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	*Building In Cloud* (BIC)
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
CATEGORIES OF DATA SUBJECTS	• End customers; • Service users; • Employees.
CATEGORIES OF PERSONAL DATA PROCESSED	The Personal Data processed by the Processor on behalf of the Controller belongs to the following categories: **COMMON DATA:** • **Personal data** (name, surname, date of birth, place of birth, nationality, gender, tax code, residence/domicile address); • **Contact data** (email, phone number); • **Browsing data** (IP address).
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 uses other companies within the Namirial Group and selected third parties that offer data confidentiality guarantees to carry out processing operations related to the provision of the Service. 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 reported 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	Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or during transport or storage on data media, and that it is possible to verify and establish to which entities the personal data are transmitted. Specifically, the following technical and organizational measures are implemented: • advanced encryption of data both in transit (TLS 1.3, VPN) and at rest (AES-256); • physical protection of data centers with biometric access and alarm systems; • proactive detection of cyber threats with SIEM tools for continuous monitoring; • load balancing and infrastructure redundancy to ensure service continuity in case of failures; • resilience tests and simulated attacks (Penetration Testing) to verify system robustness.
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	Measures capable of quickly restoring the availability and access to personal data in the event of a physical or technical incident. Specifically, the following technical and organizational measures are implemented: • monitoring and reporting of backups; • restoration through automation tools; • backup concept and recovery process based on specific criticalities and customer requirements; • control of the backup process; • regular testing of the data recovery process and recording of results; • storage of backup media in a secure location outside the server room.
Measures to protect data during storage	Measures to ensure the protection of personal data against accidental destruction or loss (UPS, air conditioning, fire protection, data backup, secure storage of data media, antivirus protection, RAID systems, disk mirroring, etc.). **TECHNICAL MEASURES:**

	• Data at Rest Encryption to ensure the protection of stored data; • centralized management of permissions to critical file systems; • fire detection systems; • fire extinguisher in the server room; • monitoring of temperature and humidity in the server room; • control of server room ventilation; • UPS system and emergency diesel generators; • RAID system / hard disk mirroring; • server room video surveillance; • alarm message in case of unauthorized access to the server room; • secure destruction of storage media at the end of their life cycle (degaussing, certified shredding). **ORGANIZATIONAL MEASURES:** • backup service; • absence of pipes in the server room; • storage of backup media in a secure location outside the server room; • separate partitions for operating systems and data, where necessary; • monitoring access to stored data, with alerts on anomalous operations.
Measures to ensure event logging	**Organizational measures provided by the Data Processor**: • protected and immutable audit logs, with access limited to System administrators; • real-time monitoring of critical activities, with automatic alarms for anomalies; • periodic analysis of system logs and correlation of suspicious events; documented process for detecting and reporting security incidents / data breaches (see, SCS-P04 Group Incident Management & Reporting Policy); • formalized procedure for managing security incidents (see, SCS-P04 Group Incident Management & Reporting Policy); • involvement of the DPO and CISO in security incidents and data breaches; • documentation of security incidents and data breaches through the ticket system (via "Jira" tool); • formal process for following security incidents and data breaches.
Measures to ensure system configuration, including default configuration	The Data Processor implements the following measures to ensure system integrity:

	• use of regularly updated firewall; • use of regularly updated spam filter; • use of regularly updated virus scanner; • intrusion detection system (IDS) for the Data Controller's systems; • intrusion prevention system (IPS) for the Data Controller's systems.
Internal IT and cybersecurity management and governance measures	The system complies with ISO/IEC 27001 certification.
Measures to ensure limited data retention	OWASP Secure Mobile Development security controls are carried out (see, SCS-P08 Group Secure Coding Policy); perimeter analysis of web applications.
Measures to ensure accountability	Data Processor employees are continuously informed and trained in 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 Data Processor are required to maintain data secrecy and confidentiality in order to comply with data protection and data secrecy under the NDA (Non-Disclosure Agreement) before starting work. All affiliated companies of the Data Processor within the EU have concluded a common framework agreement on data protection and commissioned data processing as a legal instrument under Article 28 GDPR to ensure a uniform standard of data protection and security across the group and to regulate rights and obligations for any commissioned data processing.
Measures to enable data portability and ensure deletion	The Data Processor provides measures to ensure that persons authorized to use a data processing system can only access data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage.

2. ORGANIZATIONAL SECURITY MEASURE

TYPE OF MEASURE	DESCRIPTION
Procedures for regularly testing, verifying, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing	Internal policies related to security measures are periodically reviewed and confirmed for adequacy and effectiveness during ongoing internal audits and annually by independent, external, and accredited certification bodies as part of ISO 9001 and ISO 27001 monitoring and recertification audits.

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	*Data storage*
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	Synchronization of support tickets
Yarix S.r.l.	Montebelluna (TV), Vicolo Boccacavalla n. 12, 31044	EEA	SOC (*Security Operation Center*) and MOC (*Monitoring Operation Center*)