MONOKEE – Data Processing Agreement and EU Data Act Addendum (EU Customer)

Part A – Data Processing Agreement (GDPR)
Part B – EU Data Act Addendum (Regulation (EU) 2023/2854)

Version 1.0 – Last updated: 19 October 2026

This document, consisting of Part A (Data Processing Agreement, the "DPA") and Part B (EU Data Act Addendum, the "Data Act Addendum"), forms part of the Agreement between:

the legal entity that has entered into the Agreement with Monokee for the provision of the Services

(The "**Customer**");

and

Monokee Srl, an Italian Company with registered office in:
Via Longhin 79
35129 Padova (PD)
Italy
(The "**Data Processor**").

Customer and Data Processor are each a "**Party**" and together the "**Parties**".

This DPA defines the terms and conditions applicable to the Processing of Personal Data made available by Customer to Data Processor for the performance of the Agreement.

This document is divided into two parts, which together form a single agreement between the Parties:

- **Part A – Data Processing Agreement**, which governs the Processing of Personal Data carried out by the Data Processor on behalf of Customer in accordance with Regulation (EU) 2016/679 (GDPR), including Appendix 1 (Description of Processing Activities) and Appendix 2 (Description of Security Measures); and
- **Part B – EU Data Act Addendum**, which governs the obligations of Monokee as provider of a data processing service under Regulation (EU) 2023/2854 (the "Data Act"), in particular switching between data processing services, data portability, interoperability and safeguards against unlawful third-country governmental access to non-personal data, including Annex B-1 to Annex B-4.

PART A

DATA PROCESSING AGREEMENT (GDPR)

DEFINITIONS

Term	Definition
“Appendix”	means an appendix to this DPA
“Agreement”	means the main agreement between the Parties under which Data Processor provides services and/or licensed products.
"Applicable Data Protection Legislation"	means any personal data protection regulation, law, order, standard and other text that applies in the context of the performance of this DPA, in particular (i) the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) howsoever incorporated into national laws and (ii) the UK GDPR; (iii) any other laws or regulations relating to the Processing of Personal Data.
"Data 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.
“Data Processing Agreement” or “DPA”	means this data processing agreement including its Appendices.
"Data Processor" or “Processor”	means the entity that Processes Personal Data on behalf of a Data Controller.
"Data Subject"	means an identified or identifiable natural person. For the purposes of this definition, 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.
“Data Transfer”	means: I. a transfer of Personal Data from the Customer to Processor; or II. an onward transfer of Personal Data from Processor to a Sub-Processor, or between two establishments of Processor or of a Sub-Processor; In each case, where such transfer would be prohibited by Applicable Data Protection Legislation in the absence of the safeguards set out in Section 6;
“EEA”	means the European Economic Area.
“GDPR”	means EU General Data Protection Regulation 2016/679;
"Personal Data"	means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject and that is Processed by Processor on Customer’s behalf under this DPA.

"Processing" or “Processed”	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, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Processing Activities"	means the Processing activities described in Appendix 1 (Description of Processing Activities).
"Purpose"	means the business purpose(s) for which Personal Data is Processed by Processor on behalf of Customer as detailed in Appendix 1.
"Security Incident" or “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 (also referred to as "Personal Data Breach" under GDPR-like regimes).
"Sensitive Personal Data"	means any Personal Data classified as sensitive under Applicable Data Protection Legislation (e.g., precise geolocation, government identifiers, certain health or financial data, biometric data, etc.), to the extent Processed under the Agreement.
“Services”	means the services provided by the Monokee IAM platform.
"Sub-Processor"	means a Data Processor of subsequent rank engaged by the Data Processor.
"Transfer Impact Assessment" or "TIA"	means, in the event of a transfer of Personal Data outside the EEA, the assessment of the Personal Data protection measures carried out by the exporter of the Personal Data in accordance with the legislation and practices of the third country of destination and the circumstances applicable to the transfer.

1. PURPOSE OF THE DPA

This DPA sets out the terms and conditions governing Processor’s Processing of Personal Data on behalf of Customer for the Purpose(s) described in Appendix 1.

2. QUALIFICATION AND ROLE OF THE PARTIES

2.1 Within the context of this DPA, Customer acts as Data Controller and Monokee Srl acts as Data Processor.

2.2 The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

2.3 Where Customer acts as Data Processor on behalf of a third party, Monokee acts as Sub Processor.

2.4 Monokee shall Process Personal Data only on documented instructions from Customer.

2.5 The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

2.6 The Parties wish to lay down their rights and obligations.

3. PROCESSOR'S OBLIGATIONS

3.1 Processor shall comply with Applicable Data Protection Legislation in relation to the Processing of Personal Data under this DPA.

3.2 Purpose limitation. Processor shall not Process Personal Data for any purpose other than the Purpose(s) set out in Appendix 1, except as permitted by Applicable Data Protection Legislation and the Agreement.

3.3 Processor shall implement and maintain throughout the term of the Agreement appropriate technical, organizational and contractual measures to ensure the security of Personal Data and prevent any Personal Data Breach. Such measures implemented by the Processor are described in Appendix 2 to the DPA. In any event, the Processor shall not decrease the level of protection brought to Personal Data during the term of the Agreement.

3.4 Customer instructs Processor to Process Personal Data for the Purposes set out in Appendix 1, in accordance with this DPA and the Agreement.

3.5 Processor shall take into account the category and sensitivity of Processed Personal Data, the risks presented by the Processing Activities, the harm that might result from a Personal Data Breach and conform to the state of the art and the best practices;

3.6 Processor shall guarantee that, by default, only Personal Data which are necessary are Processed for the Purposes defined by Data Controller;

3.7 Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Processor or of any Sub-Processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Data Protection Legislation in the context of that individual's duties to Processor or to the relevant Sub-Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.8 Immediately notify Data Controller about any request of communication of Personal Data it may receive from third parties, authorities or jurisdictions, as well as about any action and/or measures instigated by such third parties, authorities or jurisdiction regarding the Processing of Personal Data, unless such notification is prohibited by applicable law;

3.9 Actively cooperate with Data Controller to enable Data Controller to comply with the Applicable Data Protection Legislation, assess and document the compliance of the Processing of Personal Data, including by providing to Data Controller any information that Data Controller may need or that may be necessary to carry out among others a Personal Data protection impact assessment;

3.10 Immediately notify Data Controller if it believes that Data Controller instructions with respect to the Processing of Personal Data infringes any Applicable Data Protection Legislation and include sufficient details for Data Controller to assess the basis of such belief.

4. AUDIT

4.1 Data Processor shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and Applicable Data Protection Legislation.

4.2 Subject to this section 4, Processor shall make available to Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Personal Data by Processor and its Sub-Processors.

4.3 Upon reasonable prior notice (two (2) weeks unless an exception applies), Customer or an independent auditor mandated by Customer may audit Processor's compliance with this DPA, including by reviewing relevant documentation, policies, procedures, and (where necessary) by on-site inspection of facilities and systems used for the Processing Activities.

