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	*ClickWrap*
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) • **Contact data** (email, phone number); • **Browsing data** (IP address, log).
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	The solution enables secure storage of data packages through the use of a permissioned blockchain based on the Proof of Stake (PoS) consensus mechanism, which ensures immutability and incorruptibility. The plain data stored on ClickWrap's AWS servers is encrypted using Amazon S3's encryption system before being saved. The platform is only accessible via user authentication with ID and password, protected by two-factor authentication (2FA) through a One-Time Password (OTP) sent to the Client's email address. The APIs used for communication with the AWS storage provider are secured through API authentication.
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 blockchain does not store personal data directly, but only a hash of the JSON file, allowing data integrity to be verified without compromising security. A clear-text JSON file is sent to ClickWrap's AWS servers, so that the hash of the stored file can later be compared with the one written on the blockchain. The system is designed to ensure high availability, avoiding congestion and denial of service issues through the use of an Available-To-Promise (ATP) Server.
Measures to protect data during storage	Data stored on AWS servers is encrypted before storage and decrypted only at the time of download. The platform uses SQL relational databases, protected by perimeter defenses, ATP Server, Web Application Firewall (WAF), and encryption via Amazon S3. The system uses WORM (Write Once, Read Many) to ensure data integrity and prevent unauthorized modifications A WAF helps protect web applications by filtering and monitoring HTTP traffic between the web application and the internet, defending against attacks such as cross-site request forgery, cross-site scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a Layer 7 protection (OSI model) and is not designed to defend against all types of attacks. By placing a WAF in front of a web application, a protective shield is created between the application and the internet.

Measures to ensure event logging	The solution ensures the recording and traceability of operations via the blockchain, which stores an immutable hash of the JSON file associated with the consent. The hash of the JSON file allows the authenticity of the user's consent to be proven, verifying that it has not been altered over time. Access logs to the databases and APIs are secured and monitored to detect any suspicious activity.
Measures to ensure system configuration, including default configuration	The application layer of the platform is cloud-native and uses microservices designed to be activated only on demand and automatically removed afterward, reducing exposure to malicious code. The platform adopts a least privilege security model, limiting access strictly to necessary resources. All systems are monitored and updated to prevent configuration vulnerabilities.
Internal IT and cybersecurity management and governance measures	The blockchain used is permissioned, meaning that access is restricted to authorized users who must authenticate using digital certificates or other authentication methods. Blockchain validators are carefully selected following a thorough evaluation of their IT infrastructure and additional elements to ensure an adequate level of security. This type of solution is recommended by data protection authorities as it offers a higher level of privacy. The system is protected by a Web Application Firewall (WAF) to filter and monitor HTTP traffic and prevent attacks such as cross-site forgery, XSS, SQL injection, and file inclusion.
Measures to ensure limited data retention	No clear personal data is stored on the blockchain—only a hash of the JSON file, which cannot be used to reconstruct the original data. The hash stored on the blockchain is deterministic, meaning the same input will always generate the same output, ensuring data integrity verification without the need to store the original data. Retention rules are configured to ensure data minimization in accordance with the Data Protection by Design and by Default principle.
Measures to ensure accountability	Access to the platform is regulated by strong authentication and traceability mechanisms that make it possible to identify every operation carried out. The blockchain provides unalterable cryptographic proof of the performed operation, ensuring the non-repudiation of the consent expressed by the user. Blockchain validators are subject to audits and checks to ensure compliance with security requirements.
Measures to enable data portability and ensure deletion	The solution allows data to be exported in JSON format, ensuring portability and interoperability with other systems. The hash recorded on the blockchain can be verified at any time, ensuring transparency and accessibility of stored data.

	Clear-text data can be deleted upon request, while maintaining the hash on the blockchain for audit purposes, without this resulting in the storage of personal data traceable to the user.

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	The blockchain and encryption system is periodically tested to verify the integrity of hash registration and the reliability of the platform. Security tests are conducted on the APIs and cloud infrastructures to ensure the reliability of access controls. The platform undergoes compliance checks with security and privacy standards, in accordance with the recommendations of data protection authorities.

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*) e MOC (*Monitoring Operation Center*)