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	Platforms/*AMC platforms:* • FatturePlus; • WOW Platform; • SpinOff. (hereinafter, the "AMC Services") Platforms/TAX platforms:

	• SGAPro; • Web Successions; • Live CAF; • Tax online; • CAF Manager; • CAF Center. (hereinafter the "**Tax Services**") Collctively "**Tax/AMC Services**".
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 under 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 fall into the following categories. **COMMON DATA** (for all Tax Servoces): - **Personal details** (first name, last name, date of birth, place of birth, country, gender, tax code, residence/domicile address); - **Contact details** (e-mail, telephone number); - **Browsing data** (IP address, log data); - **Billing data** (IBAN, payment details); - **Any additional data** (for SGA Pro service): - copy of the users' identity document; - information relating to the professional activity carried out; - any registrations with social security funds; - any disciplinary proceedings concerning the users. - **Any additional data** (for the WOW Platform and Tax Services): - data contained in income tax returns. - **Altri eventuali dati** (per SpinOff): - data contained in documents uploaded within the management system. **SPECIAL CATEGORIES OF DATA (for SGA Pro):**

	- data relating to any exemption situations due to maternity, injury, or other circumstances proven by documentation.
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 purpose of providing the Services shall have the following duration: the entire duration of the Agreement with the Controller; the entire duration of the Arrangement with the Controller if, for any reason, it is longer than the duration of the Agreement. After the expiry of the above periods, the Processor is permitted to retain the Personal Data further insofar as such retention is required to comply with specific legal obligations or orders issued by competent Authorities. The retention of Personal Data is also permitted solely to the extent that such Personal Data are necessary for the Processor to establish, exercise, or defend a legal claim, for a maximum period of 10 years. For the SGA Pro service, the Processor guarantees the storage of data for 1 (one) year starting from the termination of the Agreement.
SECURITY MEASURES	**Ref. Annex III A** – TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES FOR THE SGA PRO SERVICE **Ref. Annex II** – TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES under the Agreement for all Tax Services.
SUB-PROCESSORS	The Processor makes use, for the purpose of carrying out the processing operations related to the provision of the Service, of other companies within the Namirial Group and of selected third parties that offer adequate data confidentiality safeguards. 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 Provider may rely on appropriate mechanisms for data transfers. These entities are selected in accordance with the provisions of the Agreement, receive specific instructions on data processing, and perform only the activities necessary in compliance with the directives provided. The updated list of these entities is included 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 to ensure that it is possible to verify and determine to which entities personal data are transmitted. In particular, the Processor implements the following technical and organizational measures: • protected access with username and password, with a mandatory password update every 90 days. The password must contain uppercase and lowercase letters, 8 characters, 1 number, and 1 special character; • periodic penetration tests (at least once a year); • periodic vulnerability assessments; • technical data quality controls: functions integrated into the code designed to verify the quality of the information and how the data is structured; • availability of clear-text logs for the last 30 days and availability of all password changes performed by the service's users; • all SGAPRO sites hosted on web servers are protected by a WAF (Web Application Firewall) and a Load Balancer that exposes the public IP to make the sites reachable; • possibility of connecting via SFTP (with private password) to a support server that maps a shared drive containing the PHP code of the SGAPRO sites; • possibility of accessing the RDS instance hosting the databases of the various services; • each of the above access methods is only possible after establishing a VPN connection to the Namirial network.
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	To ensure operational continuity and the timely restoration of the availability of and access to personal data in the event of a physical or technical incident, Namirial has implemented the following technical and organizational measures: • **Regular backups:** data backups are performed every 12 hours, ensuring preservation and rapid recovery capability. • **Hourly backups of application systems:** ○ an hourly backup is performed of the web server image and the file system, including the PHP code, with a retention period of 15 days;

	○ the database undergoes a full backup of the entire RDS instance every 24 hours, also with a 15-day retention period. • **Infrastructure redundancy:** ○ development servers use the same code as the production platform, ensuring consistency across environments and facilitating emergency interventions; ○ the production server is mirrored across four machines, ensuring high service availability; ○ a copy of the code is also maintained in a dedicated testing environment. • **Management of support and assistance requests:** ○ the Processor's staff uses the ZenDesk platform to manage user support requests; ○ each request generates a ticket assigned and handled by the first-level support team; ○ if advanced technical intervention is required, the request is routed to the cloud team via Jira Service Desk, ensuring a structured workflow for the handling and resolution of incidents.
Measures to protect data during storage	The data are protected by firewalls (WAF) and load balancers, and are accessible only through a secure VPN connection to the Namirial network. Additionally, the data are encrypted during transmission and storage, and periodic penetration tests and vulnerability assessments are carried out to ensure security.
Measures to ensure event logging	All access to and modifications of the systems are recorded in detailed logs, which are retained for at least 30 days and are easily accessible. Access and modification operations are traceable thanks to secure credential management (with passwords and VPN-based authentication). Every change made by users is recorded and monitored to ensure the integrity and confidentiality of the data. Furthermore, in the event of an incident, logs and backups enable a quick and secure restoration of operations.
Measures to ensure system configuration, including default configuration	The systems are delivered in the cloud through various configurations stored in databases. All configurations are automated and centralized within the system manager (AWS), and the configurations are inherited with each system reload.
Internal IT and cybersecurity management and governance measures	The system is compliant with the ISO/IEC 27001 certification.
Measures to ensure limited data retention	WASP Secure Mobile Development security checks are performed (see SCS-P08 Group Secure Coding Policy). Analysis of the perimeter of web applications is carried out. Requests for the deletion or return of information - whether personal

	data or other types of data - are handled in accordance with the instructions provided by the Customer, in compliance with Article 28 of the GDPR and the provisions of the Agreement.
Measures to ensure accountability	The Emergency Management Organizational Model (MOGE) defines the allocation of responsibilities among the various corporate roles for processes and activities related to business continuity management. All Namirial-affiliated companies within the EU have entered into a common framework agreement on data protection and commissioned data processing as a legal instrument pursuant to Article 28 of the GDPR, in order to ensure a uniform standard of data protection and security throughout the group and to regulate the rights and obligations for any commissioned data processing.
Measures to enable data portability and ensure deletion	Namirial implements measures to ensure that individuals authorized to use a data processing system can access only the data for which they have been granted authorization, and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage.

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.

SERVICE	COMPANY NAME	ADDRESS	PROCESSING LOCATION	ACTIVITY SCOPE
- SGA Pro - SpinOff	**AWS EMEA SARL**	Luxembourg, 38 Avenue John F. Kennedy L-1855	EEA	*Cloud services*
- AMC Services	**Microsoft Ireland Operations Ltd**	South County Business Park, Dublin D18, Ireland	EEA	*Cloud services*
- Tax/AMC Services	**Atlassian B.V.**	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	EEA	*Ticketing platform (back-end)*
- Tax/AMC Services	**Zendesk Inc.**	989 Market St, San Francisco, CA 94103	EEA	*Ticketing platform (front-end)*
- Tax/AMC Services	**Exalate NV**	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Ticketing synchronization
- Tax/AMC Services	**Yarix S.r.l.**	Montebelluna (TV), Vicolo Boccacavalla n. 12, 31044, Italy	EEA	SOC (*Security Operation Center*) e MOC (*Monitoring Operation Center*)
- Tax/AMC Services	**Televideocom S.r.l.**	Z.I. Predda Niedda Nord Strada n. 5 – 07100 Sassari, Italy	EEA	*Cloud services*
- Tax/AMC Services	**Wiit S.p.A.**	Via Mercanti 12, Milan, Italy	EEA	*Backup services*