ANNEX III

DATA PROCESSING SHEET

Special conditions under the General Agreement on Personal Data Processing

Article 28 Reg. EU 2018/679 ('**GDPR**')

Between

The **Data Controller**, as identified in the Agreement, represented by its legal representative vested with the necessary powers,

and

The **Data Processor**, as identified in the Agreement, represented by its legal representative vested with the necessary powers,

Furthermore, the Controller and Processor may be jointly referred to as '**Parties'** and individually as '**Party'**.

WHEREAS

I. The Parties have signed the Main Agreement on Personal Data Processing ("Agreement"), which governs the terms and methods of personal data processing carried out by the Processor in the context of providing the Services covered by the Contract;
II. Pursuant to the aforementioned Agreement, the processing of personal data related to the provision of specific Services is governed through Data Processing Sheets that define the operational characteristics, categories of data processed, purposes, security measures applied, and any involvement of Sub-Processors;
III. This Data Processing Sheet specifies the details of the Service in accordance with the Agreement. It integrates and completes the general provisions of the Agreement, constituting an integral and binding part between the Parties;
IV. In case of conflict between the provisions of this Data Processing Sheet and those of the Agreement, the provisions of the Agreement shall prevail, unless the Data Processing Sheet expressly provides for agreed exceptions between the Parties;
V. For matters not expressly provided for herein, the provisions and definitions set forth in the Agreement and the Contract shall apply, which are hereby fully incorporated by reference.

Having stated all of the above, the Parties present, in the following table, the specifications of the Personal Data processing related to the Service, including information on purposes, categories of data processed, applied security measures, and any other relevant detail for the purposes of the Agreement.

	DESCRIPTION
SERVICE	Archive Services
NATURE OF THE PROCESSING	The Processor may process the Client's Personal Data acquired in the context of providing support and maintenance activities, within the limits strictly necessary for the performance of the services under the Contract, in terms of: collection, recording, organization or structuring, consultation, selection, deletion, or destruction.
PURPOSE OF THE PROCESSING	Conclusion of the Contract and performance of the services covered by the Contract.

METHOD OF DELIVERY	*Cloud* SaaS (*Shared/Private*)
CATEGORIES OF DATA SUBJECTS	• End customers; • Service users; • Suppliers; • Employees.
CATEGORIES OF PERSONAL DATA PROCESSED	The Personal Data processed by the Processor on behalf of the Controller belong to the following categories. **COMMON AND SPECIAL CATEGORIES OF DATA:** • **Personal details** (first name, last name, date of birth, place of birth, country, gender, tax code, residential address, username); • **Contact details** (email, phone number); • **Browsing data** (IP address, log data); • **Financial data** (billing information); • **Data related to the company/organization affiliation**; • **Other data** (including special categories) present in the documents submitted for archiving. Any other personal data (both common and special, as per Articles 4 and 9 of the Regulation) necessary for the execution of the services under the contract: • **For PEC Archiving**: data contained in the Certified Email (PEC) messages entrusted to the Processor.
DATA STORAGE LOCATION	The data are stored on the servers of the Processor and/or Sub-Processors located within the European Union/EEA.
DURATION OF PERSONAL DATA PROCESSING	The processing of Personal Data for the provision of the Services will have the following duration: the entire duration of the Contract with the Controller; the entire duration of the Agreement with the Controller if, for any reason, longer than the duration of the Contract. After the expiration of the aforementioned periods, the Processor is allowed further retention of Personal Data to the extent that it constitutes compliance with specific legal obligations or orders from competent Authorities. The retention of Personal Data is also permitted exclusively to the extent that such Personal Data are necessary for the Processor to demonstrate, assert, or defend its own right, for a maximum period of 10 years.
SECURITY MEASURES	Ref. **Annex III A - Technical and Organizational Security Measures**.
SUB-PROCESSORS	The Processor makes use, for the purpose of carrying out processing activities related to the provision of the Service, of other companies within the Namirial Group and of selected third parties that offer data confidentiality guarantees.

	Some of these third parties may operate outside the European Economic Area (EEA), including the United States. To ensure compliance with the GDPR (Articles 44–49) and data protection regulations, the Provider may use appropriate data transfer mechanisms. These parties are selected in accordance with the provisions set out in the Agreement, receive specific instructions on data processing, and carry out only the activities necessary in compliance with the provided guidelines. The updated list of these entities is provided in **Annex III B** of this document.

ANNEX III - A

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

The security measures described in this Annex apply in addition to those provided in the Agreement and constitute an additional level of protection for the processing regulated by the Processing Sheet to which they are attached. They are applied and applicable to the Service Provider referred to in the Contract.

