Deed of identification and appointment of the Data Processor pursuant to art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 – General Data Protection Regulation ("GDPR") and with reference to the General Provision of the Italian Data Protection Authority (Autorità Garante Privacy) of November 27th, 2008 and subsequent amendments and additions, on the role of the System Administrator.

The **CLIENT** – in its capacity as "Data Controller" (hereinafter referred to as the "**Controller**" for simplicity) pursuant to Articles 4 and 24 of Regulation (EU) 2016/679 (hereinafter referred to as the "GDPR" for simplicity).

APPOINTS
THE EXTERNAL DATA PROCESSOR AND SYSTEM ADMINISTRATOR

STONEX Srl - hereinafter also "Data Processor" (henceforward referred to as the "**Processor**" for simplicity), pursuant to Articles 4 and 28 of the GDPR, with registered office in Via dei Mille no. 4, 20900 Monza (MB), Italy, in the person of its pro-tempore legal representative, and available for contact via e-mail: privacy@stonex.it.

WHEREAS

1. The following terms are defined as:
   a. **Data Controller**: the natural or legal person, public authority, agency or other body who, alone or jointly with others, determines the purposes and means of processing of personal data; where the purposes and means of such processing are determined by the Union or a Member State law, the controller or the specific criteria for its nomination may be provided for by the Union or a Member State law (art. 4 GDPR);
   b. **Data Processor**: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (artt. 4 and 28 GDPR);
   c. **System Administrator**: professional figure dedicated to the management and maintenance of processing systems used to process personal data, including database management systems, complex software systems such as ERP (Enterprise Resource Planning) systems used in large companies and organizations, local networks, and security equipment, to the extent they allow intervention on personal data;
   d. **Data Protection Officer** (DPO): a figure that is already historically present in some European legislations, represents a founding element for accountability, facilitates compliance and the competitive edge of companies (Section 4 of the GDPR and the WP29 - WP243 Guidelines);
   e. **Authorised/designated for processing**: anyone accessing certain information in order to perform specific tasks and functions related to the processing of personal data under the authority of the data controller or the data processor (Art. 29 GDPR and 2-quaterdecies harmonised Legislative Decree 196/2003);
   f. **Processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (art. 4 GDPR);
   g. **Personal data**: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is the one who can be directly or indirectly identified, in particular by reference to an identifier (a name), an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (art. 4 GDPR);
   h. **Special categories of personal data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 9 GDPR);
   i. **Personal data relating to criminal convictions and offences**: personal data relating to criminal convictions and offences or related security measures (art. 10 GDPR);
   j. **Accountability**: the principle of accountability, together with the other rules governing more specifically how to comply with the GDPR and the division of responsibilities, makes it necessary to define the different roles of the various actors involved in a personal data processing activity.

2. By virtue of the relationship existing between the Data Controller and the Data Processor (hereinafter, "the Parties"), pursuant to article 28 of the GDPR, the Data Processor hereby designated shall carry out personal data processing operations on behalf of the Data Controller for the specified purposes and within the scope of the activities connected with the performance of the relationship between the Parties;
3. The Data Processor has the experience, the capacity, the reliability and provides suitable guarantees regarding full compliance with the provisions in force concerning the processing of personal data, including the security profile in relation to the purposes and methods of the processing operations as well as the guarantees for the protection of the rights of the data subject. Appointing the Data Processor, the Data Controller has also taken into account the specialist knowledge (including technical expertise in security and data breach measures), the degree of reliability, reputation and resources at their disposal;
4. In order to better comply with the GDPR, and thus to offer the most appropriate protection of data subjects' data and rights, the Parties intend to regulate, by this deed of appointment, their mutual relations, without any further remuneration or reimbursement.

All the foregoing, which forms an integral part of this document, the Parties agree as follows.

OBJECT OF THE APPOINTMENT OF
THE EXTERNAL DATA PROCESSOR AND SYSTEM ADMNISTRATOR

By virtue of this deed and of the relationship existing between the Parties, the Data Processor is authorised to process the data hereunder punctually identified by nature and purpose, type and categories of data subjects who they refer to and strictly pertinent to the activities carried out on behalf of the Data Controller.

