DATA PROCESSING AGREEMENT

(pursuant to the EU 2016/679 General Data Protection Regulation)

GENERAL PROVISIONS

between

Customer who purchased the Teyuto services or executed a similar document with reference to the Teyuto services (hereinafter also "**Client**" or "**Data Controller**"),

and

Teyuto S.r.l. with registered office in Florence (FI), 50124, via Ippolito Pindemonte no. 63, fiscal code and VAT no. 06781570483, represented by its legal representative (hereinafter also "**Data Processor**").

Data Controller and Data Processor are jointly referred to as "**Parties**" and singly as a "**Party**".

The Parties are entering into this Data Processing Agreement (hereinafter also "**DPA**") to ensure that the Processing of Personal Data by Teyuto S.r.l. within the Service, on behalf of the Client, complies with Applicable Data Protection Law.

As a consequence, by accessing or using the Teyuto S.r.l. Services, the Client is accepting this DPA, which forms an integral part of the Agreement.

WHEREAS

a) this DPA determines the rights and obligations of the Parties with regard to the Processing of Personal Data in the provision of the Services. The details of the Processing are set out in Annex 1 below;
b) the Client wishes to subcontract the Services offered by the Data Processor, which imply the processing of personal data;
c) the present DPA forms an integral part of the Agreement signed by Parties and is intended to govern the obligations of each Party in relation to the Processing of Personal Data necessary for the performance of the Agreement.

Now therefore the Parties agree as follows, expressly acknowledging that the Whereas and the Annexes form a substantial and integral part of this DPA.

1. DEFINITIONS

All capitalized words used herein and not otherwise expressly defined below shall have the meaning assigned thereto in thereto in the Agreement; the terms as used in this DPA shall have the following meaning (words in the singular shall include the plural and words in the plural shall include the singular):

1.1 **Agreement**: refers to an indivisible whole consisting of the Contract of Services between Parties, the Privacy Policy, and this DPA, accepted by the Client before using the Data Processor Services;

1.2 **Applicable Data Protection Law**: means, all laws, regulations and other national and European standards applicable to the processing of personal data implemented under the Agreement between Parties, including in particular Regulation (EU) No. 2016/679 of 27 April 2016 on the protection of personal data (hereinafter "**GDPR**") and all national laws of the Member States of the European Union adopted in addition to or in application of the provisions of the GDPR;

1.3 **Data Breach:** means a security violation resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.4 **Data Controller:** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State Law. For the purposes of this DPA, the Client acts as Data Controller;

1.5 **Data Processor:** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For the purposes of this DPA, Teyuto S.r.l. acts as Data Processor;

1.6 **Data Subject's Request**: means the request submitted by the data subject to the Client or the Data Processor to exercise his/her rights under the Applicable Data Protection Law;

1.7 **Personal Data:** means any information on an identified or identifiable natural person of which the Client is Data Controller;

1.8 **Processing** or **Process:** means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.9 **Services**: means the services provided by the Data Processor to the Client pursuant the terms of the Agreement;

1.10 **Sub-processor:** means any other Data Processors engaged by Teyuto S.r.l. to process the Personal Data on behalf of the Data Controller.

1.11 **Technical and Organizational Measures:** means the technical and organizational measures required pursuant to article 32 of the Regulation (UE) 2016/679.

2. PURPOSE OF THE DPA

2.1 The purpose of this DPA is to define the terms and conditions applicable to the Processing by Teyuto S.r.l. of Personal Data within the use of Teyuto S.r.l. Services by the Client in accordance with Applicable Data Protection Law (Art. 28 § 3) and 4) of GDPR).

2.2 Purpose of these clauses is to establish the conditions under which the Data Processor agrees to carry out the Processing of Personal Data as set out below on behalf of the Data Controller.

2.3 As part of their contractual arrangements, the Parties agree to comply with the Applicable Data Protection Law.

3. DESCRIPTION OF THE PROCESSING CARRIED OUT ON BEHALF OF THE DATA CONTROLLER

The Data Processor shall be authorized to Process the Personal Data necessary to provide the Services under the Agreement which this DPA is enclosed with, on behalf of the Data Controller and pursuant to Art. 28 GDPR. The nature and purposes of Processing, the type of Personal Data processed and the categories of data subjects are specified in **Annex I**.