4.4 Processor may satisfy audit requirements by providing recent third-party audit reports or certifications (e.g., SOC 2 Type II, ISO/IEC 27001) to the extent they cover the Processing Activities.

5. SUB-PROCESSORS

5.1 Processor is authorized to engage the Sub-Processors listed in Appendix 1 for the Processing Activities.

5.2 Processor shall provide Customer with prior notice of any addition or replacement of a Sub-Processor and provide Customer the opportunity to object in writing within forty-five (45) calendar days of receipt of such notice.

5.3 Processor shall ensure that each Sub-Processor is bound by data protection obligations no less protective than those in this DPA, including appropriate security measures and confidentiality obligations.

5.4 Processor shall remain fully liable to Customer for the performance of its Sub-Processors' obligations.

6. PROCESSING LOCATIONS AND INTERNATIONAL TRANSFERS

6.1 The Processor shall not transfer, or authorise the transfer of, Personal Data to countries outside the European Union and/or the European Economic Area (EEA) without the prior written authorisation of the Customer. The Customer's authorisation of the Sub-Processors listed in Appendix 1 includes any transfer to, or access by, their affiliates as described in Appendix 1 and Annex B-4, subject to the safeguards set out therein.

Where Personal Data are transferred to a country outside the EEA, the Parties shall ensure that they are adequately protected in accordance with Chapter V of the GDPR, relying on: (a) an adequacy decision of the European Commission, including the EU-US Data Privacy Framework for recipients certified thereunder; or, failing that, (b) the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with any supplementary measures identified in the Transfer Impact Assessment.

7. SECURITY INCIDENT (Personal Data Breach)

7.1 Notification. Processor shall notify Customer without undue delay and in any event within twenty-four (24) hours after becoming aware of a Security Incident affecting Personal Data Processed under this DPA, unless a shorter notification period is required by Applicable Data Protection Legislation or the Agreement.

7.2 Minimum content. The notification shall include, as available: (a) contact details for the security/privacy point of contact; (b) the nature of the Security Incident; (c) categories and approximate number of affected individuals and records; (d) likely consequences; (e) mitigation measures taken or proposed; and (f) timeline and root cause analysis to the extent known.

7.3 Cooperation. The Parties shall cooperate in good faith to investigate, mitigate and remediate any Security Incident. Processor shall provide reasonable assistance to Customer to meet any notification or regulatory obligations under Applicable Data Protection Legislation.

7.4 Communications. Processor shall not make any public statement or notification to regulators or individuals regarding a Security Incident that references Customer without Customer's prior written consent, unless required by law.

8. RETRIEVAL / RETURN / DELETION

8 Subject to this Section 8, where Customer has not requested the return of Personal Data on or before the date of cessation of any Services involving the Processing of Personal Data (the "**Cessation Date**"), Processor shall promptly, and in any event within ten (10) business days of the Cessation Date, delete, and procure the deletion by its Sub-Processors of, all copies of such Personal Data. Where Customer has requested the return of Personal Data, the return and subsequent deletion shall take place within the period set out in the "Return or deletion" paragraph of this Section 8.

8.1 Retrieval. Upon Customer's request, Processor shall provide Customer, without undue delay, with a copy of Personal Data Processed under this DPA in a commonly used electronic format to enable Customer to respond to Data Subject requests.

8.2 Return or deletion. Upon expiration or termination of the Agreement, Processor shall, at Customer's option and upon request, return and/or delete Personal Data no later than thirty (30) days following Customer's request, unless retention is required by applicable law. If deletion is legally prohibited, Processor shall inform Customer and implement appropriate measures to protect the retained data and, where feasible, anonymize or de-identify it.

8.3 Backups. Personal Data contained in backup copies created in the ordinary course of operation of the Services shall not be deleted individually, but shall be deleted automatically upon expiry of the backup rotation cycle, which shall not exceed fourteen (14) calendar days from the date on which the deletion of such Personal Data from the production environment is completed under this Section 8. Until such deletion, the backup copies shall remain encrypted and protected by the security measures described in Appendix 2 and in Annex B-4, shall be isolated from active Processing, shall not be used for any purpose other than the recovery of the Services following an incident, and shall remain subject to this DPA. Where the Services are restored from a backup copy during this period, Processor shall ensure that the deleted Personal Data are not reinstated in the production environment or are promptly deleted again. Any certification issued under this Section 8 shall indicate the date by which the deletion of the backup copies will be completed.

8.4 Certification. Processor shall, upon request, certify in writing that deletion has been completed.

9. DATA PROTECTION IMPACT ASSESSMENT and PRIOR CONSULTATION

9.1 Processor shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data protection authorities, which Customer reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Applicable Data Protection Legislation, in each case solely in relation to the Processing of Personal Data by, and taking into account the nature of the Processing and the information available to, Processor and its Sub-Processors.

10. CONFLICT, GOVERNING LAW and JURISDICTION

10.1 Conflict. In the event of conflict between this DPA and the Agreement, this DPA shall prevail with respect to the Parties' data protection obligations.

10.2 Order of precedence. Appendices form an integral part of this DPA.

10.3 Governing law. This DPA shall be governed by the laws of Italy, unless the Parties agree otherwise in writing.

10.4 Any dispute arising out of or in connection with this document, including any dispute regarding its validity, interpretation, performance or termination, which the Parties are unable to resolve amicably, shall be governed by Italian law and submitted to the exclusive jurisdiction of the Courts of Padua (Italy), without prejudice to any mandatory rules of jurisdiction under applicable law.

APPENDIX 1 – DESCRIPTION OF PROCESSING ACTIVITIES

1. **Nature of the Processing carried out by Processor**

The Processing carried out by Processor may include:

- collection (as received from Customer),
- recording,
- hosting/storage,
- organization,
- structuring,
- retrieval,
- consultation,
- use,
- disclosure (as instructed),
- restriction,
- erasure/destruction,
- Other: management, support and maintenance of licensed software products.

2. **Purposes of the Processing**

Purpose No. 1: Data management within the Monokee IAM platform.
Purpose No. 2: Provision of technical support, integration assistance, maintenance and troubleshooting for the services and/or licensed products under the Agreement.

3. Categories of Personal Data Processed

Common Personal Data:

- identification data (name and surname),
- business contact details (email, role professional identifier and professional contact information),
- account identifier,
- technical/usage data (IP addresses, device identifiers, logs),
- support tickets and communications, and other data described in the Agreement.

Sensitive Personal Data (if any):

- None.

4. **Categories of Consumers/Data Subjects**

- Customer employees;
- Customer's customers/end users;
- Customer Processors;
- authorized users of products and services supplied by Customer.

5. Duration of the Processing

For the duration of the Agreement and any additional retention period required by law or as otherwise agreed in writing in the following table.