CATEGORIES OF PERSONAL DATA	CATEGORIES OF DATA SUBJECTS	PURPOSE OF PROCESSING	PROCESSING ACTIVITY AND PURPOSES PURSUED
Common data: identification data, contact data	End-user registered on the STX-CLOUD portal.	Technical management and maintenance of the STX-CLOUD system.	☒ the collection; ☒ the recording; ☒ the organization; ☒ the structuring; ☒ the storage, for the processing in consideration, the Processor specifies that it will retain the processed data for the duration of the contract or in any case within a maximum of 12 months from the end of the contract. ☒ the adaptation or modification, ☒ the extraction, ☒ the consultation, ☒ the use, ☒ communication by transmission, ☒ the alignment or combination, ☒ the restriction, ☒ the deletion or destruction.

A. PROCESSOR DUTIES

Signing this deed binds the Data Processor to the Data Controller and gives rise to a series of obligations specifically identified in a separate clause following this document (**Annex A**). The Data Processor is not permitted to process data in a different manner from the one set out by the Data Controller's instructions. A Data processor does violate the GDPR whether not merely processing the data in accordance with the Data Controller's instructions and he will eventually be considered starting to define his own means and purposes. The data processor will therefore be considered data controller with respect to this final processing and may be subject to penalties if he does not limit himself to processing the data according to the instructions given by the data controller.

B. SECURITY MEASURES AND DATA BREACH

The Data Processor is obliged to put in place technical and organisational measures that are adequate to guarantee a level of security appropriate to the risk of the data processing performed (Art. 32 GDPR). In addition, the Data Processor is required to ensure that technical and organisational measures are in place to guarantee a level of security appropriate to the specific risks arising from processing (ref. art. 13 GDPR).

C. EFFECTIVE DATE - DURATION – TERMINATION

Role and powers herein granted to the Data Processor shall have the same duration and effectiveness as the agreement between the Parties and shall therefore be deemed to be annually renewed until the termination of the agreement or until revocation by the Data Controller.
Upon termination of processing, the Data Processor shall, on Data Controller’s instructions, return or delete the personal data and relative existing copies unless otherwise specified in data retention policies (also in relation to the categories of data processed) provided for under Union or Member State law to which the Data Processor is subject to. In both cases, the Data Processor shall at the same time issue a written declaration that no copy of the personal data processed in the name or on behalf of the Data Controller exists.

D. ANNEXES

- ANNEX A. Appointed Data Processor and sub-processors’ duties pursuant to Article 28 and Recital 81
- ANNEX B. Security measures and Data Breach

***

ANNEX A.
APPOINTED DATA PROCESSOR AND SUB-PROCESSORS' DUTIES PURSUANT TO ARTICLE 28 AND RECITAL 81

By virtue of the deed that binds the designated Data Processor to the Data Controller, the Data Processor has the following duties.

1. **Compliance with the instructions issued by the Data Controller**: The Data Processor shall support and assist the Data Controller in the correct management of any processing activities, which shall be carried out in compliance with the obligations established by GDPR. The Data Processor will processes personal data only on documented instructions from the Data Controller, including any personal data transferral to a third country or to international organisation, unless required to do so by the European Union or Member State law to which the processor is subject to; whether the case, the Data Processor shall inform the Data Controller of that legal obligation before starting such processing, unless otherwise denied by the law for public interest's reason;

2. **Confidentiality**: The Data Processor shall ensure, for himself and for the people he has appointed, to process any personal data, with full confidentiality. Whether deemed necessary, the Data Processor shall bind to confidentiality obligations any abovementioned authorised person and covering any period of time following the main relationship' ceasing.

3. **Compliance with applicable laws and regulations**: The Data Processor is required to comply with the provisions of the GDPR and with any other legal provision concerning data protection in force or that might in future amend, integrate or replace the current legislation; The Data Processor is also required to comply with the general measures issued by the competent Supervisory Authority and the guidelines adopted by the European Data Protection Board (hereinafter referred to as "EDPB").

4. **Security measures**: Before starting the processing of personal data, the Data Processor is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from processing (art. 32 GDPR). Please refer to Annex B relating to security measures and the management of a potential data breach.