4. DATA CONTROLLER OBLIGATIONS

4.1. The Data Controller undertakes to: record in writing any instructions regarding the Processing of Personal Data by Teyuto S.r.l. within the Services and supervise the Processing, including conducting audits and inspections of Teyuto S.r.l. if necessary.

4.2. The Data Controller remains solely responsible for the lawfulness of the Processing entrusted to Teyuto S.r.l., particularly regarding the principles and obligations provided for by the Applicable Data Protection Law.

4.3. The Data Controller undertakes also to:

a) provide the Data Processor with the information referred to in article 3 of this Agreement;
b) document in writing its instructions for the Processing of Personal Data;
c) ensure compliance of these instructions with the Applicable Data Protection Law;
d) the decisions material to the security of the organisation of the Processing and of the procedures applied, shall be reached in consultation between Data Controller and Processor;
e) material changes must be agreed in a documented form (in writing, in electronic form) between the Data Processor and the Data Controller. Such arrangements must be put into safekeeping for the duration of this agreement.

5. DATA PROCESSOR'S OBLIGATIONS

5.1 The Data Processor undertakes to:

a) process Personal Data only on documented instructions from the Data Controller, as set out in the Agreement and this DPA, unless required to do so by Union or Member State law to which Teyuto S.r.l. is subject. In this case, Teyuto S.r.l. shall inform the Data Controller of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Data Controller throughout the duration of the Processing of Personal Data. These instructions shall always be documented. Teyuto S.r.l. shall immediately inform the Data Controller if, in its opinion, instructions given by the latter infringe Applicable Data Protection Law.
b) process the Personal Data only for the specific purpose(s) of the Processing, as set out in Annex I, unless it receives further instructions from the Data Controller (*purpose limitation*);
c) process the Personal Data only for the duration detailed in Annex I (*duration of processing*);
d) implement any technical and organizational measures to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the Personal Data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the data subjects (*measures*, as specified in the **Annex II**);
e) grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the Agreement. Teyuto S.r.l. shall ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality, are trained on the Applicable Data Protection Law and are under an appropriate statutory obligation of confidentiality (*access to personal data*);
f) deal promptly and adequately with inquiries from the Data Controller about the Processing of Personal Data in accordance with this DPA and make available to the Data

Controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from Applicable Data Protection Law;

g) shall promptly notify the Data Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the Data Controller (*data subjects' rights*);

h) shall assist the Data Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, considering the nature of the Processing;

i) shall furthermore assist the Data Controller in ensuring compliance with the following obligations, taking into account the nature of the Data Processing and the information available to Teyuto S.r.l.:

- the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (*data protection impact assessment*) where a type of Processing is likely to result in a high risk to the rights and freedoms of data subjects;
- the obligation to ensure that Personal Data is accurate and up to date, by informing the Data Controller without any undue delay if Teyuto S.r.l. becomes aware that the Personal Data it is Processing is inaccurate or has become outdated (*accuracy of the Processing*);

j) must rectify, delete or restrict the Processing, if instructed by the Data Controller and the Data Processor has no legitimate interests in preventing this;

k) shall, without any undue delay, inform the Data Controller of malfunctions, infringements of Applicable Data Protection Law or of specifications contained in the Agreement, and of any suspicions regarding data protection violations or irregularities in the Processing of Personal Data (*data breach*);

l) shall institute a process, if the occasion arises, but in any case, at least once a year, for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Art. 32 §1, lit. d) GDPR).

Pursuant to the Applicable Data Protection Law, the Data Processor designates a data protection officer, that could be contacted at the following e-mail address: dpo@teyuto.com.

6. AUDIT

6.1. At the Data Controller's request, the Data Processor shall permit and contribute to audits of the Processing activities covered by this DPA or if there are indications of non-compliance. In deciding on a review or an audit, the Data Controller may consider any certifications held by the Data Processor. The Data Controller may only carry out a maximum of one (1) audit per contract year.