Purpose of the Processing	Duration of the Processing
Purpose n. 1	For the duration of your use of the IAM Monokee platform
Purpose n. 2	For the duration of your use of the IAM Monokee platform

6. **Processing locations**
Primary Processing location(s): Italy and the Netherlands (Microsoft Azure)
Additional location(s): Italy – Milan (Amazon Web Services)

7. **Sub-Processors and International Transfers**
Sub-Processors authorized by Customer are listed below. If any Sub-Processor processes Personal Data outside the EEA, describe the location and the transfer safeguards.

Sub-Processor (legal name & jurisdiction)	**Subsequent Sub-Processor (if any)**	**Purpose of Sub-Processing**	**Place of Sub-Processing**	**Transfer safeguards (if applicable)**
Microsoft Ireland Operations Limited	Microsoft Corporation (USA) and Microsoft affiliates, as listed in Microsoft's published sub-processor list	Provision of the cloud infrastructure (Microsoft Azure) hosting the SaaS environment for EU customers (primary site).	EU – Azure regions in Italy and the Netherlands	EU Data Boundary; Microsoft Products and Services DPA including SCC; Microsoft Corporation certified under the EU-US Data Privacy Framework. See Annex B-4.
MongoDB Limited	MongoDB, Inc. (USA) and its affiliates; the Atlas cluster is deployed on Microsoft Azure (primary) and Amazon Web Services (disaster recovery).	Provision of the managed database service (MongoDB Atlas) used to store Customer data	EU – Azure region (Italy / the Netherlands) and AWS region (Italy)	MongoDB Data Processing Agreement including SCC; MongoDB, Inc. certified under the EU-US Data Privacy Framework. See Annex B-4.
Amazon Web Services EMEA SARL	Amazon.com, Inc. (USA) and AWS affiliates, as listed in AWS's published sub-processor list.	Provision of the cloud infrastructure hosting the disaster recovery environment of the SaaS platform, including the replica of the database service.	Italy	AWS Data Processing Addendum including SCC; Amazon.com, Inc. certified under the EU-US Data Privacy Framework. See Annex B-4.
[N/A]				

APPENDIX 2 – DESCRIPTION OF SECURITY MEASURES (DT.25)

1. INFORMATION SECURITY POLICY

The objective of the Information Security Policy is to protect Monokee's information in a manner that ensures the highest level of availability and guarantees the confidentiality and integrity of all information handled. This policy concerns the management of information security at all Monokee workplaces, including remote work, and applies to all company personnel, consultants, interns, and anyone (including third-party collaborators) who is granted access to Monokee information.

The Information Security Policy is reviewed during Management Review.

2. General Objectives Pursued by Monokee through the Information Security Management System

- continuously improve information security, particularly with respect to availability, integrity, and confidentiality;
- maintain up-to-date information systems aligned with the current state of the art, for both information management and information security;
- train and inform relevant stakeholders on the Information Security Management System and on information security topics;
- ensure the highest levels of cybersecurity for all stakeholders, in compliance with applicable regulations and standards (GDPR, NIS2, DORA, etc.);
- ensure secure and user-friendly access to information;
- keep all specific information security policies updated in line with technological changes.

3. Monokee Management is committed to:

- continually improving its Information Security Management System;
- meeting customer requirements, applicable legal and regulatory obligations, and all information-security-related requirements.

Implementation of the Information Security Policy

4. Hardware

- hardware is identified, classified, and inventoried;
- hardware purchases must be approved by Management;
- hardware installation must be performed by personnel authorized by the CISO.

5. Software (operating systems and applications)

- software is protected from cyberattacks through appropriate means (antivirus, antispyware, antispam, etc.);
- software is subject to access control;
- input and output data are evaluated for accuracy and consistency; where possible, automated controls are implemented to verify input and output correctness;
- software installations require approval from the CISO, except for software installed by technicians for strictly necessary operational needs;
- software management is regulated by specific information security policies;
- software is continuously updated;
- where feasible, software updates must be tested in a test environment before being deployed in production.

6. Networks

- network access is authenticated with personal credentials;
- networks are appropriately segmented.

7. Company Accounts

- the management of company accounts is regulated by a specific information security policy and a dedicated management procedure.

8. Access Control and Authentication Credential Management

- access control and authentication credential management are regulated by specific information security policies and a dedicated management procedure.

9. Remote Work

- remote work is regulated by a specific information security policy.

10. Cryptographic Controls and Keys

- the use of cryptographic controls is regulated by a dedicated procedure.

11. Clean Screen and Clean Desk

- the correct management of clean desk and clean screen practices is regulated by a specific information security policy.

12. Malware Protection

- malware protection is regulated by a specific information security policy and a dedicated management procedure.

13. Notebooks, Netbooks, Ultrabooks, Laptops, Desktops, Tablets

- the use of these devices is regulated by specific information security policies.

14. Bluetooth and Wireless Devices

- the use of wireless and Bluetooth devices is regulated by a specific information security policy.

15. Removable Storage Media Containing Personal Data

- the use of removable storage media containing personal data is regulated by a specific information security policy.

16. Smartphones

- smartphone use is regulated by a specific information security policy.

17. Landline Phones

- landline phone use is regulated by a specific information security policy.

18. Uninterruptible Power Supply (UPS)

- operating systems are supported by equipment capable of guaranteeing continuity of electrical power supply even in case of blackout.

19. Databases

- databases are identified, classified, and inventoried;
- databases are protected against cyberattacks;
- databases are subject to access control;
- databases require CISO approval.

20. Backups

- responsibilities and methods for performing backups are defined in the ISMS documentation.
- backups of the platform data are performed automatically at least every two (2) hours;
- backups are replicated to the disaster recovery site, separate and independent from the primary site, and remain within the European Union;
- backups are encrypted at rest and access to them is restricted to authorized personnel and logged;
- backups are retained for fourteen (14) calendar days on a rolling basis and are then automatically deleted;
- the integrity of backups is checked regularly and restore tests are carried out at least quarterly.

21. Physical Security

- appropriate security measures have been defined for server rooms;
- authorization methods have been defined for access to information-security-critical premises and to company facilities;
- security systems have been implemented to prevent theft, flooding, fire, intrusion, and overheating.

22. Internet Usage

- Internet use is regulated by a specific information security policy.

23. Email Usage

- email use is regulated by a specific information security policy, regardless of the device used (desktop, notebook, smartphone, etc.).

24. Privacy

- all actions required to comply with Legislative Decree 196/03 and EU Regulation 2016/679 (GDPR) have been implemented;
- the organization's personal data management policies are observed;
- only the data necessary and sufficient for task execution is used;
- personnel are made aware of their duty to maintain the utmost confidentiality regarding personal data they access in the course of their duties, during and after their employment;
- instructions for data processing are defined in the appointment of processors and authorized personnel.

25. Management of Paper Documents

- the management of paper documents is regulated by a specific information security policy.

