Monokee Identity and Access Management Platform – SaaS Service Management

Operations, Backup, Business Continuity and Disaster Recovery – SaaS and Dedicated SaaS

1. Introduction and Purpose

This document describes how Monokee S.r.l. ("Monokee") operates and manages the Monokee Identity and Access Management (IAM) platform delivered as a cloud service, in both the **SaaS (shared)** and **Dedicated SaaS** delivery models. It sets out the operational responsibilities of Monokee, the service availability commitments, the backup and recovery arrangements and the applicable recovery objectives, including the **Recovery Point Objective (RPO)** and the **Recovery Time Objective (RTO)**.

The management of software defects and security vulnerabilities (CVE) is described in the separate document "Support and Maintenance for the Monokee Identity and Access Management Platform – SaaS and Dedicated SaaS". The operational activities described in this document are included in the subscription fee.

This document must be read together with the "MONOKEE – Data Processing Agreement and EU Data Act Addendum (EU Customer)" (the "**DPA**"), consisting of Part A (Data Processing Agreement under the GDPR) and Part B (EU Data Act Addendum under Regulation (EU) 2023/2854). Capitalised terms not defined here have the meaning given in the DPA. In the event of conflict, the DPA prevails as regards the processing of Personal Data and the matters governed by the Data Act.

2. Operational Responsibilities

Monokee is responsible for the operation of the platform and of the cloud infrastructure on which it runs, including:

- provisioning, capacity management and scaling of the infrastructure;
- management of operating systems, databases, runtimes, container images and network components;
- 24/7 automated monitoring of the availability and performance of the platform;
- backup, replication, business continuity and disaster recovery;
- application of updates and security fixes, according to the maintenance policy in Section 8;
- management of operational incidents affecting the service.

The Customer is responsible for the configuration of its tenant or instance, for the systems and applications connected to the platform, for the management of its users and administrators and for the connectivity between its environment and the service.

2.1 Hosting architecture and data residency

The platform is deployed on two independent cloud providers, consistently with Appendix 1 of Part A and Annex B-4 of the DPA:

Component	Provider (Sub-Processor)	Location
Primary site	Microsoft Azure – Microsoft Ireland Operations Limited	EU – Italy and the Netherlands
Disaster recovery site	Amazon Web Services – Amazon Web Services EMEA SARL	EU – Italy (Milan)
Managed database service	MongoDB Atlas – MongoDB Limited (deployed on Azure, primary, and AWS, disaster recovery)	EU – Italy / the Netherlands and Italy

Customer data, including backups and replicas, are stored and processed exclusively in regions located in the European Union. Monokee does not configure replication, backup or failover to regions outside the European Union. Any change of Sub-Processor or of the hosting regions is subject to the prior notice and objection procedure set out in Section 5 of Part A of the DPA.

The deployment on two independent providers also supports the exit plan from the hosting provider described in Annex B-4 of the DPA, ensuring the continuity of the service if the use of either provider has to be discontinued.

3. Definitions

Term	Definition
Recovery Point Objective (RPO)	The maximum period of data that may be lost following an incident requiring the restoration of the platform from the available backup or recovery mechanisms.
Recovery Time Objective (RTO)	The maximum time required to restore the availability of the platform following an incident requiring the activation of the recovery or disaster recovery procedures.
Major Incident	An unplanned event that causes the total unavailability of the service, or of a primary function such as authentication, for all or a significant part of the users.
Disaster	An event that makes the primary site of the platform unusable and requires the activation of the disaster recovery procedures.
Scheduled Maintenance	Maintenance activities communicated in advance according to Section 8.
Security Incident / Personal Data Breach	Has the meaning given in Part A of the DPA.
Unplanned Downtime	Any period during which the service is unavailable, excluding Scheduled Maintenance and the exclusions listed in Section 10.

4. Service Availability

Monokee commits to a service availability of **99.794%**, measured on a monthly basis, according to the following formula:

Availability (%) = (1 – Unplanned Downtime / Total Time) × 100

Availability is measured by the Monokee monitoring systems. Any service credits are governed by the subscription terms.

5. Backup and Data Protection

- Platform data are backed up automatically with a frequency that ensures compliance with the RPO, i.e. at least every two (2) hours.
- Backups are replicated to the disaster recovery site on Amazon Web Services, separate and independent from the primary site on Microsoft Azure, and remain within the European Union.
- Backups are encrypted at rest using AES-256 or equivalent algorithms, with the multi-layer key management described in Annex B-4 of the DPA (database, infrastructure and application-level encryption with keys managed by Monokee).
- Access to backups is restricted to a limited number of authorised Monokee personnel and is logged.
- Backups are retained for fourteen (14) days on a rolling basis.
- The integrity of backups is checked regularly, and restore tests are carried out at least quarterly.

Backups are intended for the recovery of the platform following incidents and are not a service for the restore of data deleted or modified by the Customer. Requests for the restore of a tenant's data to a previous point in time are handled as described in Section 6.

5.1 Deletion of data in backups

Upon termination of the service, Customer data are deleted from the production environment in accordance with Section 8 of Part A of the DPA and, where a Switching Request has been made, at the end of the Retrieval Period in accordance with Section B.9 of Part B. Copies of the data contained in backups are deleted when the backups expire at the end of the rolling retention period of fourteen (14) days. Until then, the backups remain encrypted, isolated and protected by the security measures described in Appendix 2 of Part A, are not used for any other purpose and are not restored except where required to recover the platform. The written certification of deletion under Section 8.3 of Part A covers both the production environment and the backups.