5. **Audit**: The Data Processor shall yearly report to the Data Controller (and every time he is specifically requested to do so), information concerning the implementation of the provisions this agreement sets out and pursuant to the privacy legislation, either by means of written reports or check lists. Additionally, the Data Processor shall contribute to any auditing activities, including inspections, and promptly inform the Data Controller of any material issue, eg.:
   a. Requests by data subject;
   b. Request by the Supervisory Authority;
   c. Outcome of inspections:
   d. Infringement of the GDPR or other national or European provisions on data protection, or any loss of confidentiality, integrity, and availability of personal data.

6. **Authorised people to process personal data**: The Data Processor shall entrust any persons authorised to process personal data and operating under his responsibility with specific written instructions (unless the Union or Member State legislation otherwise requires) according to art. 29 GDPR. The appointed Data Processor is responsible for the correct execution of the issued instructions (art. 4.10 GDPR).

7. **Second-level Processors or "Sub-Processors"**: The Data Controller authorises the Data Processor to appoint the following subsequent Data Processor (hereinafter, the "Sub-Processor") for the execution of specific processing activities. The Data Processor shall forward to the Data Controller the "Sub-Processor"'s deed of appointment, informing them of any amendments concerning the addition or replacement of other Data Processors, which the Data Controller retains the right to object.

Any "Sub-Processor" do assume the same data protection obligations established in the contract between the original parties. The Sub-Processor is required to: observe, assess and organise the management and protection of processing personal data (implementing all the appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from processing), so that such data are processed in a legal and consistent way and in compliance with laws from time to time in force. Whether failing to fulfil their data protection obligations, the Data Processor remains fully liable to the Data Controller for any Sub-processor he might have appointed, including any case of compensation for damages caused by improper processing, except when he can demonstrate that the damaging event "cannot be attributed to him" (art. 82.1 and 82. 3 GDPR).

8. **Compliance with the General Provision on System Administrators of the Italia Data Protection Authority of November 27th, 2008** (Official Gazette no. 300 of December 24th, 2008) as amended by the General Provision of the Italian Data Protection Authority of June 25th, 2009 (Official Gazette no. 149 of June 30th, 2009): the Processor shall guarantee the Controller that each appointed/authorised System Administrator will access the systems with their own user account and unique password. By accepting this appointment, the Processor undertakes to:
   a. Individually appoint the designated System Administrators of their own organization;
   b. Guarantee that the appointment of the System Administrators is individual and includes a detailed list of the areas of operation permitted, based on the authorization profile assigned;
   c. Annually provide the Controller with an updated list of the System Administrators (names) and verify the activity of the identified subjects, as prescribed by the Italian Data Protection Authority;
   d. Adopt appropriate systems for recording logical access (computer authentication) to processing systems and electronic archives by Systems Administrators. Access logs must be complete, immutable and with the possibility to verify adequately their integrity, to achieve the verification purpose for which they are required.

   The records must include time stamps and the description of the event that has generated them and must be kept for an appropriate period of time, not less than six months.

9. **Data transfers to countries outside the European Economic Area (EEA).** Personal data must remain in EEA countries. Only with the prior Data Controller's written consent they be transferred to countries outside the EEA. Any transfellar shall take place in compliance with the applicable legislation and the EDPB Guidelines ("Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems", adopted on 23 July 2020). The Data Processor must constantly inform the Data Controller about any Extra EEA countries transferral, any guarantees underlying the data transfer and the additional safeguards placed on the importer of personal data through the European Commission's Standard Contractual Clauses (SCC), ref: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf.

10. **Records of processing activities:** Where applicable, each Data Processor shall maintain a record of processing activities carried out on behalf of a controller (art. 30 GDPR). This record, which may eventually be electronically stored, shall contain the information collected by the Data Processor on behalf of the Data Controller. It shall in particular contain:
    a. Data Processor's name and contact details;
    b. the categories of processing carried out on behalf of each Data Controller;
    c. any transfers of personal data to a third country or international organisation;
    d. a general description of the adopted technical measures.
    e. The Data Processor shall make the record available to the supervisory authority upon request and in order to guarantee the monitoring of processing activities (considering art. 82 GDPR).