26. Personnel Responsibilities

Personnel must:

- comply with information security policies and all prescribed documentation provided by Monokee;
- access only information relevant to their job role;
- communicate or disseminate only the information Monokee has authorized, or that is strictly required for job execution, and only to individuals indicated by Monokee or strictly necessary recipients;
- report any violations or errors that may compromise information security;
- not use colleagues' or consultants' accounts to access services;

- protect paper documents and IT media containing company data (USB drives, external hard drives, etc.);
- upon resignation or termination, return all Monokee IT equipment and delete all Monokee-owned data possibly stored on personal devices.

27. Personnel Training and Awareness

Personnel must:

- actively participate in training provided by Monokee;
- propose relevant training initiatives useful to improve skills or fill gaps;
- carefully read all documents provided by the company.

28. Ethics

- A code of ethics is available.

29. Cybercrime

- Requirements to prevent or reduce cybercrime risk are detailed in a specific document.

30. Outsourcing

- Contracts with third parties include confidentiality agreements and specify required information security measures;
- where possible, security measures implemented by the supplier are verified.

31. Use by Third Parties of Monokee Systems and Information

- Contracts with third parties who use Monokee systems or information include confidentiality agreements and specify information security requirements;
- where possible, the security measures implemented by the supplier are verified;
- access authorization to third parties (e.g., authentication credentials) is regulated.

32. Use of Cryptographic Controls

- Requirements for cryptographic controls are defined in a dedicated management procedure.

PART B

EU DATA ACT ADDENDUM – REGULATION (EU) 2023/2854

B.1 PURPOSE AND SCOPE

B.1.1 This Part B (the "**Data Act Addendum**") sets out the terms and conditions under which Monokee, in its capacity as provider of a data processing service within the meaning of Article 2(8) of the Data Act, complies with the obligations laid down in Chapter VI (Articles 23 to 31), Article 32 and Article 34 of the Data Act in relation to the Services provided to Customer under the Agreement.

B.1.2 This Data Act Addendum applies to all data and Digital Assets of Customer processed by Monokee in the provision of the Services, whether such data qualify as Personal Data or as Non-Personal Data. To the extent that such data include Personal Data, Part A continues to apply in full.

B.1.3 The Parties acknowledge that the Services consist of a cloud-based identity and access management (IAM) platform delivered as software-as-a-service and do not involve the placing on the market of connected products or the provision of related services within the meaning of Article 2(5) and Article 2(6) of the Data Act. Accordingly, Chapters II and III of the Data Act do not apply to the Services. Should Monokee provide connected products or related services to Customer in the future, the Parties shall amend this Data Act Addendum in good faith.

B.1.4 Nothing in this Data Act Addendum shall be construed as requiring Monokee to disclose trade secrets other than in accordance with the Data Act, or as granting Customer any right in Monokee's intellectual property beyond those expressly granted under the Agreement.

B.2 DEFINITIONS

Capitalised terms used but not defined in this Part B shall have the meaning given to them in Part A or in the Agreement. In this Part B, the following terms shall have the following meanings:

Term	Definition
"Data Act"	means Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, as amended from time to time.
"Data Processing Service"	has the meaning given in Article 2(8) of the Data Act and, for the purposes of this Part B, means the Services provided by Monokee under the Agreement.
"Data Egress Charges"	means data transfer fees charged to customers for extracting their data through the network from the ICT infrastructure of a provider of data processing services to the system of a different provider or to on-premises ICT infrastructure (Article 2(35) of the Data Act).
"Destination Provider"	means the provider of data processing services to which Customer decides to switch.
"Digital Assets"	means elements in digital form, including applications, for which Customer has the right of use, independently from the contractual relationship with the Data Processing Service it intends to switch from (Article 2(32) of the Data Act).
"Exportable Data"	means the input and output data, including metadata, directly or indirectly generated, or co-generated, by Customer's use of the Data Processing Service, excluding any assets or data of Monokee or of a third party that are protected by intellectual property rights or constitute a trade secret (Article 2(38) of the Data Act), as further specified in Annex B-1.
"Non-Personal Data"	means data other than Personal Data (Article 2(3) of the Data Act).
"Notice Period"	has the meaning given in Section B.6.1.

Term	Definition
"On-Premises ICT Infrastructure"	means ICT infrastructure and computing resources owned, rented or leased by Customer, located in the data centre of Customer itself and operated by Customer or by a third party (Article 2(33) of the Data Act).
"Online Register"	means the up-to-date online register hosted by Monokee in a restricted area, made available to Customer before the conclusion of the Agreement and thereafter upon request, containing details of all data structures and data formats as well as the relevant standards and open interoperability specifications in which the Exportable Data are available (Article 26(b) of the Data Act).
"Retrieval Period"	has the meaning given in Section B.9.1.
"Switching"	means the process involving Monokee as source provider, Customer and, where relevant, a Destination Provider, whereby Customer changes from using the Data Processing Service to using another data processing service of the same service type, or other service, offered by a different provider, or to an On-Premises ICT Infrastructure, including through extracting, transforming and uploading the data (Article 2(34) of the Data Act).
"Switching Charges"	means charges, other than standard service fees or early termination penalties, imposed by Monokee on Customer for the actions mandated by the Data Act for switching to the systems of a different provider or to On-Premises ICT Infrastructure, including Data Egress Charges (Article 2(36) of the Data Act).
"Switching Request"	means the written notice given by Customer in accordance with Section B.5.2.
"Transitional Period"	has the meaning given in Section B.7.1.

B.3 RELATIONSHIP WITH PART A, THE GDPR AND THE AGREEMENT

B.3.1 Part A and Part B form a single agreement and shall be read together. Part A governs the Processing of Personal Data; Part B governs Monokee's obligations under the Data Act. References in Part A to "this DPA" shall be read as references to Part A.

B.3.2 In accordance with Article 1(5) of the Data Act, this Part B is without prejudice to the GDPR. In the event of conflict between Part B and Part A in relation to the Processing of Personal Data, Part A and the Applicable Data Protection Legislation shall prevail. Any Processing of Personal Data carried out in the context of Switching (including the export of Personal Data, its transfer to a Destination Provider and its erasure) is a Processing Activity carried out on behalf of Customer, on the basis of Customer's documented instructions and in accordance with Part A.

B.3.3 **Interplay with Section 8 of Part A.** A Switching Request constitutes Customer's documented instruction to Monokee to retain the Personal Data included in the Exportable Data for the duration of the Notice Period, the Transitional Period and the Retrieval Period. Accordingly, where a Switching Request has been made, the deletion periods set out in Section 8 (Retrieval / Return / Deletion) of Part A – including the period of ten (10) business days following the Cessation Date – shall start to run only upon expiry of the Retrieval Period (or of any longer period agreed under Section B.9.3). The certification obligations under Section 8 of Part A remain unaffected.

B.3.4 In the event of conflict between this Part B and the Agreement, this Part B shall prevail as regards the matters governed by the Data Act. Any term of the Agreement that is contrary to Chapter VI of the Data Act – including any term that hinders, delays or makes Switching subject to conditions not permitted under the Data Act – shall not apply to the extent of such conflict.

