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	Certified Electronic Delivery Service (SERC) and Qualified Certified Electronic Delivery Service (SERCQ)
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); • **Other possible data**: data present in certified communications. **SPECIAL CATEGORIES OF PERSONAL DATA:** • **Other possible data**: special data present in certified communications.
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 of the Namirial Group and selected third parties that offer data confidentiality guarantees to carry out the processing operations related to the provision of the Service. 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 Service Provider Uanataca SAU as indicated in the Sub-Processor Annex.

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 process of verifying the integrity of information packages and documents within the service includes: • Periodic internal audits to check and verify that the state of the Information Security Management System is adequate and compliant with the law; • Employees are trained to understand communication flows, and without prior authentication, they will not have access to the processed data; • Communication flows are protected through the use of virtual private networks (VPNs). In this way, the connections established with the VPNs will protect the exchanged information, as the information will be encrypted between the two ends of the tunnel; • For each offered service, procedures are drafted to determine the extent and frequency of encrypted backups (AES256) of the processed data, specifying the retention duration. In these cases, the number of necessary copies and the retention duration will be established.

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	In the event of a data breach, Uanataca has a process for managing IT incidents that operates as follows:
	• A responsible team, based on a thorough analysis of previous IT incidents, will develop an action plan consisting of preventive measures to limit the recurrence of such episodes;
	• Upon detecting a physical or technical incident, it will be classified and divided into appropriate categories necessary to determine the severity and priority of the treatment to be implemented;
	• Subsequently, through the incident notification process, the immediate actions to be taken to ensure the ability to promptly restore the availability and access to the affected personal data will be highlighted;
	• Uanataca also provides for the drafting of an IT incident register, in which it is necessary to have as much information as possible about the incident, namely:
	  • Date and time of the incident;
	  • Type and severity of the incident;
	  • Affected resources;

	• Possible origins; • Incident status; • Actions taken to resolve the problem; • Who performed the above actions; • Date and time of resolution and closure of the incident. • Finally, for the resolution of the IT incident, an explanatory document of the procedure to be implemented in the event of a data breach is drafted, taking into account the different possible scenarios.
Measures to protect data during storage	Uanataca will monitor the evolution of existing tools and mechanisms to control malware (antimalware, antiphishing, antispam, web and email analysis) to improve the protection of the information assets. The monitoring will be able to: • Perform automatic and periodic analyses to detect any type of malware; • Conduct automatic checks of email attachments and downloads from the web, as they may contain malicious codes; • Block access to certain applications or websites based on the privacy policy, thus creating prevention "blacklists"; • Allow access to certain applications or websites based on the privacy policy, thus creating "whitelists"; • Analyze and detect possible web pages that may contain threats that could jeopardize the processed data.
Measures to ensure event logging	For Uanataca employees and collaborators, a registration phase is provided in which specific accounts with the domain uanataca.com will be created. These registration measures also apply to accounts with direct access to Uanataca's VPNs for remote work. Uanataca has equipped itself with software (Kibana + ElasticSearch) for managing security-related events and monitoring users. This software is configured in On-premise mode, directly on Uanataca's servers. This management system provides that the considered subjects can access their accounts by entering a password, which must meet certain requirements to be sufficiently difficult to guess or decipher. Uanataca also provides for the development of procedures to ensure the custody of centralized archives, allowing access to them only through two-factor authentication, consisting of entering a Password and PIN. Furthermore, considering that access devices may belong to Uanataca or the employee or collaborator, various types of access are distinguished: • Simple worker access, which will have access to the information contained in the archives, emails, wikis, to carry out their work activity, even remotely; • Administration access, via VPN, with two-factor authentication (password plus RSA private key), for those holding higher-level