1. TECHNICAL SECURITY MEASURES

TYPE OF MEASURE	DESCRIPTION
Measures to ensure the confidentiality, integrity, availability, and resilience of processing systems and services on a permanent basis	The process for verifying the integrity of information packages and documents within the service includes: • Verification of document count consistency (i.e., checking the number of actual documents stored in the Preservation System against the number of records in the database structure for a given Document Producer); • Validation check of the integrity tools applied to documents and package indexes (i.e., verification of the digital signature and timestamp on a selected percentage of documents and XML indexes (IPdA) present in the Preservation System for a given Document Producer). Regarding readability checks, the StrongDox Preservation System includes automated mechanisms that, within a five-year timeframe, perform a series of checks on a sample basis, using a pseudorandom algorithm. This sampling considers the full set of IDs among the preserved documents. The sample selected represents a statistically significant portion of all documents preserved for each Document Producer. The following checks are performed on the selected documents: • Integrity check, carried out by automatically recalculating the hash of the document and comparing it with the hash stored at the time of the Archival Package's creation. Following each control operation, a digitally signed Control Report is generated by the Preservation Service Manager and stored within the StrongDox Preservation System. Any additional procedures requested by the Document Producer are described in the relevant Service Sheet.
Measures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	During the Business Continuity Plan restoration phase, all necessary activities are carried out to rebuild the information system and, if needed, activate emergency workstations through the use of a secondary site. To ensure efficient task division and execution, the System Recovery Task Force (GI-RS) is structured by environment, enabling greater specialization and a more precise breakdown into sub-phases. The process is automated within the system and defined internally in the

	Preservation Manual.
Measures to protect data during storage	The compliant document preservation service (LTA) enables any organization to digitally store any type of document (e.g., administrative, accounting, contracts, disclosures, etc.). The service has been designed and implemented in full compliance with the AgID Guidelines on the creation, management, and preservation of digital documents (adopted in May 2021), and with the applicable provisions of the DPCM of December 3, 2013, in effect since April 2014. Below is a brief description of the service components: • Application Front End • Core Service Layer (Web Services) • Database, based on NoSQL for data storage • Data Repository, Object Storage via S3 protocol.
Measures to ensure event logging	The Namirial Production and Software Development departments are responsible for the infrastructure and systems, and they perform online monitoring and application/system-level checks through the indicators and controls defined in the Information Security Management System (ISMS). Namirial uses security event management software and tools to monitor security and operational continuity across essential components of the preservation system. This includes IBM QRadar, operated by Yarix S.p.A. (Montebelluna), which runs a 24/7 Security Operations Center (SOC), monitoring the system year-round. In the event of critical security or continuity incidents, Yarix promptly contacts the designated Namirial personnel to mitigate risks. • Operationally, the Namirial Preservation Office uses ZenDesk to manage service requests from Distributors and End Clients. Each request generates a ticket that is assigned and handled by the team, which provides first-level support. If software development support is needed, the request is redirected to Jira Service Desk, managed by the Cloud Team.
Measures to ensure system configuration, including default configuration	The Preservation Systems are delivered via cloud services through various configurations stored in the database. All configurations are automated and centralized within the AWS System Manager, and are inherited with each system reload.
Internal IT and cybersecurity management and governance measures	The system is certified in compliance with ISO/IEC 27001.
Measures to ensure limited data retention	In the event of a request for the return of all preserved Archival Packages, the Document Producer (User) may request distribution from the StrongDox system, either by using web interface filters or via a dedicated

	WebService method. Each Distribution Package contains a Distribution Package Index (IPdD), generated according to UNI SInCRO 11386:2010, and digitally signed by the Preservation Service Manager. This package serves as an official distribution report, and includes an XSLT file to allow proper rendering of the IPdD.
Measures to ensure accountability	The Organizational Emergency Management Model (MOGE) defines the allocation of responsibilities across various business roles involved in Business Continuity Management processes and activities.
Measures to enable data portability and ensure deletion	The primary data structure ensuring interoperability for Namirial's Preservation Services is the Archival Package, which is generated according to the technical rules for Preservation Systems and complies with the national UNI SInCRO 11386:2020 standard.

ANNEX III - B

SUB-PROCESSORS

This Annex lists the approved Sub-Processors as of the date of signing the relevant Data Processing Sheet, pursuant to the Agreement.

The listed entities have been selected based on criteria of experience, reliability, and compliance guarantees with applicable regulations, particularly the provisions of Article 28 of EU Regulation 2016/679.

They operate under the authority of the Processor, adhering to the instructions received and adopting adequate security measures for the protection of the processed Personal Data.

The list of Sub-Processors may be updated over time in accordance with the provisions of the Agreement.

COMPANY NAME	ADDRESS	PROCESSING LOCATION	ACTIVITY SCOPE
AWS EMEA SARL	Luxembourg, 38 Avenue John F. Kennedy L-1855	EEA	Cloud Services
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	EEA	Support ticket management
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEA	Support ticket management
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Synchronizing support tickets
Yarix S.r.l.	Montebelluna (TV), Vicolo Boccacavalla n. 12, 31044	EEA	SOC (Security Operation Center) and MOC (Monitoring Operation Center)
MongoDB Limited	Building Two, Number One Ballsbridge, Dublin 4, Ireland	EEA	Cloud Services
Dynatrace S.r.l.	Viale Enrico Forlanini, 23 20134 Milan, Italy	EEA	Log monitoring