B.4 INFORMATION AND TRANSPARENCY

B.4.1 In accordance with Article 26 of the Data Act, Monokee shall provide Customer, before the conclusion of the Agreement and thereafter upon request, with:

(a) information on the available procedures for Switching and porting to the Data Processing Service, including information on the available switching and porting methods and formats, as well as the restrictions and technical limitations which are known to Monokee; and

(b) a reference to the Online Register.

B.4.2 In accordance with Article 28 of the Data Act, Monokee shall make available on its website, and keep up to date: (a) the jurisdiction to which the ICT infrastructure deployed for the data processing of the Services is subject; and (b) a general description of the technical, organisational and contractual measures adopted by Monokee to prevent international governmental access to, or transfer of, Non-Personal Data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State. The relevant web addresses are set out in Annex B-3 and are incorporated in this document by reference.

B.4.3 In accordance with Article 29(4) of the Data Act, Monokee shall provide Customer, before the conclusion of the Agreement, with clear information on the standard service fees and early termination penalties that might be imposed. Monokee confirms that no Switching Charges apply, as set out in Section B.10 and Annex B-3.

B.4.4 Monokee shall inform Customer in writing of any material change to the information referred to in Sections B.4.1 to B.4.3 no later than thirty (30) calendar days after such change takes effect.

B.5 CUSTOMER'S RIGHT TO SWITCH, PORT OR ERASE

B.5.1 Customer may, at any time and without undue obstacles, decide to:

(a) switch to a data processing service offered by a different provider, in which case Customer shall provide the necessary details of that Destination Provider;

(b) port all its Exportable Data and Digital Assets to an On-Premises ICT Infrastructure; or

(c) erase its Exportable Data and Digital Assets.

B.5.2 Customer shall exercise the rights under Section B.5.1 by sending a Switching Request in writing to the switching contact point indicated in Annex B-3. The Switching Request shall specify the option chosen under Section B.5.1, the details of the Destination Provider (where applicable) and, where possible, the desired timing.

B.5.3 In accordance with Article 23 of the Data Act, Monokee shall not impose, and shall remove, any pre-commercial, commercial, technical, contractual or organisational obstacle which inhibits Customer from: (a) terminating the Agreement, after the Notice Period and the successful completion of Switching; (b) concluding new contracts with a different provider covering the same service type; (c) porting its Exportable Data and Digital Assets to a different provider or to an On-Premises ICT Infrastructure; and (d) unbundling, where technically feasible, the Services from other data processing services provided by Monokee.

B.5.4 In accordance with Article 25(2)(c) of the Data Act, the Agreement shall be considered terminated with respect to the Services concerned, and Monokee shall notify Customer of such termination: (a) upon the successful completion of Switching; or (b) at the end of the Notice Period, where Customer does not wish to switch but to erase its Exportable Data and Digital Assets upon termination of the Services.

B.6 NOTICE PERIOD

B.6.1 The notice period for the initiation of the Switching process shall be Thirty (30) calendar days from Monokee's receipt of the Switching Request (the "**Notice Period**") and shall in no event exceed two (2) months.

B.6.2 During the Notice Period the Services shall continue to be provided in accordance with the Agreement, and the Parties shall agree in good faith a switching plan setting out the activities, responsibilities and timeline of the Switching process, involving the Destination Provider where relevant.

B.7 TRANSITIONAL PERIOD AND SWITCHING ASSISTANCE

B.7.1 Upon expiry of the Notice Period, Monokee shall enable Customer to switch, or to port all its Exportable Data and Digital Assets to an On-Premises ICT Infrastructure, without undue delay and in any event within thirty (30) calendar days (the "**Transitional Period**"), during which the Agreement shall remain applicable.

B.7.2 During the Transitional Period, Monokee shall:

(a) provide reasonable assistance to Customer and to third parties authorised by Customer in the Switching process;

(b) act with due care to maintain business continuity and continue the provision of the functions or services under the Agreement;

(c) provide clear information concerning known risks to continuity in the provision of the functions or services on its part; and

(d) ensure that a high level of security is maintained throughout the Switching process, in particular the security of the data during their transfer and the continued security of the data during the Retrieval Period, in accordance with the security measures described in Appendix 2 of Part A.

B.7.3 In accordance with Article 25(2)(b) of the Data Act, Monokee shall support Customer's exit strategy relevant to the Services, including by providing all relevant information.

B.7.4 **Technical unfeasibility.** Where the Transitional Period of thirty (30) calendar days is technically unfeasible, Monokee shall notify Customer within fourteen (14) working days after the Switching Request has been made, shall duly justify the technical unfeasibility with a detailed report and shall indicate an alternative transitional period, which shall not exceed seven (7) months. Business continuity shall be ensured throughout the alternative transitional period.

B.7.5 **Extension by Customer.** Without prejudice to Section B.7.4, Customer shall have the right to extend the Transitional Period once, for a period that Customer deems more appropriate for its own purposes. The standard service fees under the Agreement shall continue to apply to the Services provided during any such extension.

B.7.6 **Customer cooperation.** Customer shall provide Monokee in a timely manner with the information and cooperation reasonably necessary for the Switching process and shall procure the cooperation of the Destination Provider. Monokee shall not be responsible for delays or failures attributable to Customer or to the Destination Provider.

B.8 EXPORTABLE DATA AND DIGITAL ASSETS

B.8.1 Annex B-1 contains an exhaustive specification of all categories of data and Digital Assets that can be ported during the Switching process, including, at a minimum, all Exportable Data (Article 25(2)(e) of the Data Act).

B.8.2 Annex B-2 contains an exhaustive specification of the categories of data specific to the internal functioning of the Services that are exempted from the Exportable Data where a risk of breach of Monokee's trade secrets exists (Article 25(2)(f) of the Data Act). Such exemptions shall not impede or delay the Switching process.

B.8.3 Exportable Data shall be made available in a structured, commonly used and machine-readable format, as described in the Online Register and in Annex B-1.

B.8.4 **Authentication secrets.** Given the nature of the Services, certain categories of authentication secrets (such as password hashes, multi-factor authentication seeds and cryptographic keys) may be subject to technical or security restrictions on export. Such restrictions, if any, are identified in Annex B-1 and in the information provided under Section B.4.1(a). Where a category cannot be exported without compromising the security of the data or of the Data Subjects, Monokee shall offer reasonable alternative migration support (for example, assisted credential reset or re-enrolment procedures) so that the Switching process is not impeded.

B.9 DATA RETRIEVAL PERIOD AND ERASURE

B.9.1 Customer may retrieve its Exportable Data and Digital Assets during a period of thirty (30) calendar days – in any event not shorter than thirty (30) calendar days – starting after the end of the Transitional Period, as possibly extended under Section B.7.4 or B.7.5 (the "**Retrieval Period**").

