DATA PROCESSING ADDENDUM

By entering into the App Software License Agreement, the Customer accepts all the provisions from the Terms and Conditions of Jenz.app, as well as this Data Processing Addendum (“DPA”)

This Addendum is to reflect the Parties’ agreement with regard to the processing of personal data under Jenz as defined in these Terms and Conditions, in accordance with the requirements of regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“GDPR”) and national laws of Croatia incorporating elements of GDPR in the Act on Implementation of General Data Protection Regulation (Official Gazette, No. 44/2018) (“the Act”) in particular.

While providing the services of setting up a Workspace account, in accordance with the respective Agreement (the „Services“) Jenz.app will have access to the Customer’s Confidential Information and personal data as will be submitted by the Customer.

Jenz.app agrees to comply with the following provisions with respect to any Personal Data provided or made accessible by the Customer. By referring to Personal Data throughout this DPA, Parties acknowledge that Personal Data means Account Information, as defined below.

I. DEFINITIONS, SUBJECT MATTER, NATURE AND PURPOSE OF PROCESSING

1.1. Terms used in this DPA shall have following meaning:

- “Account Information” means types of Personal Data Jenz.app collects, as defined under 1.2.c.
- “Data Controller” has the meaning specified for “controller” in the GDPR.
- “Data Processor” has the meaning specified for “processor” in the GDPR.
- “Data Subject” has the meaning specified for “data subject” in the GDPR.
- “Personal Data” (“Data”) has the meaning specified for “personal data” in the GDPR.
- “Processing” has the meaning specified for “processing” in the GDPR.
- “Personnel” means any employee, other authorised staff and/or external contractor with access to Confidential Information.
- “Confidential Information” means materials, information and ideas of or about the Customer/, and their employees, partners, clients, vendors, licensors and other persons, that are not generally known to the public, including without limitation materials, information and ideas relating to business, marketing, information technologies, information systems, plans, operations, products, services, software, methods, procedures, clients, equipment and systems, whether in written, oral or any other form. For the sake of clarity, Personal Data are also Confidential Information.

1.1.1. The Parties acknowledge and agree that when processing Personal Data as part of the Services,
The Customer’s (hereinafter the Customer shall be referred to as the “Data Controller” and/or Customer) employees are acting as Data Subjects and Jenz.app is in the position of Data Controller (hereinafter Jenz.app shall be referred to as the “Data Processor” and/or Jenz.app). and shall process such Personal Data as Data Processor. In such circumstances, the scope of the processing of Personal Data carried out by the Data Processor is as follows:

a. Subject matter, nature and purpose of processing: Personal Data will be processed in order to enable the performance of the Services (i.e. to set-up the Workspace account).

b. Duration: for the entire term of the DPA.

c. Types of Personal Data and categories of the Data Subject: name, surname, email address, phone number, start of work date, title and department, profile picture, Slack ID and profile description.

II. OBLIGATIONS OF DATA PROCESSOR

2.1. The Data Processor shall only process Personal Data on the documented instructions of the Data Controller unless required to do so by the EU/EEA law, which Data Processor is subject to. In such case, Data Processor must disclose that legal requirement to the Data Controller before processing, unless that law prohibits such disclosure on important grounds of public interest.

2.2. Data Processor shall promptly comply with Data Controller’s requests or assist the Data Controller with data subject’s requests for access to, correction of, erasure of, restrictions on processing, objections to processing of Personal Data, defined as Account Information, and the right of portability of Personal Data in Data Processor’s possession.

2.3. If the Data Processor receives any complaint, notice, or communication which relates directly or indirectly to the Processing of the Personal Data or either Party’s compliance with applicable law in connection with Personal Data, it shall promptly notify Data Controller and it shall provide Data Controller with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

2.4. In providing the Services, the Data Processor shall provide Data Controller with access to Personal Data in a manner consistent with the features and functions of the Services and shall ensure that the Data Subjects will be able to execute all their rights in accordance with the GDPR.

III. OBLIGATIONS OF DATA CONTROLLER

3.1. Data Controller has the primary responsibility to ensure that consent of Data Subjects is obtained for the use of Personal Data in situations where such consent is required by the Act or the GDPR.

