Data Processing Agreement

1. Background

The Agreement includes the following appendices:

1.1. Existing and approved subprocessors

1.2. Technical and organizational security measures

2. Definitions

The terms used in the Agreement shall have the same meaning as defined in Article 4 of the General Data Protection Regulation (EU) 2016/679, hereinafter (GDPR).

"**Processing**" of personal data means any operation or set of operations which is performed on personal data such as storage, modification, reading, transmission, etc.

"**Applicable Law**" refers to the legislation applicable to the processing of personal data under the Agreement, including the GDPR, supplementary national legislation, and practices, guidelines, and recommendations issued by a Supervisory Authority.

"**Personal Data**" means any information relating to an identified or identifiable natural person ("Data Subject"). In the Agreement, "personal data" is synonymous with "personal data for which the Data Controller is responsible and which the Data Processor processes on behalf of the Data Controller.

"**Data Controller**" is the entity that determines the purposes and means of the processing of personal data and is responsible for ensuring that personal data is processed according to Applicable Law.

"**Data Processor**" is the entity that processes personal data on behalf of the Data Controller and may only process the personal

data according to the Data Controller's instructions and Applicable Law.

“**Data Subjects:** Any identified or identifiable natural person whose personal data is being processed. In the context of this Agreement, this refers to individuals whose personal data is processed by the Data Processor on behalf of the Data Controller, including but not limited to employees, customers, or other individuals associated with the Data Controller.”

"**Supervisory Authority**" means the Swedish Data Protection Authority or any other relevant supervisory authority under law.

3. Introduction

3.1. The Agreement regulates the processing of personal data that the Data Processor performs on behalf of the Data Controller.

3.2. The Agreement is established to meet the requirements of Article 28.3 of the European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC ("GDPR"). According to this provision, a written agreement must be in place regarding the Data Processor's processing of personal data on behalf of the Data Controller.

4. Description of Data Processing

4.1. The Data Processor will have access to personal data in the following ways:

4.1.1. Directly from the Data Controller

4.1.2. Directly from the Data Controller through data input into the Saibon platform.

4.1.3. Automatically through the Saibon platform's usage (e.g., metadata, logs, and analytics data).

4.2. The Data Processor will process personal data for the following purposes:

4.2.1. Enabling and maintaining the functionality of the Saibon platform, including user authentication, account management, and system performance monitoring.

4.2.2. Supporting data analytics and reporting features requested by the Customer to enhance operational efficiencies.

4.2.3. Storing and backing up Customer data securely to ensure business continuity and disaster recovery.

4.2.4. Performing updates, troubleshooting, and resolving technical issues related to the platform.

4.3. The Data Processor will process personal data exclusively according to the Customer's instructions and within the scope defined in this Agreement.

5. Data Processor’s Special Commitments

5.1. The Data Processor undertakes to, in connection with all processing, observe and comply with the principles for processing personal data as stated in Article 5 of the GDPR.

5.2. The Data Processor shall, at the request of the Data Controller, through appropriate technical and organizational measures, assist the Data Controller in fulfilling their obligation to respond to requests for exercising the Data Subjects' rights and, considering the type of processing and available information, conduct data protection impact assessments and prior consultations with the supervisory authority in accordance with Applicable Law. The time taken to execute the Data Controller's request will be invoiced to the Customer according to the current rate. Other costs for the Data Controller's request will be invoiced to the Customer.

5.3. If the Data Processor considers that the instructions provided by the Data Controller are incomplete, deficient, or incorrect, the Data Processor must immediately notify the Data Controller. The Data Processor also has the right to refrain from following the Data Controller's instructions if they are deemed to be contrary to Applicable Law.

5.4. The Data Processor may only process personal data on behalf of the Data Controller in accordance with the Agreement and Applicable Law, unless required to do so by EU law or the national law of a Member State to which the Data Processor is subject. In such cases, the Data Processor shall inform the Data Controller of this legal requirement before processing the personal data unless the law prohibits this on important grounds of public interest.