11. **Data subjects' rights:** The Data Processor shall promptly inform by written communication the Data Controller of any requests a data subject should have addressed under Articles 15 to 22 of GDPR and relating to the purposes of the processing, the source of data, their updating, rectification or erasure , the data portability and restriction of or objection to processing (including for profiling purposes), or in order to withdraw consent and/or lodge a complaint with the Supervisory Authority. In particular, the Data Processor is required to:

a. co-ordinate his activities with the corporate functions the Data Controller has appointed to when dealing with data subjects;
b. implement any appropriate procedures when responding to data subjects' requests or rights' exercise without undue delay, in compliance with art. 12 GDPR.

12. **Other requirements:** the Data Processor is further required to:
    a. co-operate with the Supervisory Authority when requested;
    b. support the activities of the DPO (Data Protection Officer) who acts on behalf of the Data Controller, whehter appointed (articles 37, 38 GDPR);
    c. designate by letter a representative in the Union as per art. 27 GDPR (if applicable).

LIST OF SUB-PROCESSORS OF PROCESSOR:

COMPANY NAME SUB PROCESSOR	E-MAIL OF THE PRIVACY CONTACT PERSON OF THE SUB-PROCESSOR	SERVICE/PROCESSING OF PERSONAL DATA	EEA or EXTRA-EEA COUNTRIES OF LOCATION PROCESSING OF PERSONAL DATA
Amazon Web Services (AWS S3 and AWS EC2).	aws-EU-privacy@amazon.com	Provider of the server where the data processed by the Processor is stored.	The servers are ubicated in the European Economic Space (Frankfurt).

***

ANNEX B.
SECURITY MEASURES AND DATA BREACH
(Section 2 of the GDPR and Recitals 83, 85, 86, 87, 88)

1. **Security Measures**. Taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organisational measures ensuring a level of security appropriate to the risk, as detailed in art. 32 GDPR, and whether possible, including among others:
   a. the pseudonymisation and encryption of personal data;
   b. the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services;
   c. the ability to guarantee the availability of personal data in a timely manner in case of a physical or technical incident;
   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

   Such measures shall ensure a high level of security. While assessing the appropriate level of security, the Data Processor shall in particular consider the risks related to that specific processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed, which might cause material or immaterial physical damage.
   Any further detailed provisions on security objectives to be achieved, and the specific security measures to be implemented, may also be separately provided, by means of correspondence or opinions containing instructions.

2. **Obligations to support**. The Data Processor, whether necessary and upon request, shall help the Data Controller when drafting the "DPIA" (Data Protection Impact Assessment), containing the assessment of specific likelihood and severity of risk related to the processing to be assessed (taking into account the nature, scope, context and purposes of the processing and the sources of risk) and to the technical and organisational measures to be implemented and aiming to mitigate these risks, thus ensuring the protection of personal data and the compliance with GDPR. If necessary, the Data Processor shall submit the DPIA to the DPO (Data Protection Officer) for his/her opinion, if one has previously been appointed (art. 35 and C.90 GDPR).

3. **Data Breach**. Should it become aware of a Data Breach, the Data Processor shall inform the Data Controller by means of written communication without undue delay, so that the Data Controller can notify the personal data breach to the relevant supervisory authority (art. 33 GDPR) and, whether likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall communicate the personal data breach to the data subject (art. 34 GDPR).
   The Data Processor shall help the Data Controller designing specific procedures that make it possible to promptly identify any Data Breaches and specific responses, through the development of a specific policy. This latter policy shall include:
   a. guidelines for the assessment of any data breaches, in order to determine among them which one is likely to result in a high risk to the rights and freedoms of natural persons and therefore needs to be notified to the relevant Supervisory Authority;
   b. guidelines when selecting the information to be disclosed to the data subject through the notification of the data breach when, from a previous assessment, such breach has likely been considered to result in a high risk to the rights and freedoms of the data subject.

   The Data processor shall help the Data Controller to document any data breach by written communication, together with the circumstances in which it occurred, its consequences and the adopted measures to resolve it. Specifically, the following information shall be included:
   a. the nature of breach, including, where possible, the categories and the approximate number of personal records concerned;
   b. the DPO's contact details (if appointed) or other contact details where more information can be obtained;
   c. a description of the likely consequences of the breach;

d. a description of the measures taken (or proposed to be taken) by the controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

This documentation must be made available to the competent supervisory authority through the data breach notification procedure provided for in Article 33 (3) of the GDPR.

***