Data Processing Agreement (DPA)

This Sompani Data Processing Agreement is made between “Sompani”, which stands for Sompani Talent communities, operated by Sompani UG (haftungsbeschränkt), and “Customer”, which stands for any company that registers on one of the talent pools operated by Sompani as "Company" and creates a user account and accepts this agreement for the placement of applicants, by clicking the field "I accept the DPA” on the respective registration website.

Sompani and Customer individually referred to as "Party" and jointly as the "Parties".

WHEREAS

Customer will in the aftermath of the Agreement receive and have access to certain Personal Data from Sompani, as further described that Sompani wishes to be treated by Customer in full compliancy with the applicable privacy and data protection legislation;

Therefore Parties agree to establish the present data processing agreement (the “Data Processing Agreement”) to describe the terms and conditions for the data processing activities in the context of the Services.

In case of conflict between this Data Processing Agreement and the Agreement or another document with regard to the Processing of Personal Data, the modalities of this Data Processing Agreement will prevail.

HAVE AGREED AS FOLLOWS

1. DEFINITIONS

“**Data Protection Legislation**” meaning as in the General Data Protection Regulation 679/2016 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of data (“General Data Protection Regulation” or “GDPR”) and all other national or European legislation implementing or completing the GDPR as well as cyber security legislation.

“**Controller**”, “**Processor**”, “**Data Subject**”, “**Personal Data**”, “**Data Breach**”, “**Processing**” shall have the meaning as defined in the GDPR.

2. QUALIFICATION OF PARTIES

Parties agree that Customer will act as the “Processor” and SOMPANI will act as the “Controller”.

3. TYPE OF PERSONAL DATA COLLECTED AND CATEGORIES OF DATA SUBJECTS

The following Personal Data may be collected if voluntary provided by a Candidate :

- Identification Data (e.g. first name and surname, ID-card Number)
- Previous employment data
- LinkedIn Profile data
- Electronic Data
- Phone Data
- Educational Data
- Personal picture

Categories of Data Subjects:

- Business Customers
- Job-Candidates

4. NATURE AND PURPOSE OF THE COLLECTION AND PROCESSING OF PERSONAL DATA

All Personal Data is uploaded voluntarily, no information is collected without the explicit consent of affected Data Subject. A complete list of Personal Data is provided in Section 3 Privacy Statement in Exhibit D of this Agreement.

5. OBLIGATIONS OF THE CUSTOMER

The Customer (including its employees, agents, (sub) contractors, work-for-hire, or any other person working under its authority) shall, at all times, comply with the Data Protection Legislation in relation to Personal Data Processed by it under the Agreement. The Processor warrants, represents and undertakes to the Controller that it shall only process the Personal Data as limited in de following paragraphs.

The Processor shall:

- not do or allow anything to be done which might bring Controller in any way to be in breach of the Data Protection Legislation.
- assist Controller promptly and appropriately with requests to ensure compliance with Data Protection Legislation.
- not process or disclose Personal Data other than in accordance with Controller's instructions or if required by EU or member state law to which Processor is subject, in which case Processor shall inform Controller of that legal requirement before Processing the Personal Data, unless that law prohibits such information being provided on ground of public interest.
- keep the Personal Data it receives and/or has access to strictly confidential unless allowed under the Agreement.
- take all necessary and appropriate measures to limit the access to the Personal Data to only those persons of its organization under its authority who have a "need-to-know" basis and who are informed and aware of the confidential nature of these Personal Data and are contractually bound by confidentiality obligations.
- create and maintain a record of their "Processing activities" in accordance with article 30 (2) of the General Data Protection Regulation.
- take all necessary and appropriate measures to comply to the principles of Data Protection by Design and Data Protection by Default in accordance with article 25 of the General Data Protection Regulation.
- Implement technical & organizational measures to ensure protection of Personal Data against accidental loss, damage, alteration, unauthorized disclosure or access, destruction or any other form of unlawful, unauthorized or accidental Processing.
- not, without prior written consent of Controller, transfer or give access to the Personal Data to any third party or sub-processor.
- in the event a Data Subject exercises one or more of its rights under the Data Protection Legislation notify Controller of this request as soon as possible and not later than within five (5) business days.
- give assistance to Controller to comply and to answer the exercise of rights of a Data Subject within the timeframe foreseen in the Data Protection Legislation.
- immediately, and in any case within twenty-four (24) hours after such event takes place inform Controller if :
    - It receives an inquiry or a request for inspection or audit from a public authority
    - It intends to disclose Personal Data to any public authority
    - It becomes aware or reasonably suspects that a Data Breach has/will occur
        - In case of a Data Breach, the notification to Controller will as a minimum describe:
            - The nature of the Personal Data
            - The categories and numbers of Data Subjects concerned
            - The categories and numbers of Personal Data records concerned
            - Name and contact details of the Data Protection Officer (DPO) or another relevant contact from whom more information may be obtained
            - The likely consequences of the Data Breach
            - The measures taken or advised to be taken
        - Processor shall give assistance to Controller and take all steps and measures as requested by Controller to assist in the investigation, mitigation of the effects and remediation by proving solutions to solve the Data Breach. Processor shall at its own costs and expenses and following consultation of Controller take all necessary measures to end, and to limit to the maximum extent possible the consequences of the Data Breach.
- give assistance to Controller to comply with the obligations of the Data Protection Legislation (including the articles 32 – 36 of the General Data Protection Regulation).
- cease the Processing of Personal Data immediately upon termination or expiry of the Agreement and, depending on the choice of Controller, immediately return or delete the Personal Data and any copies of it from its systems.