6. Data Controller's Special Commitments

6.1. The Data Controller determines the purposes of processing personal data. The Data Controller has ownership and formal control over the personal data processed by the Data Processor.

6.2. The Data Controller is responsible for the processing of personal data in relation to the Data Subject.

6.3. The Data Controller is responsible for ensuring that the personal data is accurate and up-to-date and undertakes to indemnify the Data Processor from any claims from Data subjects, or injunctions from appropriate regulator, and pledges to at own cost, assist the Data Processor in any litigation or other administrative proceedings.

7. Personal Data Breach

7.1. In the event of a situation that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data ("Personal Data Breach"), the Data Processor shall without undue delay and at the latest within 48 hours from the discovery of the Personal Data Breach, inform the Data Controller in writing according to the details in the appendix "Contact Details".

7.2. The information shall, to the extent available to the Data Processor, include at least the following:

7.2.1. A description of the circumstances surrounding the Personal Data Breach.

7.2.2. A description of the measures taken or proposed to address the Personal Data Breach and, where appropriate, measures to mitigate its potential adverse effects.

7.2.3. Contact details of the data protection officer or another contact person who can provide more information to the Data Controller.

7.3. If it is not possible for the Data Processor to provide the information at once, the information may be provided in stages without undue further delay.

8. Audit and Review

8.1. The Data Processor shall, at the request of the Data Controller, provide the Data Controller with all necessary information to demonstrate compliance with the obligations set out in Applicable Law and the Agreement.

8.2. If the information provided is not reasonably sufficient to demonstrate compliance with the obligations set out in Applicable Law, the Data Controller has the right to conduct physical audits.

8.3. The Data Processor shall facilitate and contribute to audits and inspections conducted by the Data Controller or an impartial third party appointed by the Data Controller. The Data Controller must notify the Data Processor in writing of the planned audit at least 15 business days in advance.

8.4. Audits may only be conducted:

8.4.1. During normal business hours

8.4.2. After the Data Controller has ensured that the auditor is subject to a confidentiality obligation appropriate to the personal data and information to be audited

8.4.3. In accordance with the Data Processor’s internal policies and security procedures.

8.5. The Data Controller shall bear all costs associated with the audit.

9. Subprocessor

9.1. If the Data Processor plans to engage a subprocessor or replace an existing subprocessor, the Data Processor shall inform the Data

Controller at least 15 business days in advance to allow the Data Controller to object to the change.

9.2. If the Data Controller has reasonable grounds to object to a subprocessor, the parties shall first cooperate to find a suitable alternative; otherwise, the Data Controller and the Data Processor have the right to terminate this Agreement, including any associated Main Agreement.

9.3. When engaging a subprocessor, the Data Processor shall ensure through a contract ("Subprocessor Agreement") that the subprocessor has the same obligations as the Data Processor under the Agreement. This applies particularly to providing sufficient guarantees to implement appropriate technical and organizational measures required to comply with Applicable Law.

9.4. The Data Controller has the right to access the Data Processor's subprocessor agreements (strict commercial information may be redacted).

9.5. The Data Processor shall maintain an updated list of its subprocessors. The list shall be made available to the Data Controller upon request.

10. Records and Data Protection Officer

10.1. If the nature of the processing or the business requires the Data Processor to appoint a Data Protection Officer under Article 37 of the GDPR, the contact details of the Data Protection Officer shall be listed in the appendix "Contact Details."

11. Contact With Supervisory Authority and Data Subjects

11.1. The Data Processor shall promptly inform the Data Controller of any contact with the Data Subject, supervisory authority, or other third party regarding the Data Processor's processing of personal data.

11.2. If the Data Subject makes a request to the Data Processor regarding their rights related to the processing, the Data Processor shall refer the Data Subject to the Data Controller.

