and infrastructure;
- Return all Personal Data to the Controller in a commonly used, machine-readable, and portable format, if requested by the Controller prior to deletion;
- Provide the Controller with written certification of the deletion of Personal Data upon request.

13.3 The Processor may retain Personal Data to the extent required by European Union or Member State law, provided that the Processor ensures the confidentiality of such Personal Data and processes it only for the purpose required by law.

13.4 Sections of this DPA that by their nature should survive termination shall survive, including but not limited to provisions relating to confidentiality, liability, and data deletion obligations.

14. Liability

14.1 Each party's liability arising out of or in connection with this DPA, including but not limited to liability for Personal Data Breaches, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

14.2 The Processor shall be liable for damages caused by Processing only where it has not complied with obligations of the GDPR specifically directed to processors, or where it has acted outside of or contrary to lawful instructions of the Controller, in accordance with Article 82(2) GDPR.

14.3 Each party shall indemnify the other party against any costs, claims, damages, or expenses incurred as a result of any breach of this DPA or applicable data protection law by the indemnifying party, subject to the limitations set forth in the Agreement.

14.4 The limitations and exclusions of liability set out in the Agreement and in this DPA shall not apply to the extent they would limit liability that is mandatory and cannot be excluded under applicable data protection law, including liability arising under Article 82 GDPR.

15. Governing Law and Jurisdiction

15.1 This DPA shall be governed by and construed in accordance with the laws of Romania and the applicable laws of the European Union.

15.2 Any disputes arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the competent courts of Satu Mare, Romania.

15.3 Nothing in this DPA shall affect the right of any Data Subject to lodge a complaint with a Supervisory Authority or to seek a judicial remedy in accordance with Articles 77, 78, and 79 GDPR.

16. Amendments

16.1 This DPA may only be amended by a written instrument signed by both parties, except as provided in Section 16.2.

16.2 The Processor may from time to time propose updates to this DPA. For non-material updates — including, without limitation, those reflecting changes in applicable law, regulatory guidance, updated Standard Contractual Clauses, corrections of typographical errors, changes to contact details, or other changes that do not adversely affect the Controller's rights or the protection of Personal Data — the Processor shall notify the Controller at least thirty (30) days in advance, by email to the Controller's registered account email address. If the Controller does not agree with such non-material updates, the Controller may terminate the affected services without penalty within the notice period. For material updates — including, without limitation, changes to the categories of Personal Data processed, the purposes of Processing, the security measures set out in Annex C, the rights of Data Subjects, the location of Processing, or the addition or replacement of Sub-processors (which shall be governed by Section 7) — the Processor shall obtain the Controller's prior affirmative written consent, which may be given by countersignature, electronic acceptance, or other written confirmation. Continued use of the services shall not, by itself, constitute acceptance of any material update.

17. Severability

If any provision of this DPA is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, the remaining provisions shall continue in full force and effect. The invalid

provision shall be replaced by a valid provision that most closely achieves the economic and legal purpose of the invalid provision.

18. Entire Agreement

This DPA, together with the Agreement, constitutes the entire agreement between the parties with respect to the processing of Personal Data and supersedes all prior or contemporaneous agreements, understandings, or representations, whether written or oral, relating to the subject matter hereof.

19. Contact Information

Data Processor	Contact Details
IFAS Consult SRL (trading as DanubeData) CUI: RO46614360 Trade Register: J30/870/2022 Str. Ilarie Chendi 28, Ap.1 440084 Satu Mare, Romania	**Data Protection Officer:** dpo@danubedata.ro **Privacy Inquiries:** privacy@danubedata.ro **General Contact:** contact@danubedata.ro

20. Signatures

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the date last signed below.

DATA PROCESSOR	DATA CONTROLLER
IFAS Consult SRL (trading as DanubeData) **Name:** Adrian Silaghi **Title:** Managing Director **Date: May 22**, 2026 **Signature:** Digitally signed by Adrian-Flaviu-Ionut Silaghi Date: 2026.05.22 11:04:49 +03'00'	**Company:** _____ **Name:** _____ **Title:** _____ **Date:** _____ **Signature:** _____

Annex A: Details of Processing

The following table sets out the details of the Processing carried out by the Processor on behalf of the Controller pursuant to this DPA.