3.2. Data Processor acknowledges that it is responsible for its own compliance with all applicable data protection laws and that the Data Processor does not determine the purpose for which or the manner in which the Personal Data shall collected and processed.

IV. PERSONAL DATA AND CONFIDENTIAL INFORMATION PROTECTION

4.1. The Data Processor acknowledges and agrees that:

(a) it may use Personal Data solely and exclusively for the limited purpose of providing the Service to Data Controller (the "**Approved Use**");
(b) it shall limit access Personal Data solely to its Personnel who have a need of such access in connection with the performance of the Service and have committed themselves to confidentiality, and grant that access in accordance with the security controls as set out in Article 7;
(c) it shall not disclose or transfer the Personal Data to any third parties, unless necessary and approved by Data Controller in advance and in writing;
(d) it shall reproduce the Personal Data only to the extent necessary for the Approved Use;
(e) it shall implement and maintain appropriate technical and organizational measures and other protections for Personal Data against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to Personal Data, whereas specific requirements for data security are set out in Article 7. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of Personal Data to be protected.

The Data Processor will make available upon the Data Controller's request all information necessary for the Data Controller to demonstrate compliance with all obligations arising from data privacy laws and regulations and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

V. PERSONAL DATA TRANSFERS/SUBPROCESSING

5.1. Data Processor may use third party to process Personal Data with prior written approval by Data Controller.

5.2. Data Processor shall impose on the third parties the same data protection obligations as stipulated in this DPA by way of a written agreement and Data Processor shall ensure that the third party complies with the obligations. Data Processor remains fully liable to Data Controller for the performance of that third party's obligations.

5.3. Data Processor uses the following subprocessors: Q Ltd., in charge of maintenance and support, development of new functionalities and bug fixing, Amazon Web Services EMEA Sarl, for AWS services, such as servers, Firebase, the platform for tracking analytics and Sentry, the platform for error and performance monitoring and the Data Controller, by signing the Agreement explicitly agrees to the processing of its Personal Data by within mentioned subprocessors.

VI. PERSONAL DATA RETENTION AND ARCHIVING

Upon termination of the Agreement, this DPA and/or upon request of the Data Controller, the Data Processor is obliged to return all Personal Data to Data Controller and after the receipt by Data Controller destroy, remove and delete all Confidential Information and Personal Data of its systems immediately unless instructed otherwise in writing by Data Controller or required otherwise by law.

VII. DATA SECURITY MEASURES

7.1. The Data Processor shall establish technological, physical, administrative and procedural safeguards which are consistent with the state of the art practices and include, but are not limited to policies, procedures, standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part, to: (1) protect and ensure the confidentiality, integrity or accessibility of the Personal Data and Data Processor

systems; (2) prevent the unauthorized use of or unauthorized access to Data Processor systems; or (3) prevent a breach or malicious code infection of Data Controller and Data Processor systems.

7.2. In order to adhere to requirements in paragraph 1, the Data Processor shall:

(a) establish security controls for the Confidential Information and Personal Data which include the following items for its Personnel
  (i) security related processes for providing access to internal systems on a need-to-know basis;
  (ii) individual accountability and reasonable protection for administrative and root accounts, and password management;
  (iii) providing individual and unique login ID's;
  (iv) encrypting passwords when passwords are stored or transmitted;
  (v) requiring password to the Data Processor's systems;
  (vi) conducting periodic reviews of access logs to identify unusual occurrences;
  (vii) requiring strong passwords;
(b) implement and apply industry best practices for data security;
(c) maintain commercially reasonable, industry standard back-up, redundancy, disaster recovery, and service continuity measures and procedures related to the Service and preservation of Confidential Information. Data Processor will also periodically test those procedures;
(d) monitor for server-based security events and record such events in audit logs for a minimum of 60 days after an event occurrence. The Data Processor shall also monitor for application-based security, including security events, and record and retain such actions in audit logs for a minimum of 60 days;
(e) implement and maintain Data and Systems Access policy ensuring role-based access controls are in place that restrict access by the Processor Personnel to Personal Data and the systems. If an access to Confidential Information and Personal Data and the systems by the Data Processor Personnel is agreed upon, the Data Processor shall keep an up-to-date list of the Data Processor Personnel with an access to Confidential Information and the scope of rights each person has.