6.2. The Data Processor undertakes to allow and facilitate the performance of such audits, by providing access to any information strictly required to carry out the verifications, and by making available the personnel and all documentation necessary and useful for the proper implementation of the audit operations.

6.3. Audit will be implemented during business hours, and subject to thirty (30) days' written notice to the Data Processor including the designation of the persons or entities assigned to perform the audit. The Data Controller may choose to conduct the audit by itself or mandate an independent auditor at its exclusive costs. In the latter case, the Data Controller shall ensure that the auditor:

(i) has committed itself to confidentiality or is under an appropriate statutory obligation of confidentiality; (ii) is not a competitor of the Data Processor.

7. SUB-PROCESSORS

7.1. The Data Processor has the Data Controller's general authorization for the engagement of sub-processors from an agreed list (set in the **Annex III**).

7.2. Any changes of that list through the addition or replacement of sub-processors will result in an electronic written notice sent to the Data Controller and warning about the update of the sub-processors' list at least two (2) weeks in advance, thereby giving the Data Controller sufficient time to be able to reasonably object to such changes prior to the engagement of the concerned sub-processor(s). If Data Controller objects to the update of the sub-processors' list, Data Controller may terminate the use of the Data Processor Services by providing written notice, without prejudice to any fees incurred prior to the termination pursuant to the Agreement.

7.3. Where Data Processor engages a sub-processor for carrying out specific processing activities, it shall do so by way of a contract which imposes on the sub-processor, in substance and to the extent possible, the same data protection obligations as the ones imposed on Data Processor in accordance with this DPA. The Data Processor shall ensure that the sub-processor complies with the obligations to which the Data Processor is subject pursuant to this DPA and Applicable Data Protection Law.

7.4. Sub-processor located in third countries may be commissioned for this for purpose, only if the special conditions contained in Art. 44 et seqq. GDPR are fulfilled (such as an adequacy decision of the Commission, standard contractual clauses, approved codes of conduct – Chapter V GDPR). The agreement with the sub-processor must be drafted in writing, which can also take place using an electronic format (Art. 28 §4) and 9) GDPR).

8. DATA TRANSFER

8.1. The Data Controller acknowledges that the Data Processor and/or its sub-processors may transfer and/or maintain the Processing operations in countries outside of the European Economic Area ("EEA").

8.2. Any transfer of data to a third country or an international organization by the Data Processor and/or its sub-processors shall be done only based on documented instructions from the Data Controller or to fulfill a specific requirement under Union or Member State law to which the Data Processor is subject and shall take place in compliance with Applicable Data Protection Law.

9. DATA BREACH

9.1. In the event of a personal Data Breach the Data Processor shall cooperate with and assist the Data Controller to comply with its obligations under Art. 33 and 34 GDPR or under Art. 34 and 35 GDPR (where applicable), considering the nature of processing and the information available to the Data Processor.

9.2. In the event of a personal Data Breach concerning data processed by the Data Controller, the Data Processor shall assist the Data Controller in:

a) notifying the personal Data Breach to the competent supervisory authority/ies, without any undue delay after the Data Controller has become aware of it (when the personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons);

b) obtaining the following information which, pursuant to Applicable Data Protection Law, shall be stated in the Data Controllers' notification, and must at least include: the nature of the Personal Data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; the likely consequences of the personal Data Breach; the measures taken or proposed to be taken by the Data Controller to address the personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

10. SECURITY

The Data Processor undertakes to process the Personal Data in compliance with the measures as set forth in **Annex II**.

11. RELATIONSHIPS WITH THE DATA SUBJECTS

11.1. It's duty of the Data Controller, upon gathering the Personal Data, to provide the data subjects with adequate information on the Processing carried out by the Data Processor.

11.2. The Data Processor shall assist the Data Controller, insofar as possible, with the performance of the obligations deriving from the data subjects' requests.

11.3. The Data Controller is solely responsible for exercising the rights of the data subjects in accordance with Art. 12 to 22 GDPR, including also Art. 7 §3 and 77 GDPR.