- not transfer Personal Data to any affiliate or third party located in a country outside the European Economic Area without the prior written consent of Controller, unless this third party is located in a country offering an equivalent level of protection of Personal Data.
- appoint and identify a named individual of Processor to act as a Single Point of Contact (SPOC) for any questions regarding Personal Data.

6. AUDIT

At the Controller's request the Processor shall provide the Controller with all information needed to demonstrate that it complies with this Data Processing Agreement. The Processor shall permit the Controller, or a third-party auditor acting under the Controller's instruction, to conduct, at the Processor's cost, a data protection and security audit, concerning the Processor's data security and privacy procedures relating to the processing of Personal Data, and its compliance with the Data Protection Legislation. The Controller shall provide the Processor with at least five (5) days prior written notice of its intention to perform an audit. The notification must include the name of the auditor, a description of the purpose and the scope of the audit. Every auditor who does an inspection will be at all times accompanied by a dedicated employee of the Processor. The cost for an audit will be for the Processor.

7. LIABILITY

Processor shall during and after the term of this Agreement indemnify Controller against all claims, proceedings or actions brought by a competent public authority and/or any Data Subjects against Controller with respect to the Processing by Processor and/or its sub-Processors and shall indemnify Controller against all claims, proceedings or actions brought against Controller arising out of any breach by Processor and/or its Sub-Processor of its data protection obligations under this Agreement. Processor shall indemnify Controller against all costs related to a Data Breach.

8. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

Sompani stores most of its data (including Personal Data) within Germany data centers (Frankfurt, Karlsruhe, Nürnberg), however it has stored certain personal data (namely the CVs of Candidates) outside the European Economic Area (EEA), namely to a company named Cloudinary, which resides in Israel. Cloudinary participates in the EU-US privacy shield (Please read https://cloudinary.com/blog/yet_another_gdpr_blog_post) and is ISO/IEC 27001:2013 certified (Please read: https://cloudinary.com/trust).

Sompani currently uses the following Sub-Processors (evolutive list subject to modifications):

Entity name	Address and company number	Processing activities
Cloudinary	Nadav Soferman, Itai Lahan, Tal Lev-Ami	Candidate CV storage
Hubspot	Cambridge, Massachusetts, United States	CRM system storing name, email etc. of VCs, Recruiters, Candidates
Amazon Web Services (AWS)	440 Terry Avenue North Seattle, WA 98109 USA	Digital infrastructure provider
Google	1600 Amphitheater Parkway	Using Gmail for emailing services, Google Drive for data storage
Zappier Inc.	548 Market St. #62411. San Francisco, CA 94104-5401	Process automations with integrations into database
NetCup GmbH	Daimlerstraße 25 D-76185 Karlsruhe	Server Host, hosting webservices

Sompani will only transfer Personal Data with companies (Processors or Sub-Processors) that (i) bind themselves to the Standard Contractual Clauses (SCC) in accordance with Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council; or alternatively should SCCs not be a possibility (ii) are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, please read European Commission: EU-US Privacy Shield.

Please contact support@sompani.com if you want further information on the specific mechanism used by SOMPANI when transferring Personal Data outside the EEA.

9. TECHNICAL AND ORGANISATIONAL MEASURES

In line with Article 32 GDPR Sompani uses the following *state of the art* technical and organizational measures in its Services:

*** SSL encryption**
*** OAuth authentification**
*** Encrypted passwords using state-of-the-art encryption algorithms.**

Taking into account the state of the art, the 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 Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event 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 the processing.

10. TERM

This Data Processing Agreement shall be valid as of signature by both Parties and for as long as the Agreement is in force and effect. During this Term, this Data Processing Agreement can only be terminated upon mutual agreement between Parties. After the termination of the Processing of the Personal Data or earlier upon request of the Data Controller, the Data Processor shall cease all use of Personal Data and delete all Personal Data and copies thereof in its possession unless otherwise agreed or when deletion of the Personal Data should be technically impossible.

11. ENTIRE AGREEMENT

This Data Processing Agreement shall supersede any other written or oral negotiations, agreements, understanding or representations between the Parties with respect to privacy and the protection of the Personal Data Processed under the Agreement.

12. MODIFICATIONS

This Data Processing Agreement may be supplemented, amended or modified only by the mutual consent of the Parties. No supplement, modification or amendment to this Data Processing Agreement shall be binding unless it is in writing and signed by both Parties.

13. GOVERNING LAW – JURISDICTION

This Data Processing Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with German Law. Any litigation relating to the conclusion, validity, interpretation and/or performance of this Data Processing Agreement or of subsequent contracts or operations derived therefrom, as well as any other litigation concerning or related to this Data Processing Agreement, without any exception, shall be submitted to the exclusive jurisdiction of the commercial courts Berlin.