B.9.2 Upon expiry of the Retrieval Period, or of any later period agreed under Section B.9.3, and provided that the Switching process has been successfully completed, Monokee guarantees the full erasure of all Exportable Data and Digital Assets generated directly by Customer or relating to Customer directly. Monokee shall certify the erasure in writing in accordance with Section 8 of Part A.

B.9.3 The Parties may agree in writing on a retrieval period longer than the Retrieval Period.

B.9.4 Where Customer has chosen erasure under Section B.5.1(c), Monokee shall erase the Exportable Data and Digital Assets upon termination under Section B.5.4(b) and certify such erasure in writing.

B.9.5 Sections B.9.2 and B.9.4 are without prejudice to any retention obligation imposed on Monokee by Union or Member State law, in which case Section 8 of Part A applies.

B.10 SWITCHING CHARGES

B.10.1 From 12 January 2027, Monokee shall not impose any Switching Charges, including Data Egress Charges, on Customer for the Switching process (Article 29(1) of the Data Act).

B.10.2 Monokee does not apply any Switching Charges, including Data Egress Charges, to Customer. This also applies to the period until 11 January 2027 during which reduced Switching Charges would be permitted under Article 29(2) of the Data Act.

B.10.3 Standard service fees due under the Agreement for the Services provided during the Notice Period and the Transitional Period (including any extension thereof) do not constitute Switching Charges.

B.10.4 **Parallel use.** Where Customer uses the Services in parallel with another data processing service, Monokee may impose Data Egress Charges only for the purpose of passing on egress costs incurred, without exceeding such costs (Article 34 of the Data Act).

B.11 INTEROPERABILITY AND OPEN INTERFACES

B.11.1 In accordance with Article 30(2) of the Data Act, Monokee shall make open interfaces available to an equal extent to all its customers and to the concerned Destination Providers, free of charge, to facilitate the Switching process. Such interfaces shall include sufficient information on the Services to enable the development of software to communicate with the Services for the purposes of data portability and interoperability.

B.11.2 In accordance with Article 30(3) of the Data Act, Monokee shall ensure compatibility with common specifications based on open interoperability specifications, or with harmonised standards for interoperability, at the latest twelve (12) months after the references to such specifications or standards are published in the central Union standards repository for the interoperability of data processing services.

B.11.3 Monokee shall keep the Online Register up to date in line with the evolution of the Services and of the applicable specifications and standards.

B.12 INTERNATIONAL GOVERNMENTAL ACCESS TO NON-PERSONAL DATA

B.12.1 In accordance with Article 32 of the Data Act, Monokee shall take all adequate technical, legal and organisational measures, including contracts, to prevent international and third-country governmental access to, and transfer of, Non-Personal Data held in the Union where such access or transfer would create a conflict with Union law or with the national law of the relevant Member State, without prejudice to Sections B.12.2 and B.12.3.

B.12.2 Any decision or judgment of a third-country court or tribunal, and any decision of a third-country administrative authority, requiring Monokee to transfer or give access to Non-Personal Data held in the Union shall be recognised or enforceable only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, or between the requesting third country and a Member State.

B.12.3 In the absence of such an international agreement, Monokee shall transfer or give access to Non-Personal Data only where the conditions set out in Article 32(3) of the Data Act are met and, in such case, shall provide the minimum amount of data permissible in response to the request, based on a reasonable interpretation of the request.

B.12.4 Monokee shall inform Customer about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

B.12.5 Monokee shall impose on its Sub-Processors and subcontractors involved in the provision of the Services contractual obligations consistent with this Section B.12, to the extent permitted by the standard terms of such providers, and shall describe the resulting measures in the information made available under Section B.4.2.

B.12.6 As regards Personal Data, requests from third-country authorities shall be handled in accordance with Part A (including Sections 3 and 6) and Chapter V of the GDPR.

B.12.7 The technical, contractual and organisational measures adopted by Monokee pursuant to this Section B.12, including those relating to its hosting Sub-Processors, are described in Annex B-4, which forms an integral part of this Part B.

B.13 FAIR CONTRACTUAL TERMS

B.13.1 In accordance with Article 13 of the Data Act, any contractual term of the Agreement concerning access to and use of data, or liability and remedies for the breach or the termination of data-related obligations, which has been unilaterally imposed by one Party on the other and which is unfair within the meaning of Article 13 of the Data Act, shall not be binding on the latter Party.

B.13.2 Where any such term is severable from the remaining terms of the Agreement or of this document, the remaining terms shall continue to be binding.

B.14 GOOD FAITH COOPERATION AND TRADE SECRETS

B.14.1 In accordance with Article 27 of the Data Act, the Parties – and, where relevant, the Destination Provider – shall cooperate in good faith to make the Switching process effective, enable the timely transfer of data and maintain the continuity of the Services.

B.14.2 Data and assets of Monokee protected by intellectual property rights or constituting trade secrets are excluded from the Exportable Data. Customer shall ensure that any information on the Services received in the context of Switching is used only for the purposes of Switching and is kept confidential in accordance with the Agreement, also by any Destination Provider and third party authorised by Customer.

B.15 TERM, AMENDMENTS, GOVERNING LAW

B.15.1 This Part B shall remain in force for the duration of the Agreement and, in the event of Switching or erasure, until the completion of the Retrieval Period and of the erasure under Section B.9.

B.15.2 The Parties shall negotiate in good faith any amendment to this Part B that may become necessary to reflect implementing or delegated acts, guidelines or model contractual terms adopted by the European Commission, or common specifications and harmonised standards adopted under the Data Act.

B.15.3 Without prejudice to Customer's right to lodge a complaint with the competent authority designated by Italy pursuant to Article 37 of the Data Act, Section 10 (Conflict, Governing Law and Jurisdiction) of Part A applies to this Part B mutatis mutandis.

B.15.4 Monokee may update this document from time to time, in particular to reflect changes in applicable law, in the Sub-Processors or in the Services. The current version is published at https://www.monokee.com/DPA-EU_DATA_Act. Monokee shall notify Customer of any material change at least thirty (30) calendar days before it takes effect. Changes shall not reduce the level of protection of Customer data. Where Customer reasonably objects to a material change on data protection grounds, the procedure set out in Section 5 of Part A shall apply *mutatis mutandis*. Changes required by applicable law shall apply from the date required by such law.

ANNEX B-1 – EXPORTABLE DATA AND DIGITAL ASSETS

The following categories of data and Digital Assets can be ported during the Switching process.