11.3. The Data Processor shall permit inspections required by the supervisory authority under Applicable Law.

11.4. The Data Processor is not entitled to represent the Data Controller or otherwise act on behalf of the Data Controller towards the Data Subject, supervisory authority, or any other third party.

12. Technical and Organizational Security Measures

12.1. The Data Processor shall implement appropriate organizational and technical security measures to protect the personal data covered by the Agreement against unauthorized or unlawful access. This includes ensuring sufficient capacity, technical solutions, competence, financial and human resources, procedures, and methods.

12.2. The appropriateness of the technical and organizational security measures shall be assessed considering the latest developments, implementation costs, nature, scope, context, and purposes of the processing, as well as the risk to the fundamental rights and freedoms of individuals.

12.3. If the Data Controller assesses the risk level of the processing as high and thereby conducts a data protection impact assessment, the Data Controller shall share the results with the Data Processor so that they can be considered when determining appropriate security measures.

12.4. The Data Processor shall follow any decisions and consultation opinions issued by the supervisory authority regarding measures to meet the security requirements of Applicable Law and all other requirements concerning the Data Processor under Applicable Law.

12.5. The Data Processor shall ensure that employees (at the Data Processor or its subcontractors) only have access to personal data to the extent necessary and that those who have access to personal data have committed to confidentiality (e.g., by signing an individual confidentiality agreement).

12.6. Only employees or consultants of the Data Processor assessed to have the necessary level of knowledge concerning the nature and

scope of the processing of personal data may process the personal data.

12.7. Computer equipment, storage media, and other equipment used for processing personal data by the Data Processor must be stored in such a way that unauthorized persons cannot access them.

12.8. The security of the Data Processor's premises where personal data is processed must be adequate, including proper lock systems, functioning alarm equipment, protection against fire, water, and burglary, protection against power outages and power disturbances. Equipment used for processing personal data must be well protected against theft and incidents that may destroy the equipment and/or personal data.

13. Control Over Personal Data

The Data Processor shall ensure that the personal data is not accidentally or unlawfully destroyed, altered, or corrupted. The data shall be protected against unauthorized access during storage, transmission, and other processing. Personal data may only be transferred to the Data Controller after verifying the identity of the recipient.

14. Transfer of Personal Data Outside the EU/EES

14.1. The Data Processor primarily processes personal data within the EU/EEA. If personal data is processed outside the EU/EEA, the Data Processor shall ensure that the processing is lawful under Applicable Law by fulfilling one of the following requirements:

14.1.1. There is a decision from the EU Commission that the country ensures an adequate level of protection.

14.1.2. The Data Processor applies the EU Commission's standard contractual clauses for third-country transfers.

14.1.3. The Data Processor has taken other appropriate safeguards that comply with Applicable Law.

15. Liability and Compensation

15.1. A Party is exempt from liability for commitments under the Agreement if the fulfillment is hindered by circumstances of an extraordinary nature beyond the Party's control, which the Party could not reasonably have anticipated and whose consequences the Party could not reasonably have avoided or overcome.

15.2. The Data Processor is liable for direct damages up to a maximum of four price base amounts as defined in Socialförsäkringsbalken (2010:110) SEK resulting from the Data Processor processing personal data in violation of the Data Controller's instructions according to the Agreement and Applicable Law.

15.3. The Data Processor shall compensate the Data Controller for direct damage up to a maximum of four price base amounts SEK. Compensation shall not be paid if the claim is related to processing approved or performed according to the Data Controller's instructions.

15.4. The Data Processor is not responsible for the Data Controller's legal costs.

15.5. The Data Processor's liability does not cover indirect or consequential damages such as lost revenue or profits, contracts, customers or business opportunities, loss of goodwill, or expected savings.

