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	**"AI SpinOff" Module for automatic data extraction functionality** The "AI SpinOff" Module is an optional component of Namirial's on-premise SpinOff management software, dedicated to the automatic extraction of data contained in documents or images. The module uses artificial intelligence models to identify and structure the information contained in the documents, returning a validated JSON output. The processing is structured in the following operational flow: Acquisition: the document remains within the Controller's infrastructure. The Module performs locally the technical processing necessary to prepare the content to be transmitted to

	the AI Provider, according to the methods supported by the Module from time to time; AI processing: the content of the document, or a technical representation thereof generated by the Module, is transmitted through an encrypted channel to the AI Provider, which returns structured data in JSON format. The transmitted data are not used by the AI Provider to train its own models, according to the applicable contractual conditions; Human validation: the Module makes available to the Controller's operator functionality for verifying, checking and possibly approving or modifying the output before recording it in the SpinOff management software, according to the applicable configurations; Recording: the validated data are recorded in the Controller's local SpinOff database.
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 of document contents by means of artificial intelligence (AI) models. The processing takes place exclusively on the initiative and under the control of the Controller, who remains responsible for the accuracy and completeness of the data entered into the management software.
PURPOSE OF THE PROCESSING	Performance of the Contract for the provision of the "AI integrated in SpinOff" Module, including: • calculation and communication to the operator of the Confidence Score for each extraction, in order to support human validation; • pre-filling of the SpinOff management software fields to reduce manual entry and typing errors; • improvement of process efficiency.
METHOD OF DELIVERY	*On-premise. The Module is installed directly on the Controller's infrastructure (local servers or corporate network). Documents are processed locally by the Module and the content necessary for AI processing, or a technical representation thereof, is transmitted in transient and encrypted form to the AI Provider for inference. No persistent storage of personal data is envisaged at the AI Provider.*

DATA PROCESSING SHEET

CATEGORIES OF DATA SUBJECTS	• Employees/collaborators of the Controller; • Operators of the Controller in charge of validating the AI outputs and recording them in the SpinOff management software; • Third parties whose identification data may be present in the documents (e.g. clients, final recipients of the goods).
CATEGORIES OF PERSONAL DATA PROCESSED	The Personal Data processed on behalf of the Controller are those contained in the documents submitted to the AI Module and belong to the following categories. **COMMON DATA:** • The data contained in the documents submitted to the AI Module may include, by way of example and not exhaustively: identification data, contact data, tax data, commercial data, logistics data, administrative data; • Technical processing data: extraction Confidence Score, processing timestamp, API tokens consumed, response times. **SPECIAL DATA (Art. 9 GDPR):** • No systematic processing of special categories of data is envisaged. However, it cannot be excluded that, in specific cases, document contents may include information attributable to special categories (e.g. health data in medical supplies). The Controller is responsible for assessing and limiting the provision of such data to the AI Module.
DATA STORAGE LOCATION	Controller's premises (on-premise): the original documents, technical logs and data recorded in the SpinOff management software are stored exclusively on the servers of the data Controller. Namirial has no remote access to the stored data, except for technical support interventions expressly authorized by the Controller. AI Provider (for transient processing): the information extracted from the document is transmitted to the AI Provider's API exclusively for real-time AI inference. The AI Provider does not store the sent data persistently. The transfer to the USA, if necessary, is carried out pursuant to Art. 46 GDPR, by means of Standard Contractual Clauses (SCC) adopted by the European Commission with implementing decision 2021/914 of 4 June 2021. It is understood that Namirial may process technical and consumption metrics relating to the use of the Module, such as number of processings, pages processed, timestamps, technical outcomes, tokens or other consumption indicators, for the purposes of monitoring, reporting and billing of the service, without access to the content of the processed documents, except for technical support interventions expressly authorized by the Controller.
DURATION OF PERSONAL DATA PROCESSING	The personal data contained in the uploaded documents are processed exclusively for the time necessary for inference (real-time processing, without persistent storage). The JSON extraction results are available to the Controller's operator for the duration of the working session. Local technical logs are retained on the Controller's server for a maximum period of 12 months, unless otherwise indicated by the Controller or specific legal obligations.