11.4. The Data Controller shall inform the Data Processor promptly if errors or irregularities are detected during its examination of the results of the commissioning.

12. MISCELLANEOUS AND FINAL PROVISION

12.1. Following termination of the Agreement, the Data Processor shall, at the choice of the Data Controller,

a) delete all Personal Data processed on behalf of the Data Controller and certify on demand to the latter that it has done so or,

b) return all the Personal Data to the Data Controller and delete existing copies, unless Union or Member State law requires storage of the Personal Data. Until the Personal Data is deleted or returned, the Data Processor shall continue to ensure compliance with this DPA.

12.2. Any amendment or modification of this DPA shall be notified by the Data Processor to the Data Controller.

12.3. The terms and conditions of this DPA are confidential and each Party agrees and represents, on behalf of itself, its employees and agents to whom it is permitted to disclose such information that it will not disclose such information to any third party; provided, that each Party shall have the right to disclose such information to its officers, directors, employees, auditors, attorneys and third party contractors who are under an obligation to maintain the confidentiality thereof and may disclose such information as necessary to comply with an order or subpoena of any administrative agency or a court of competent jurisdiction, or as reasonably necessary to comply with any applicable law or regulation.

12.4. Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns. This DPA

constitutes the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject-matter.

12.5. Each Party's liability deriving from or related to this Agreement shall be subject to the limitations and obligations stated in the Agreement. The Processor shall be liable to the Data Controller for damage culpably caused solely by the Processor, its employees or by its sub-contractors when providing the contractual performance. The contractual parties shall be jointly liable to the data subject for the damage sustained by the latter as a result of data processing that is unauthorised or inaccurate according to the Data Protection Legislation, other data security regulations and performed as part of the commissioned data processing arrangement. According to Art. 82 § 4) GDPR, the Data Controller (controller) and the Processor (processor) shall be jointly and severally liable for all damage caused. The Data Controller reserves its right of recourse against the Processor in the event that it is obliged to pay compensation to the data subject. Moreover Reference is made to Art. 82 GDPR. The liability provisions in this DPA take precedence over all other liability provisions.

12.6. Provisions of this Agreement shall remain in force as long as the Data Processor carries out the Processing of Personal Data on behalf of the Data Controller or until termination of the contract of Services for whatever reason, whether or not the Agreement is replaced by a subsequent one, without prejudice to the provisions of this DPA.

12.7. For the execution of the DPA the Data Processor could be contacted at the following e-mail addresses:

a) For technical and services matters: support@teyuto.com;

b) For privacy and data protection matters: dpo@teyuto.com.

12.8. This Agreement shall be regulated by the laws of Italy. Any disputes deriving from or in connection with this DPA shall be exclusively subject to the jurisdiction of the Court of Milan (Italy).

Florence, July 2024

ANNEX 1

Details on the Processing of Personal Data

Annex 1 includes the information on the Processing of Personal Data required by Article 28 § 3) GDPR.

Object and duration of the Processing

The object of the Processing concerns personal data of the users to grant them the services offered by Teyuto digital platform.

The duration will follow the period of the Agreement signed with the Data Controller (data will be deleted or anonymized or returned to the Data Controller, except for any other retention periods required by law).

Nature and purpose of the Processing

The process is referred to users data that will use the Teyuto digital platform and its services.

The data will be processed to allow the Data Processor to comply with the service Agreement signed with the Data Controller.

Categories of Personal Data to process

All data related to the categories of personal technical data (IP address, IP location, internet service provider used, metadata, browser and device used), personal user data (contact data, fiscal and payment data, common data), personal admin/superuser data (company name, channel name, domain name, company size and employees number, focal point person).

Categories of Data Subjects to whom Personal Data refer

Teyuto digital platform User and Teyuto digital platform SuperUser.

Processing operations

Collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

Obligations and rights of the Data Controller

The obligations and rights of the Company are set out in the Contract and this Agreement.