Category	Description	Format / standard	Export method
Identity data	User accounts, profile attributes (including custom attributes), account status and related identifiers	JSON	DB Export/ REST API
Groups, roles and entitlements	Group definitions and memberships, role definitions and assignments, entitlements	JSON	DB Export/ REST API
Application and federation configuration	Configured applications and service providers, attribute mappings, SAML 2.0 metadata, OpenID Connect / OAuth 2.0 client registrations	XML (SAML metadata), JSON	DB Export/ REST API
Access and authentication policies	Access policies, authentication rules, MFA policies and other policy configuration defined by Customer	JSON	DB Export/ REST API
Provisioning and workflow configuration	Connector configurations, provisioning rules and workflows defined by Customer	JSON	DB Export/ REST API
Audit and activity logs	Authentication events, administrative activity and access logs relating to Customer's tenant, within the applicable retention period	JSON	DB Export/ REST API
Branding and customisation	Logos, templates, custom texts and other content uploaded or created by Customer	HTML / JSON	DB Export/ REST API
Metadata	Timestamps, identifiers and other metadata associated with the above categories	JSON	DB Export/ REST API
Authentication secrets	Password hashes (including hashing algorithm and parameters), where technically and contractually permissible. MFA seeds and FIDO2/passkey private keys are not exportable for security reasons or because they are held on the user's authenticator; FIDO2 public key credentials and certificate metadata are exportable. For non-exportable items, alternative migration support is provided under Section B.8.4.	JSON	DB Export
Digital Assets	Scripts, custom connectors, templates and other Digital Assets for which Customer holds the right of use	Original format	Upon request

ANNEX B-2 – DATA EXEMPTED FROM EXPORTABLE DATA

The following categories of data are specific to the internal functioning of the Services and are exempted from the Exportable Data where a risk of breach of Monokee's trade secrets exists. These exemptions shall not impede or delay the Switching process.

- source code, object code, architecture and internal algorithms of the Monokee IAM platform, including the logic and models used for risk-based or adaptive authentication;
- internal system and infrastructure logs, telemetry, monitoring and performance data of Monokee that do not relate directly to Customer's tenant;
- cryptographic keys, signing keys and private keys managed by Monokee for the operation of the platform (without prejudice to any key material provided by Customer, which shall be returned or exported where technically feasible);
- internal security configurations, detection rules and threat intelligence of Monokee;
- aggregated or anonymised statistical data derived from the use of the platform across multiple customers.

ANNEX B-3 – SWITCHING INFORMATION, CONTACTS AND ONLINE REFERENCES

Item	Details
Switching contact point (Section B.5.2)	CTO – privacy@monokee.com
Online Register of data structures, formats and standards (Article 26(b))	Hosted by Monokee in a restricted online area. Access is provided to Customer before the conclusion of the Agreement and thereafter upon request to privacy@monokee.com . Pending activation of the online area, the register is provided as an electronic document.
Jurisdiction of the ICT infrastructure and measures against unlawful governmental access (Article 28)	https://www.monokee.com/DPA-EU_DATA_Act - see Annex B-4.
Jurisdiction of the ICT infrastructure	European Union – Italy and the Netherlands (Microsoft Azure, primary site); Italy (Amazon Web Services, disaster recovery site). Consistent with Appendix 1 of Part A.
Notice Period (Section B.6.1)	Thirty (30) calendar days
Transitional Period (Section B.7)	Thirty (30) calendar days; up to seven (7) months where technically unfeasible; extendable once by Customer
Retrieval Period (Section B.9.1)	thirty (30) calendar days – minimum thirty (30) calendar days
Switching Charges (Section B.10)	None, including during the period until 11 January 2027 (Section B.10.2)
Standard service fees and early termination penalties (Article 29(4))	Standard service fees are set out in the Agreement and in the applicable price list. No early termination penalties apply.
Known restrictions and technical limitations (Article 26(a))	(a) MFA seeds and FIDO2/passkey private keys cannot be exported (Annex B-1 and Section B.8.4); (b) password hashes are exported together with the hashing algorithm and parameters, and may not be usable by a Destination Provider that does not support the same algorithm; (c) audit and activity logs are available only within the applicable retention period; (d) data listed in Annex B-2 are excluded; (e) Digital Assets are exported upon request in their original format.

ANNEX B-4 – MANAGEMENT OF THIRD-COUNTRY GOVERNMENTAL ACCESS RISK (US CLOUD ACT)

This Annex describes how Monokee identifies, mitigates and monitors the risk that authorities of countries outside the European Union obtain access to, or the transfer of, Customer data processed in the provision of the Services. It applies to both Personal Data (Part A and Chapter V of the GDPR, including Article 48 GDPR) and Non-Personal Data (Articles 28 and 32 of the Data Act).

1. Context and risk description

1.1 The Services are hosted on Microsoft Azure data centres located in the European Union (Italy and the Netherlands), which serve as the primary site, and are replicated in full on Amazon Web Services data centres located in the European Union (Italy), which serve as the disaster recovery site. Microsoft Ireland Operations Limited and Amazon Web Services EMEA SARL act as Sub-Processors; their ultimate parent companies, Microsoft Corporation and Amazon.com, Inc., are established in the United States of America. The managed database service is provided by MongoDB Limited (Ireland), whose ultimate parent company, MongoDB, Inc., is also established in the United States of America. Microsoft Corporation, Amazon.com, Inc. and MongoDB, Inc. are together referred to in this Annex as the "**US Parent Companies**".

1.2 As companies subject to US jurisdiction, the US Parent Companies may receive orders from US authorities requiring the disclosure of data within their possession, custody or control, irrespective of where such data are stored, in particular under the Clarifying Lawful Overseas Use of Data Act ("**CLOUD Act**", 18 U.S.C. § 2713) and, for electronic communications service providers, Section 702 of the Foreign Intelligence Surveillance Act ("**FISA 702**"), as amended or reauthorised from time to time.

1.3 Compliance with such orders may conflict with Article 48 GDPR and Article 32 of the Data Act, which require that third-country decisions requiring the transfer of or access to data held in the Union be based on an international agreement in force between the requesting country and the Union or a Member State. The resulting conflict of laws cannot be entirely eliminated by contractual means; this Annex therefore aims to reduce the likelihood and the impact of such access to a level that Monokee considers acceptable, and to ensure transparency towards Customer on the residual risk.

1.4 Monokee S.r.l. is a company established in Italy.

2. Risk assessment

2.1 Monokee assesses the risk of third-country governmental access through the Transfer Impact Assessment (TIA) referred to in Part A, taking into account: (a) the categories and sensitivity of the data processed (Appendix 1 of Part A and Annex B-1); (b) the legal framework of the third country concerned and the safeguards available; (c) the contractual commitments of the Sub-Processors; (d) the technical measures in place, in particular encryption and key management; and (e) publicly available information on the number and type of governmental requests received by the Sub-Processors.

2.2 The TIA is documented, made available to Customer upon request and reviewed in accordance with Section 9.

3. Technical measures

3.1 **Data residency.** Customer data are stored and processed exclusively in Microsoft Azure and Amazon Web Services regions located in the European Union, both for the primary site and for the disaster recovery site. Monokee does not configure replication, backup or failover to regions outside the European Union.

3.2 **Encryption in transit.** All data are transmitted using TLS version 1.2 or higher.

3.3 **Encryption at rest.** All data at rest, including backups, are encrypted using AES-256 or equivalent algorithms. Backups are stored in the European Union, retained for fourteen (14) calendar days on a rolling basis and then automatically deleted, in accordance with Section 8.3 of Part A.

