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	*PreventGO*
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.
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.
CATEGORIES OF PERSONAL DATA PROCESSED	The Personal Data processed by the Processor on behalf of the Controller belong to the following categories. **COMMON DATA:** • **Personal data** (name, surname, email, date of birth, place of birth, nationality, gender, tax code, residence/domicile address); • **Contact data** (email, phone number); • **Browsing data** (IP address); • **Details and copy of the identity document and of the health card/tax code;** • **Images.**
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 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	A stable operation and protection of the IT system from external or internal attacks is ensured through the implementation of pseudonymization and encryption of the processed data, the use of firewalls and antivirus programs, event logging and high availability of the data centers, among other measures. • In addition, measures are adopted for the external security of the data processing systems, including an alarm system for building protection, locks on windows and doors, access systems with fingerprint and badge.
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 possibility of restoring access to data in the event of any incidents is ensured through the implementation of an adequate backup process, thus guaranteeing the availability of information. Daily and weekly backups are provided, as well as off-site backups.
Measures to protect data during storage	Encryption (AES-256, TLS, hash functions) is used to ensure the confidentiality and integrity of data and, where appropriate, pseudonymization.
Measures to ensure event logging	Logs are collected, centralized and reviewed monthly via the ELK stack, including system logs, application logs and traffic logs, in order to ensure traceability.
Measures to ensure system configuration, including default configuration	A hardening procedure is adopted for system configuration, accompanied by continuous monitoring.
Measures to ensure limited data retention	Data protection policy (retention and archiving policy). • Once the retention period of a given data set has expired, the data are transferred as historical data to a secondary archive, as needed.

Measures to ensure accountability	The Processor's employees are continuously informed and trained on data protection and are contractually bound to data secrecy and confidentiality. Third parties who may come into contact with personal data during their work for the Processor are required to maintain secrecy and confidentiality to comply with data protection and data secrecy under an NDA (Non-Disclosure Agreement) before starting work. All Namirial affiliated companies within the EU have concluded a common framework agreement on data protection and commissioned data processing as a legal instrument under Article 28 GDPR in order to ensure a uniform standard of data protection and security across the group and to regulate the rights and obligations for any commissioned data processing.
Measures to enable data portability and ensure deletion	Processes have been implemented to ensure an adequate response to data portability requests from customers. Data are transmitted in structured, commonly used and machine-readable formats. Secure methods are used for data transmission (encryption).

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
Namirial SAS	Les Centuries I - 93 place Pierre Duhem 34000 Montpellier	EEA/USA	IT

TABLE B

THIRD-PARTY SUB-PROCESSORS

COMPANY NAME	ADDRESS	PROCESSING LOCATION	ACTIVITY SCOPE
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEA	Support ticket management
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	EEA	Support ticket management
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Support ticket synchronization
Var Group S.p.A. (Yarix)	Via della Piovola, 138 - 50053 Empoli FI	EEA	SOC (Security Operation Center) e MOC (Monitoring Operation Center)