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	*PECMailer*
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); • **Access data** (username and password); • **Navigation data** (IP address, log data); • **Financial data** (billing data); • **Additional data** (including special categories) present in the Certified Electronic Mail 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 Processor 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	**a. Confidentiality:** • Access to PECMailer is allowed only through TLS protocols version 1.2 or higher. • Encryption of access credentials for accounts and operators. • Multi-database management to ensure logical/functional separation of email accounts. **b. Integrity:** • Integrity of certified email (PEC) messages is ensured by the digital signature applied by the service provider. • Data integrity control during transfer is guaranteed through TLS encryption. **c. Availability:** • Three-tier infrastructure with availability zones located within the European Community. • Use of Azure Storage Premium with automatic snapshots every 24 hours and 14-day retention. • Differential backups every 12 hours with weekly retention of 4 weeks. • Point-in-time recovery every 10 minutes with 7-day retention for databases. **d. Resilience:** • Redundant and load-balanced virtual machines (VMs) configured to ensure service continuity.
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	• Automatic snapshots every 24 hours for storage, with 14-day retention. • Point-in-time recovery every 10 minutes for critical databases. • Infrastructure distributed across multiple availability zones within the European Community.
Measures to protect data during storage	• Data stored in Azure Storage Premium with local redundancy. • Encryption of access credentials and data at rest. • Integration with federated authentication systems to ensure secure access.
Measures to ensure event logging	• Detailed logs of backend service activities (ServicesActivity) and user operations (_SysEventsLog);

	• Full traceability of operator activities: access, sending, reading, and deletion of messages; • Logs stored in client-dedicated databases, with options for consultation and historical analysis.
Measures to ensure system configuration, including default configuration	Periodic security updates applied to VMs and services.
Internal IT and cybersecurity management and governance measures	CrowdStrike EDR installed on all machines.
Measures to ensure limited data retention	Retention policies on the PEC account (excluding PECMailer): configurable for PEC messages (1 day, 3 days, 15 days).
Measures to ensure accountability	• Comprehensive tracking of administrative and user activities via logs. • Internal auditing policies to verify compliance with GDPR regulations.
Measures to enable data portability and ensure deletion	• Data export through PECMailer SDK for external integrations.

2. ORGANIZATIONAL SECURITY MEASURE

TYPE OF MEASURE	DESCRIPTION
Procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing	Penetration tests are carried out semi-annually, and weekly vulnerability assessments are performed by the cybersecurity team, with vulnerabilities categorized as Critical, High, Medium, or Low, and remediation SLAs defined based on the level of severity.
Certification/assurance measures for processes and products – Security Testing and Verification	**Security Testing and Verification** • Quarterly vulnerability assessments and penetration tests. • Continuous monitoring of vulnerabilities and patch management processes with defined SLAs. • Regular audits of the security configurations of both cloud and on-premises infrastructures.

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
Microsoft Ireland Operations Ltd	South County Business Park, Dublin D18, Ireland	EEA	*Data Storage*
Datlas S.p.A.	San Martino In Rio (RE) Viale Della Resistenza 47	EEA	Support for assistance activities
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*)