6. Recovery Objectives

6.1 Recovery Point Objective (RPO)

Monokee applies a **Recovery Point Objective (RPO) of no more than two (2) hours** to the SaaS service.

Accordingly, in the event of a service disruption or disaster recovery scenario, the platform recovery procedures are designed to limit the potential loss of customer data to a maximum of the two hours immediately preceding the incident. The RPO applies to data managed and stored within the Monokee SaaS platform and is subject to the proper operation of the configured backup, replication and recovery mechanisms.

6.2 Recovery Time Objective (RTO)

Monokee guarantees a **Recovery Time Objective (RTO) of no more than two (2) hours** for the SaaS service.

The RTO is measured from the declaration of the Major Incident or Disaster by Monokee to the moment the service is available again to users. The declaration is made as soon as Monokee establishes that the incident cannot be resolved without activating the recovery procedures.

6.3 Recovery times by scenario

Scenario	RPO	RTO
Failure of a single component (application node, database node, network component), managed through redundancy and automatic failover	No data loss	Within 1 hour
Data corruption or loss requiring restore from backup	Up to 2 hours	Within 2 hours
Disaster: loss of the primary site, with activation of the disaster recovery site	Up to 2 hours	Within 2 hours
Restore of a tenant's data to a previous point in time at the Customer's request (for example, after an error by the Customer)	Last available backup within the retention period	Within 2 business days, quoted separately

6.4 Dedicated SaaS

The same RPO and RTO apply to the Dedicated SaaS model, unless different values are agreed in writing with the Customer. Any improved recovery objectives, for example through additional replication, can be agreed as a separate service.

7. Incident Management and Communication

In the event of a Major Incident or Disaster, Monokee:

- notifies the Customer's designated contacts within one (1) hour of the declaration of the incident;
- provides status updates at least every two (2) hours until the service is restored;
- notifies the Customer when the service has been restored, indicating any data that could not be recovered;
- delivers a post-incident report within five (5) business days, describing the causes, the impact, the actions taken and the measures adopted to prevent recurrence.

Where the incident involves a Security Incident affecting Personal Data, Monokee will notify the Customer without undue delay and in any event **within twenty-four (24) hours** of becoming aware of it, with the content set out in Section 7 of Part A of the DPA, and will cooperate with the Customer in meeting its notification obligations. Monokee will not make any public statement referencing the Customer about the incident without the Customer's prior written consent, unless required by law.

Monokee tests its disaster recovery procedures at least once a year. On request, Monokee will provide the Customer with a summary of the results of the most recent test.

8. Scheduled Maintenance

- Scheduled Maintenance is carried out during night hours, to minimize the impact on the service.
- Customers are informed at least five (5) business days in advance of Scheduled Maintenance that may cause an interruption of the service.
- All updates are verified in a test environment for at least one week before they are released into production.
- For each update Monokee prepares a rollback procedure to restore the previous state in the event of malfunctions.
- Urgent security fixes may be applied with shorter notice, according to the vulnerability management process.
- **Dedicated SaaS:** Maintenance Windows are agreed with the Customer.

9. Service Continuity during Switching and Exit

Where the Customer exercises its right to switch to another provider, to port its data to its own infrastructure or to erase its data under Part B of the DPA (EU Data Act):

- the service, including monitoring, backup and the recovery objectives set out in this document, continues to be provided in full during the Notice Period (30 calendar days) and the Transitional Period (30 calendar days, extendable in accordance with Section B.7 of Part B);
- Monokee acts with due care to maintain business continuity, informs the Customer of any known risks to continuity and maintains a high level of security for the data during their transfer and during the Retrieval Period;

- the Exportable Data are made available in the formats and with the methods described in Annex B-1 of Part B, through the open interfaces made available by Monokee;
- no Switching Charges, including Data Egress Charges, are applied. The restore of data from backup at the Customer's request described in Section 6.3 is a separate service and does not constitute a condition or charge for Switching.

10. Exclusions

The availability commitments and recovery objectives do not apply to unavailability caused by:

- Scheduled Maintenance carried out according to Section 8;
- configurations, systems, applications or networks of the Customer or of third parties connected to the platform;
- failures of internet connectivity outside the control of Monokee;
- use of the platform in breach of the subscription terms or of the documentation;
- force majeure events, as defined in the subscription terms.

11. Customer Responsibilities

- Designate and keep up to date the contacts to be notified in the event of incidents and maintenance.
- Configure the connected systems so that they can manage temporary unavailability of the service (for example retries and emergency access procedures).
- Promptly report to Monokee any malfunctions detected and any suspected Security Incident.
- Where it wishes to keep a copy of its data independent of the service, periodically export its data using the methods described in Annex B-1 of Part B of the DPA.

12. Transparency and Verification

In accordance with Section 4 of Part A of the DPA, Monokee makes available to the Customer, on request, the information needed to demonstrate compliance with this document, including a summary of the results of the most recent disaster recovery test and of the backup restore tests. The Customer may also exercise the audit rights set out in Section 4 of Part A.