ANNEX III

DATA PROCESSING SHEET

Special conditions under the General Agreement on Personal Data Processing

Article 28 Reg. EU 2016/679 ('**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	Service "AI Classification" integrated into Namirial Archive/LTA. The "AI Classification" Service enables automatic document classification and extraction of the related metadata by means of artificial intelligence models, for the purpose of digital archiving and preservation (LTA) within the Namirial Archive system. The processing comprises two operational flows: Manual Flow: in which the Client verifies and approves the outputs before archiving; Automated Flow: in which outputs with a confidence score above the configured threshold are archived automatically, while those below are subject to human review.
PROVIDING ENTITY	**Namirial S.p.A.**

	Where the Providing Entity does not coincide with the Supplier identified in the Commercial Proposal, it acts as Intra-Group Sub-Processor on behalf of the Supplier, operating under pre-existing intra-group agreements between the companies of the Namirial Group, compliant with Article 28 GDPR.
NATURE OF THE PROCESSING	The Processor may process the Client's Personal Data in the context of providing the service, within the limits strictly necessary for the performance of the services under the Contract, in terms of: collection, recording, organization or structuring, consultation, processing, selection, extraction, comparison, use, communication, deletion, or destruction, as well as automated analysis and classification of documents by means of AI models based on machine learning and configured rules, with generation of structured metadata and JSON output files.
PURPOSE OF THE PROCESSING	Performance of the Contract for the provision of the "AI Classification" Service, including: automatic document classification and assignment of document categories; extraction, normalization and automatic population of metadata; routing of documents to Namirial Archive/LTA according to mapping and preservation rules; improvement of traceability and efficiency of document processes.
METHOD OF DELIVERY	*Cloud SaaS (Shared/Private) - AI pipeline on AWS infrastructure with model management via AWS Bedrock (European node) and Namirial components for classification, integration and review.*
CATEGORIES OF DATA SUBJECTS	• End customers; • Service users; • Employees/Collaborators of the Controller in charge of validating the outputs; • Individuals whose personal data may be contained in the documents to be classified.
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 DATA:** • Personal data (name, surname, date of birth, place of birth, nationality, gender, tax code, residence/domicile address, username); • Contact data (email, phone number); • Browsing data (IP address, log data); • Financial data: billing data; • Data relating to the company/organization of affiliation; • Additional data (including special categories pursuant to Art. 9 GDPR) contained in the documents to be classified; • Technical metadata extracted automatically (e.g. document date, type, customer code, amount, VAT number); • Technical logs and confidence scores generated by the system; • Structured outputs (labels, metadata JSON).

	The Service does not apply automatic anonymization of personal data but operates on complete documents. It is the Controller's responsibility to verify the lawfulness and minimization of the uploaded data**.**
DATA STORAGE LOCATION	The data are processed and stored on the servers of the Processor and/or Sub-Processors located within the European Union, in particular on AWS infrastructure (EU-West-1 Frankfurt). No extra-EU transfers are envisaged unless specifically configured by the Controller.
DURATION OF PERSONAL DATA PROCESSING	The data are retained for the time necessary for processing and integration with Namirial Archive/LTA. Technical logs are kept for audit and traceability purposes for a maximum period of 12 months, or in any case until termination of the Service, unless otherwise required by law. Classification outputs, in .json format, are forwarded, together with the classified document, to the Namirial Archive/LTA system and are not retained by the Processor.
SECURITY MEASURES	Ref. **Annex III A - TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**
SUB-PROCESSORS	The Providing Entity of the Service (identified in the row above) uses, for the provision of the Service, other Namirial Group companies and selected third parties that offer data confidentiality guarantees. The updated list is provided in Annex III B, divided into **Table A** (Namirial Group companies involved in service delivery, operating under pre-existing intra-group agreements compliant with Article 28 GDPR and separate from this Agreement) and **Table B** (Third-Party Sub-Processors). Some of these third parties may also operate outside the European Economic Area (EEA), including the United States. To ensure compliance with the GDPR (Articles 44-49) and personal data protection regulations, the Supplier may use appropriate mechanisms for data transfer. These entities are selected in accordance with the provisions of the Agreement, receive precise instructions on data processing, and perform only the necessary activities in compliance with the provided directives. 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 Providing Entity of the Service referred to in the Contract, which may or may not coincide with the Processor.