	The data recorded in the SpinOff management software following human validation are subject to the Controller's own retention policies, defined in relation to applicable tax and accounting obligations (typically 10 years for tax documents).
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 Module operates on the Controller's on-premise infrastructure, with access limited to authorized operators through application authentication managed by SpinOff. • Communications between the AI Module and the AI Provider's API are protected by TLS and encrypted channels. The contents or technical representations transmitted to the AI Provider are processed transiently for the time necessary for processing and do not persist locally after sending. • Namirial maintains ISO/IEC 27001 compliance for its software development and distribution processes. The Enterprise contract with the AI Provider includes certified security commitments (ISO 27001, SOC 2 Type II).
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 operational continuity of the AI Module depends on the Controller's on-premise infrastructure (local servers, corporate backups) and on the availability of the AI Provider service. • The Module is designed to be resilient to transient API errors (automatic retries with exponential backoff). In case of unavailability of the AI Provider's API, the manual entry flow in the SpinOff management software remains fully operational without dependence on the AI Module. • Business Continuity of the on-premise infrastructure is the responsibility of the data Controller, in accordance with its own internal policies.
Measures to protect data during storage	The AI Module processes documents locally on the Controller's infrastructure and, where technically necessary for AI processing, generates a technical representation of the relevant content. Solely for inference purposes, such content or technical representation may be transmitted to the AI Provider through an encrypted channel, for the time strictly necessary for processing. **The AI Provider ensures that data sent via API are not used to train or improve the AI Provider's models. The data sent are not shared with third parties and are not subject to persistent storage at the AI Provider.** • Each API call is authenticated through dedicated technical credentials, configured in the Namirial environment and associated with the client or the service according to applicable configurations. The credentials are not exposed in the user interface or in application logs.

Measures to ensure event logging	**Each document extraction operation generates local application logs containing:** • unique identifier of the request and of the processed document; • start/end processing timestamp; • calculated Confidence Score and per-field detail; • number of API tokens consumed and estimated cost (USD); Logs are stored locally on the Controller's server and accessible via dedicated API endpoints (/api/v1/metrics, /api/v1/metrics/dashboard). Retention is limited to 12 months unless otherwise configured by the Controller.
Measures to ensure system configuration, including default configuration	The Module's configurations are set so as to make available to the operator a functionality for verifying the AI output and an indication of its level of reliability or completeness, according to the thresholds and parameters configured from time to time. The "privacy by design and by default" principle (Art. 25 GDPR) is implemented through: • local processing of documents on the Controller's infrastructure, except for the transmission to the AI Provider of the content or technical representation strictly necessary for processing; • transmission of data to the AI Provider through encrypted channels and for the time strictly necessary for AI inference; • configuration of the Module so as to allow the operator to verify, modify, approve or reject the AI output before its operational use, according to the available functionality; • minimization of the output returned by the Module to the data and fields relevant to the specific functionality used; • provision of informational notices in the user interface regarding the automated and probabilistic nature of the AI output and the need to verify its accuracy before operational use, where provided by the Module configuration. • disclaimer shown to the operator in the user interface regarding the probabilistic nature of the AI output.
Internal IT and cybersecurity management and governance measures	The AI Module is developed and distributed within Namirial's Information Security Management System, certified ISO/IEC 27001. Internal policies are applied for access management, software version control (release management), change management and periodic assessment of sub-processors. AI governance is progressively aligned with the principles of ISO/IEC 42001:2023, also through documentation of the development, testing and maintenance activities of the AI Module and tracking of the versions of the models used. The Controller is responsible for the IT governance of its own on-premise infrastructure (physical and logical access to servers, operating system updates, backups).
Measures to ensure limited data retention	The contents or technical representations generated for AI processing are processed for the time strictly necessary for processing and are not retained by the Processor in persistent form, except as necessary for technical logs, service metrics or authorized support activities. The JSON outputs of the processing are kept in application memory only for the time necessary for human validation and recording in the

	management software. They are not retained by the Processor in a form that allows identification of the data subjects. Technical logs are retained for a maximum of 12 months and subsequently deleted automatically or upon request of the Controller.
Measures to ensure accountability	Each document extraction cycle is tracked with a unique identifier, the version of the AI model used and the Confidence Score. The Module makes available functionality that allows the Controller's operator to verify, validate, modify or reject the AI output before its operational use, according to applicable configurations (compliance with Art. 22 GDPR - prohibition of automated decisions with significant legal effects). Namirial maintains the technical documentation of the Module, the version register and the records of the AI models used, in compliance with the requirements of the AI Act (Reg. EU 2024/1689) and its own internal policies.
Measures to enable data portability and ensure deletion	The data processed by the AI Module are recorded in the Controller's SpinOff management software and are therefore subject to the Controller's own portability and deletion policies. The Processor does not retain copies of the personal data processed in performance of the Service and is therefore not the entity to be contacted for data subjects' requests for access, rectification, portability or erasure. Upon termination of the Contract, the Controller may request the uninstallation of the Module and the deletion of any data possibly stored on the Processor's system (e.g. API keys, tenant configurations). The deletion will be documented and certified.

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
OpenAI LLC	3180 18th Street San Francisco, CA 94110 USA	USA (extra-EU) Transfer under Art. 46 GDPR SCC EC Dec. 2021/914	AI inference for structured data extraction from documents. Transient processing: no persistent storage of personal data.
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEA	Support ticket management
Atlassian B.V.	Amsterdam, Singel 236 1016 AB, Netherlands	EEA	Support ticket management
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Support ticket synchronization