ANNEX 2

Technical and Organizational Measures

The Data Processor processes the Personal Data with respect to the following safety measures:

a) measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
b) measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
c) measures for the pseudonymisation and the encryption of Personal Data;
d) measures for user identification and authorization;
e) measures for the protection of data during transmission;
f) measures for the protection of data during storage;
g) measures for ensuring events logging;
h) measures for ensuring system configuration, including default configuration;
i) measures for internal IT and IT security governance and management Measures for ensuring accountability;
j) measures for allowing data portability and ensuring erasure;
k) measures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In particular, The Data Processor adopts:

a) two-factor authentication on third-party services used by Teyuto;
b) SSH keys are all password-protected;
c) all features are designed with security and reliability;
d) every device and tool in use is protected and updated (avoiding the storage of data);
e) staff, agents and suppliers are continuously trained on data security practices (yearly training and auditing program in place);
f) backup and restore procedure in place;
g) DDoS attack protection in place;
h) network protection with firewalls;
i) system runs an automated monitoring system that allows us to be aware of problems before they affect the customers;
j) technical staff use alerts so that we are notified immediately of incidents;
k) all domains are protected with DNSSEC, server authentication uses secure SSH keys and direct password authentication is not possible. SSH services are not publicly accessible and are limited to a set of permitted IP addresses;
l) abusive IPs are automatically banned or restricted (preventing brute force attacks on accounts);
m) hardware token generators for all our infrastructure-related sensitive accounts (TOTP supported by hardware);
n) encryption use TLS (1.3) – RSA 2048 bit (elliptic curve and forward secrecy with Diffie-Hellman parameters) and Strict Transport Security (HSTS).

ANNEX 3

Sub-Processors List

The Data Processor uses the third party companies below (*sub-processor*) to Process Personal Data on behalf of the Data Controller, in accordance also with its instructions and strictly pursuant to this DPA and the terms of the agreement between the Data Processor and the sub-processor.

The Data Processor imposes obligations on its sub-processors to implement appropriate technical and organizational measures ensuring that the sub-processing of Personal Data is protected to the standards required by applicable data protection laws. Further information relating to sub-processor security measures can be found via the external links below.

The Data Processor maintains an up-to-date list of the names and locations of all sub-processors below. Data Processors' Client may subscribe to notifications of sub-processor changes to receive updates.

Duration of processing: for each sub-processor below, Processing of Personal Data will be for the duration that the Data Controller uses and continues to use the Data Processor Services, and for the retention periods as set out in this Agreement.

Sub Processor and location	Personal Data Involved	Purposes of processing	Data Transfer Countries	Documentation Link
Microsoft Azure	Technical data Personal User and SuperUser Data	Cloud Storage Provider and Content Delivery Network	USA	Privacy Policy
CloudFlare	Technical data Personal User and SuperUser Data	Content Delivery Network	USA	Privacy Policy
GCore	Technical data Personal User and SuperUser Data	Cloud Storage Provider	Luxembourg	Privacy Policy
Google Cloud	Technical data Personal User and SuperUser Data	Cloud Storage Provider and Content Delivery Network	USA	Privacy Policy
PayPal	Payment data	Payment Provider	USA	Privacy Policy
Stripe	Payment data	Payment Provider	USA	Privacy Policy
Acumbamail	Technical data Personal User and	Ticketing Service Provider	Spain	Privacy Policy

Sub Processor and location	Personal Data Involved	Purposes of processing	Data Transfer Countries	Documentation Link
	SuperUser Data			
Formaloo	Technical data Personal User and SuperUser Data	Customer Care Services	Canada	Privacy Policy
Assembly AI	Technical data Personal User and SuperUser Data	Speech-to-text transcriber provider	USA	Privacy Policy
CrowdPower.io	Technical data Personal User and SuperUser Data	Event Tracking provider	USA	Privacy Policy
Make.com (Celonis Inc.)	Technical, communication and interaction data Personal User and SuperUser Data	Ticketing Service Provider	USA	Privacy Policy
Together.ai	Technical, common and contact data Teyuto Personnel	Prompt engineering	USA	Privacy Policy
Fresh Chat (Freshworks Inc.)	Technical and common data Personal User and SuperUser Data	Customer Care Service	USA	Privacy Policy