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 "AI Classification" infrastructure runs on AWS cloud, compliant with ISO/IEC 27001, 27017, 27018 and 42001 certifications. • Data and metadata are encrypted in transit (TLS 1.2/1.3) and at rest (AES-256). The integrity of outputs (JSON files, labels, technical logs) is verified through hashes and automatic consistency checks between original documents and extracted metadata. • Each classification session is logged with unique identifiers and model versions. Resilience mechanisms include multi-zone replication, automatic failover and 24/7 monitoring via SOC.
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	The "AI Classification" Service inherits the Business Continuity and Disaster Recovery plans of the Namirial Archive system. • For all matters relating to RTO/RPO and restoration, reference is made to the rules established for Namirial Archive.
Measures to protect data during storage	Documents uploaded for classification are processed in segregated environments (dedicated tenant per customer). AI models operate on images or files (PDF, XML, P7M, ZIP) processed via the AWS Bedrock pipeline, which does not store persistent inputs. Outputs are sent in structured form to Namirial Archive/LTA through encrypted and authenticated channels. All phases generate technical logs stored for audit purposes.
Measures to ensure event logging	Each classification operation generates application logs containing document identifiers, timestamp, model version, outcome (ok/review/ko), confidence score and requesting user. Logs are stored in segregated environments and in the SIEM system, which monitors security and performance anomalies 24/7. Access to and changes of configuration parameters are tracked.
Measures to ensure system configuration, including default configuration	Classification configurations (taxonomies, operational thresholds, mapping to Archive) are stored in encrypted and versioned databases. The "privacy by default" principle requires that the minimum confidence threshold trigger human validation and that only strictly necessary data be extracted. Every update of configurations or models is subject to technical and logical validation.

Internal IT and cybersecurity management and governance measures	The AI Classification service is managed within Namirial's Information Security Management System, certified ISO/IEC 27001. Internal policies are applied for access management, version control, change management and sub-processor assessment. AI governance also follows the principles of the ISO/IEC 42001:2023 management system, with recording of AI model development and maintenance activities.
Measures to ensure limited data retention	Documents and metadata are retained only for the time necessary for processing and transfer to Namirial Archive/LTA. Upon termination of the service or at the Client's request, data are deleted or anonymized through documented automatic procedures.
Measures to ensure accountability	Each classification cycle is tracked with identifier, model and confidence score. Outputs below the threshold are mandatorily subject to human validation by authorized operators of the Client. Namirial maintains the technical documentation of the system and the records of the versions of the AI models used, in compliance with the AI Act and its own internal Compliance & Privacy guidelines on the use of AI.
Measures to enable data portability and ensure deletion	Client data are deleted or returned within the contractual terms at the end of the service, through secure wipe procedures on S3 storage. All deletion operations are tracked and certified in the system's technical register.

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.

TABLE A

NAMIRIAL GROUP COMPANIES INVOLVED IN SERVICE DELIVERY

COMPANY NAME	ADDRESS	PROCESSING LOCATION	ACTIVITY SCOPE
Namirial SPA	Via Caduti sul Lavoro 4 – Senigallia (AN) Italy	EEA	Service provider

TABLE B

THIRD-PARTY SUB-PROCESSORS

COMPANY NAME	ADDRESS	PROCESSING LOCATION	ACTIVITY SCOPE
AWS EMEA SARL	Luxembourg, 38 Avenue John F. Kennedy L-1855	EU-West-1 Frankfurt	AI processing & infrastructure (Bedrock).
MongoDB Limited	Building Two, Number One Ballsbridge, Dublin 4, Ireland	EEA	Metadata management and temporary repositories