	administrative roles; • Finally, special access. This type of access, which must be previously authorized, will be granted for the completion of specific and limited-time activities.
Measures to ensure system configuration, including default configuration	Development projects will be managed through REDMINE, an integrated ticket, source code, and documentation (wiki) management tool. It is an open-source and web-based project management and bug tracking software that has been downloaded and configured directly on Uanataca's internal servers.The source code of the applications will be kept up to date through data management repositories (GIT). Authentication to access the repositories will occur through the insertion of username and password (held by each data processing user) through encrypted communication channels. Each project, both REDMINE and GIT, will have different access roles, such as: Administrator, Product Owner, developer. Changes and iterations of the code will be made in independent branches within the same source code manager.
Internal IT and cybersecurity management and governance measures	Uanataca has a Technical Security Committee that will perform the following functions: • Preparation of security standards, in accordance with the prepared guidelines; • Preparation of security procedures, for the implementation of controls derived from the above standards and in accordance with the Security Committee; • Development and elaboration of procedures derived from operational plans for business continuity. • The system complies with ISO/IEC 27001 certification.
Measures to ensure limited data retention	The custody of information and data is classified in terms of retention and deletion of information held by Uanataca. To comply with this requirement, documents will be prepared for each country, taking into account the different legal regimes to be respected, in order to identify the following terms: • Retention period: refers to the minimum period during which Uanataca must retain the information provided by users; • Maximum deletion period: refers to the maximum period after which Uanataca must delete the aforementioned information. This period starts from the moment the retention period expires.
Measures to ensure accountability	To ensure the security of the processed data, Uanataca will appoint a Security Officer responsible for the following functions: • Preparation of risk analysis. • Centralize all actions of Uanataca's Information Security Management System (ISMS). • Communicate the Security Policy to all personnel and interested parties. • Conduct training in the ISMS and classify information according to the classification criteria defined in the corresponding regulations. • Coordinate and monitor the actions carried out by Risk Managers.

	• Notify all personnel entering Uanataca of their obligations regarding compliance with the Security Policy and its regulatory framework. • Verify compliance with the Security Policy in the management of all contracts with third parties, which fall within the scope of the ISMS. • Organize, plan, and conduct periodic ISMS audits. Uanataca will also appoint Risk Managers, who will have the following functions: • They will be responsible for directing and controlling improvement actions to minimize risks; • They will control risk minimization actions so that there is always their traceability; • They will coordinate with the security officer to report on their progress towards the ISMS.
Measures to enable data portability and ensure deletion	Uanataca ensures the deletion of processed data when legal and contractual requirements are no longer met. Below are some of the causes that will allow the deletion of information: • End of the legitimate condition of processing, associated with the end of the contractual relationship that allows the retention of such information. • Expiration of the legal term for the retention of processed information and data. • Repressive exercises by the data subjects. The data subjects may legitimately request the deletion of their personal information held by Uanataca. For this activity, the legislation of the data subject's country of origin will be taken into account. To address these hypotheses, Uanataca has developed a procedure capable of ensuring the deletion of data through two different methods: • The information can be completely destroyed, if in paper format, through the use of shredders or by using specific paper information destruction services. • Digital information will be deleted from the IT archives. Any backups containing copies of such information will also be deleted, so that they cannot be reused.

2. ORGANIZATIONAL SECURITY MEASURES

TYPE OF MEASURE	DESCRIPTION

Procedures to regularly test, verify, and evaluate the effectiveness of technical and organizational measures to ensure the security of processing	Uanataca ensures the authenticity and integration of content by complying with applicable electronic signature regulations and adhering to international standards. Uanataca uses TLS encryption for the HTTPS protocol in its communication systems, applying limited encryption suites where only protocols considered sufficiently secure for AES256 access (TLS 1.2 or higher) are allowed. All algorithms used by Uanataca for the creation and validation of digital and electronic signatures comply with the "cryptographic suite" ETSI TS 119 312. Activities are carried out within the controls for ISO/IEC 27001 certification.

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
Uanataca S.A.U.	Avenida Meridiana 350, piso 3 08027 Barcelona (Spain)	EEA/USA	Provision of SERQC and SERC Service The list of additional data processors can be consulted at the following address: https://www.evicertia.com/es/rgpd
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	EEA/USA	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)