3.4 **Key management.** Encryption at rest is applied at several layers: (a) database encryption at rest is managed by MongoDB Atlas; (b) disk encryption of the virtual machines is managed by Microsoft Azure and by Amazon Web Services, respectively (platform-managed keys); and (c) at application level, Monokee applies its own encryption using keys generated and managed by Monokee, on both the primary and the disaster recovery site. Access to application-level keys is restricted to a limited number of authorised Monokee personnel and is logged.

3.5 **Data minimisation and pseudonymisation.** Monokee processes only the data necessary for the Services and applies pseudonymisation where technically feasible, in particular to logs and data used for support and analytics.

3.6 **Control of provider access.** Where available for the services used, Monokee activates features requiring Monokee's explicit approval for any access by Microsoft personnel to Customer data (such as Customer Lockbox) and equivalent controls, where available, on Amazon Web Services and monitors administrative access logs.

4. Contractual measures

4.1 Monokee relies on the Microsoft Products and Services Data Protection Addendum in force between Monokee and Microsoft, including the Standard Contractual Clauses and the additional safeguards contained therein, under which Microsoft commits, among other things, to: (a) redirect governmental requests to the customer where possible; (b) notify the customer of a request unless legally prohibited; (c) use all lawful efforts to challenge requests, including where they conflict with Union or Member State law; and (d) disclose only the minimum amount of data required.

4.1-bis Monokee also relies on the AWS Data Processing Addendum in force between Monokee and Amazon Web Services, including the Standard Contractual Clauses and the commitments therein regarding governmental requests, and on the MongoDB Data Processing Agreement.

4.2 Monokee also takes into account the EU Data Boundary commitments and the further public commitments made by Microsoft in relation to European customers. Public commitments that are not part of the contract are considered as supporting information only.

4.3 Monokee imposes on all other Sub-Processors obligations consistent with Section B.12 of Part B and with Part A, and gives preference to providers not subject to third-country jurisdiction where an equivalent service is available.

4.4 Towards Customer, Monokee's commitments are set out in Part A and in Section B.12 of Part B.

4.5 **Transfer mechanisms for Personal Data.** Any transfer of Personal Data to, or access by, the US Parent Companies is based on their respective certifications under the EU-US Data Privacy Framework and, as a fallback mechanism, on the Standard Contractual Clauses incorporated in the Microsoft Products and Services Data Protection Addendum, the AWS Data Processing Addendum and the MongoDB Data Processing Agreement, respectively. These are supplemented by the safeguards introduced by US Executive Order 14086, including the redress mechanism before the Data Protection Review Court. The EU-US Data Privacy Framework does not apply to Non-Personal Data, which remain governed by Section B.12 of Part B and by this Annex.

5. Organisational measures – Governmental Access Request Procedure

5.1 Monokee maintains a documented internal procedure for handling requests from public authorities (the "**Procedure**"), under the responsibility of the Data Protection Officer of Monokee, with the support of the CTO for technical matters. Personnel who may receive such requests are trained on the Procedure.

5.2 Upon receipt of a request from a third-country authority, directly or through a Sub-Processor, Monokee shall:

(a) register the request and immediately inform the person responsible for the Procedure;

(b) verify the identity and authority of the requesting body and the legal basis of the request, in particular whether it is based on an international agreement within the meaning of Article 48 GDPR and Article 32(2) of the Data Act;

(c) where no such agreement exists, assess whether the conditions of Article 32(3) of the Data Act and Chapter V of the GDPR are met and, where appropriate, seek the opinion of the competent national bodies or authorities;

(d) inform Customer before complying with the request, unless the request serves law enforcement purposes and for as long as notification would jeopardise the effectiveness of the law enforcement activity;

(e) use all reasonable legal remedies to challenge a request that is unlawful, disproportionate or in conflict with Union or Member State law, including by seeking interim measures;

(f) where disclosure is legally required, disclose only the minimum amount of data permissible based on a reasonable interpretation of the request; and

(g) document each request, the assessment carried out and the outcome.

5.3 Where a request is received by any Sub-Processor, Monokee shall cooperate with the Sub-Processor in challenging the request, inform Customer as soon as Monokee becomes aware of it (subject to Section 5.2(d)) and support Customer in exercising its rights.

5.4 **Transparency.** Monokee shall provide Customer, upon request and at least annually, with aggregated information on the number and type of governmental requests received concerning Customer data, to the extent legally permitted.

6. Residual risk

6.1 Customer acknowledges that, given the jurisdiction to which the US Parent Companies are subject, the measures described in this Annex reduce but cannot entirely exclude the possibility of access by US authorities to Customer data. Monokee considers that, in light of the technical, organisational and contractual measures described above, such residual risk is limited, as documented in the TIA.

6.2 Customer remains free to adopt additional measures under its own control, such as limiting the categories of data entrusted to the Services or applying its own encryption to specific attributes, and Monokee shall reasonably support Customer in doing so.

7. Specific scenarios

7.1 **Invalidation or suspension of the EU-US Data Privacy Framework.** Transfers of Personal Data, if any, shall continue on the basis of the Standard Contractual Clauses and the supplementary measures described in this Annex. Monokee shall update the TIA without undue delay and inform Customer of any material change.

7.2 **Adoption of an EU-US international agreement on access to electronic evidence.** Monokee shall assess its impact on this Annex and on Section B.12 of Part B and inform Customer of any resulting change.

7.3 **Material increase of the risk.** Where, following a change in law, case law or the practices of the Sub-Processor, Monokee considers that the residual risk is no longer acceptable, Monokee shall inform Customer and evaluate additional measures, including the use of alternative hosting providers not subject to third-country jurisdiction, in accordance with the Sub-Processor change procedure of Part A.

8. Business continuity

8.1 Monokee maintains an exit plan from its hosting provider, consistent with Part B, aimed at preserving the continuity of the Services and the portability of Customer data in the event that the use of the current Sub-Processor must be discontinued for legal or regulatory reasons. The Services are deployed on two independent cloud providers (Microsoft Azure as primary site and Amazon Web Services as disaster recovery site), which reduces dependency on a single hosting provider and supports the continuity of the Services in the event of a provider failure or of a required discontinuation of either provider.

9. Review

9.1 Monokee reviews this Annex, the TIA and the information published under Section B.4.2 at least at least annually and in any case upon: (a) a relevant change in Union, Member State or third-country law or case law; (b) a change of Sub-Processor or of the hosting regions; (c) a material change in the contractual commitments of the Sub-Processor; or (d) the receipt of a governmental request concerning Customer data.

ACCEPTANCE AND INCORPORATION This document, comprising Part A (Data Processing Agreement, including Appendix 1 and Appendix 2) and Part B (EU Data Act Addendum, including Annex B-1 to Annex B-4), is incorporated by reference into the Agreement and is accepted by Customer upon acceptance of the Agreement, without the need for a separate signature. Upon request, Monokee shall provide Customer with a countersigned copy of this document.