Element	Description
Subject Matter	Provision of cloud infrastructure and managed application services as described in Section 3.1 of this DPA and the Agreement.
Duration	The Processing shall continue for the duration of the Agreement. Upon termination, the provisions of Section 13 of this DPA shall apply.
Nature of Processing	Storage, transmission, backup, recovery, build, deployment, message queuing, execution, and maintenance of data and workloads on infrastructure provided by the Processor, as described in Section 3.2.
Purpose of Processing	To provide, maintain, secure, and technically optimise the cloud infrastructure and managed application services in accordance with the Controller's documented instructions.
Types of Personal Data	Determined by the Controller. May include any category of Personal Data that the Controller chooses to store, transmit, or process using the services, including but not limited to: names, email addresses, telephone numbers, physical addresses, IP addresses, identifiers, financial data, health data, or any other Personal Data.
Categories of Data Subjects	Determined by the Controller. May include employees, contractors, customers, end users, suppliers, partners, or any other individuals whose data the Controller processes using the services.
Special Categories	The Controller shall determine whether Special Categories of Data are processed and shall ensure that a valid legal basis and appropriate safeguards are in place.

Annex B: Authorised Sub-Processors

The following Sub-processors are authorised by the Controller as of the effective date of this DPA. An up-to-date list is maintained at https://danubedata.ro/sub-processors.

Sub-Processor	Purpose	Data Categories	Location	Transfer Safeguard
Hetzner Online GmbH	Data centre infrastructure, networking, compute	Customer workloads, metadata, network traffic	Germany (EU)	No transfer (intra-EEA)
Bugsnag (SmartBear Software Inc.)	Application error monitoring	Error metadata, stack traces, and request context (which may incidentally include Personal Data)	United States	EU SCCs

Annex C: Technical and Organisational Measures

The following measures are implemented by the Processor pursuant to Article 32 GDPR to ensure the security of Processing. These measures are subject to continuous improvement and may be updated from time to time.

C.1 Encryption and Data Protection

- All data in transit is encrypted using TLS 1.2 or higher, with TLS 1.3 used as the default for all new connections. Mutual TLS (mTLS) is enforced for all service-to-service communication within the infrastructure.
- Data at rest is encrypted using AES-256 encryption for object storage (via Ceph RGW), persistent volumes, and all backup media.
- Cryptographic keys are managed centrally using HashiCorp Vault with a Shamir seal mechanism (3-of-5 threshold) for unseal operations, ensuring no single person can access the master key.
- All backup data, including offsite backups via Velero, is encrypted before storage.

C.2 Access Control

- Role-based access control (RBAC) is enforced across all systems, with the principle of least privilege applied to all access grants.
- Multi-factor authentication (MFA) is available for all customer accounts via TOTP and WebAuthn/FIDO2, and is required for all administrative access to infrastructure.
- SSH key-based authentication is used for VPS instance and database access, with password authentication disabled by default.
- Scoped API tokens with configurable expiration are provided for programmatic access.
- Quarterly access reviews are conducted to verify that all access rights remain appropriate and necessary.

C.3 Network Security and Tenant Isolation

- Multi-tenant isolation is enforced through dedicated Kubernetes namespaces per tenant, with Cilium network policies preventing cross-tenant network access.
- Network firewalls and DDoS mitigation systems protect all external-facing infrastructure.
- Internal service communication uses the Kubernetes internal DNS (*.svc.cluster.local) and is not exposed to the public internet.
- Customer-configurable firewall rules allow Customers to restrict access to their resources.

C.4 Monitoring, Logging, and Incident Detection

- Prometheus is used for real-time infrastructure metrics collection, with Grafana dashboards providing visibility into system health and performance.
- Loki, deployed via Alloy agents, provides centralised log aggregation with structured querying capabilities.
- Bugsnag provides application-level error monitoring with automatic alerting for critical errors.
- Immutable audit logs are retained for a minimum of ninety (90) days for all administrative and security-relevant actions.

C.5 Backup and Disaster Recovery

- Automated daily snapshots are performed for VPS instances (KubeVirt VirtualMachineSnapshot), databases, and cache instances (Kubernetes VolumeSnapshot via TopoLVM).
- Offsite backups are performed via Velero to S3-compatible object storage (Ceph RGW) with AES-256 encryption.
- Object storage data is protected through erasure coding with multi-replica distribution across storage nodes.
- Backup integrity is verified through automated restore testing to non-production environments on a quarterly basis.
- Default backup retention period is thirty (30) days.
- Documented disaster recovery procedures with defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) per service type.

C.6 Physical Security

- All infrastructure is hosted in Hetzner Online GmbH data centres in Germany (Falkenstein and Nuremberg), which hold ISO 27001 and SOC 1/2 Type II certifications.
- Data centres feature 24/7 CCTV surveillance, biometric access controls, on-site security personnel, redundant power supply (UPS and diesel generators), and environmental controls including fire suppression and climate management.

C.7 Personnel Security

- All employees and contractors with access to Personal Data are bound by confidentiality agreements that remain in force after termination of employment.
- Background verification is performed proportionate to the role and level of access to Personal Data.
- Mandatory security awareness training is provided to all personnel, with regular refresher courses.
- Access to customer data is logged and reviewed, and is limited to what is strictly necessary for the provision of support and services.

--- End of Data Processing Agreement ---