16. Confidential Information

16.1. The Data Processor may not disclose or reveal information about the processing of personal data or the content of personal data covered by this Agreement to third parties or other unauthorized persons. This does not apply to information that the Data Processor is required to disclose by law. The confidentiality obligation is valid from the day both Parties sign the Agreement and indefinitely thereafter. The Data Processor shall ensure that the confidentiality commitment applies to all employees and other persons working for or on behalf of the Data Processor and who are authorized to process personal data.

17. Term and Termination

17.1. The Agreement is valid for as long as the Data Processor processes personal data on behalf of the Data Controller or until the Agreement is replaced by another data processing agreement.

17.2. The Data Processor's obligations under the Agreement shall continue to apply regardless of whether the Agreement has been terminated or otherwise ceased to be valid, as long as the Data Processor processes personal data on behalf of the Data Controller.

18. Deletion and Return of Personal Data

18.1. Upon termination of the Agreement, the Data Processor and any subprocessors shall, at the request of the Data Controller, either delete or return the personal data covered by the Agreement, unless the Data Processor is bound by legal restrictions, such as regulations on accounting, to keep the Data in question.

18.2. If the Data Controller has not requested the return or deletion of personal data within 30 days from the termination of the Agreement, the Data Processor may delete the personal data.

19. Applicable Law and Dispute Resolution

19.1. Swedish law shall apply to this Agreement.

19.2. Disputes arising from the Agreement shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (SCC).

19.3. The Rules for Simplified Arbitration Procedure shall apply unless the SCC considers, taking into account the complexity of the case, the value of the dispute, and other circumstances, that the Arbitration Rules should apply. In such cases, the SCC shall also decide whether the arbitral tribunal shall consist of one or three arbitrators. The SCC shall appoint all arbitrators.

19.4. The seat of arbitration shall be Stockholm, and the language of the proceedings shall be Swedish unless otherwise agreed.

1. Appendix 1 – Existing and Approved Subprocessors

1.1. The following subprocessors are used for processing personal data covered by the Agreement:

Name	**Description**	**Location**	**Safeguards for transferring personal data to third country**
Google Cloud Platform (Google Cloud EMEA Ltd) Google Ireland Ltd, 70 Sir John Rogerson's Quay, Dublin, Ireland	Hosting and storage of platform data, including backups and analytics.	EU	No additional safeguards needed; data processed within the EEA under GDPR compliance.
OpenAI OpCo, LLC 3180 18th St., San Francisco, CA 94110, USA	Integration of OpenAI's LLMs into the Saibon platform.	USA	Standard contractual clauses to ensure compliance with GDPR for international transfers.
Amplitude, Inc. 631 Howard St., San Francisco, CA 94105, USA	Analytics provider to track and understand user engagement on the Saibon platform.	USA	Standard contractual clauses to ensure compliance with GDPR for international transfers.

2. Appendix 2 – Technical and Organizational Security Measures

The Data Processor has implemented the following technical and organizational measures to ensure that personal data is processed securely and protected from loss, misuse, and unauthorized or unlawful access:

2.1. **Technical security measures** include actions implemented through technical solutions:

2.1.1. End-to-end encryption of data in transit and at rest.

2.1.2. Secure access protocols, including multi-factor authentication for system administrators.

2.1.3. Logging and monitoring of all access to personal data.

2.1.4. Secure network

2.1.5. Regular penetration testing and vulnerability scanning.

2.1.6. Backup

2.2. **Organizational security measures** are actions implemented in work processes and routines within the organization:

2.2.1. Internal governance documents (policies/instructions)

2.2.2. GDPR training for all employees with access to personal data

2.2.3. Policies for secure password management and incident response

2.2.4. Strict access controls based on the principle of least privilege

The Data Processor shall conduct reviews of all technical and organizational security measures to ensure alignment with the latest industry standards and evolving security threats. This includes regular updates to encryption protocols, monitoring tools, and incident response plans. Results from these reviews, along with any recommended improvements, shall be shared with the Data Controller upon request.