7.3. A "**Security Incident**" means any actual or reasonably suspected unauthorized use of or access to Data Processor systems or access or theft of Confidential Information, an inability to access those systems or Confidential Information and Personal Data due to a malicious use, attack or exploitation of information or systems, unauthorized use of information by a person for purposes of theft, fraud or identity theft, unauthorized disclosure or alteration of information, and/or transmission of malicious code.

7.4. If a Security Incident occurs the Data Processor shall:

(a) immediately notify the Data Controller Privacy and Confidentiality Officer via the email address specified in the Agreement of the Security Incident;
(b) conduct an investigation of the reasons for and circumstances surrounding the Security Incident and report its outcome to Data Controller;
(c) use best efforts and take necessary actions to prevent, contain, and mitigate the impact of the Security Incident;
(d) preserve evidence concerning the Security Incident, including documentation regarding incident response and remedial actions taken;
(e) take all commercially reasonable steps to remedy the Security Incident.

7.5. The Data Processor shall assist and fully cooperate with Data Controller in connection with any investigation that Data Controller conducts with respect to a Security Incident, including:
(a) facilitating interviews with the Data Processor Personnel;
(b) making available to Data Controller all relevant information about the Security Incident;
(c) providing status reports to Data Controller about the Security Incident response activities.

VIII. RIGHTS OF THE DATA SUBJECT

8.1 The Data Processor shall provide the Data Controller with commercially reasonable cooperation and assistance in relation to any request made by a Data Subject or by Data Controller for access to that person's Personal Data, to the extent legally permitted and to the extent the respective Data Subject or Data Controller do not have access to such Personal Data through its use of the Services.

8.2 The Data Processor shall not disclose the Data Subject's Personal Data to a third party other than at the written instruction of the respective Data Subject, unless otherwise required by law or if explicitly stated otherwise in this DPA.

8.3. As soon as the usage of the Services is terminated by the Data Controller, The Data Processor shall delete employees' account information. Data Controller shall remain responsible for collecting any data request or questions from its employees.

IX. LIABILITY AND INDEMNITY

9.1. The Data Processor agrees to indemnify Data Controller and its respective employees (Data Controller and each such person being an ”Indemnified Party“) from losses, claims, including the third party claims, damages and liabilities, joint and several, to which such Indemnified Party may become subject under any applicable law, and related to or arising out of Personal Data defined as Account Information, processing by the Data Processor directly or indirectly to Data Controller. The Data Processor shall reimburse any Indemnified Party for all expenses (including counsel fees and expenses) as they are incurred in connection with the investigation of, preparation for or defence of any pending or threatened claim or any action or proceeding arising there from, whether or not such Indemnified Party is a party and whether or not such claim, action or proceeding is initiated or brought by or on behalf of the client of Data Controller resulting from a breach of any service or negligence by the Data Processor in the performance of the Services contemplated in this DPA.

9.2. The Data Processor will not be responsible for any losses, liabilities, claims, judgments, costs, demands and expenses caused by the negligence, gross negligence or wilful misconduct of Data Controller, its partners, principals, agents, representatives or employees.

9.3. Data Controller shall remain responsible for complying with Data Protection provisions in relation to the content submitted to Jenz and shall remain responsible for obtaining approval from its employees. In no event shall Data Processor be liable for Data Controller not complying with its obligations.

X. SEVERABILITY

In the event any clause of the DPA is considered to be invalid, unlawful, non-enforceable or null and void, this will not result in the invalidity, unlawfulness, non-enforceability or nullity of the entire DPA. In this case, the parties are released from all rights and responsibilities ensuing from such a clause, but only in as far as this stipulation is invalid, non-enforceable or null and void. In this event, the parties will use their best efforts to replace such a clause by a valid clause that has the nearest possible economic and legal significance, as the invalid, non-enforceable or null and void clause.

XI. CLOSING PROVISIONS

This Data Processing Agreement shall enter in force at the moment when the Processing of Personal Data commences under the Agreement or the Trial period as stipulated in the Terms and Conditions at the latest and shall survive valid and applicable through the duration of the Personal Data Processing. This Data Processing Agreement expires with the termination of the Agreement.

Governing Law: The DPA shall be governed by the Croatian law