Data Processing Agreement (DPA)

This Agreement is made between:

Data Controller:

[Customer Name]

Address: [Data Controller's Address]

Email: [Data Controller's Email]

And

Data Processor:

Weavo AS

Organization Number: 932918137

Address: Dyrlandsveien 1, 0875 Oslo, Norway

Email: post@weavo.net

Each referred to as a “Party” and collectively as the “Parties.”

Whereas:

The Data Controller has engaged the Data Processor to provide integration services which necessitate the processing of personal data.

The Parties seek to implement a data processing agreement in compliance with the requirements of the General Data Protection Regulation (EU) 2016/679 (“GDPR”) Article 28(3).

This Agreement outlines the Parties' data protection obligations related to the processing of personal data.

Now, Therefore, the Parties Agree as Follows:

1. Definitions and Interpretation:

Terms used in this Agreement shall have the meanings given to them in the GDPR. "Personal Data," "Processing," "Data Subject," and other relevant terms are as defined in the GDPR.

2. Processing of Personal Data:

2.1. The Data Processor agrees to process Personal Data only on documented instructions from the Data Controller, including with respect to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law.

2.2. Annex 1 specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, and categories of Data Subjects.

3. Rights and Obligations of the Data Controller:

The Data Controller is responsible for ensuring that the processing of Personal Data under this Agreement is in compliance with the GDPR, including the lawfulness of data processing and the protection of the rights of Data Subjects.

4. Confidentiality:

The Data Processor ensures that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security of Processing:

In accordance with applicable data protection regulations, including the General Data Protection Regulation (GDPR), the Data Controller and Data Processor must implement a security framework to protect personal data. This framework should reflect the latest technology and be cost-effective, considering the nature, scope, and purposes of processing, along with potential risks to individuals' rights and freedoms.

Both parties are obligated to employ suitable technical and organizational measures to guard against unauthorized or unlawful processing and against accidental loss, destruction, or damage of personal data. Key strategies include data pseudonymization, encryption, ensuring system resilience, prompt data restoration after incidents, and regular security assessments.

The Data Processor is also tasked with supporting the Data Controller in meeting security obligations by providing necessary information on implemented security measures and assisting in risk mitigation strategies..

6. Use of Sub-processors:

6.1. The Data Processor shall not engage another processor without prior specific or general written authorization of the Data Controller.

6.2. A list of current Sub-processors and the process for adding or replacing Sub-processors is outlined in Annex 2.

7. Data Subject Rights:

The Data Controller must ensure all personal data processing complies with the GDPR (refer to Article 24), relevant EU or Member State data protection laws, and the stipulations of this agreement. They hold the authority and responsibility to define the purpose and method of data processing, ensuring it rests on a lawful basis. This oversight includes verifying that tasks delegated to the Data Processor are legally grounded and aligned with data protection principles.

8. Personal Data Breaches:

Upon discovering any personal data breach, the Data Processor must promptly notify the Data Controller, aiming to do so within 48 hours. This timely notification supports the Data Controller in fulfilling their obligation to report the breach to the appropriate supervisory authority as required by GDPR Article 33.

The Data Processor's support in breach notification includes providing details necessary for the Data Controller's report to the supervisory authority. This information encompasses:

- The type and categories of personal data affected, including an estimate of the number of Data Subjects and personal data records involved.
- Potential consequences of the breach.
- Measures proposed or taken by the Data Controller to address the breach, including efforts to mitigate possible adverse effects.

This streamlined approach ensures swift action and compliance with GDPR requirements regarding personal data breaches.

9. Data Erasure and Return:

Upon termination of the services related to processing, the Data Processor shall, at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller and delete existing copies unless EU or Member State law requires storage of the Personal Data.

10. Audit and Inspection:

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

11. Duration and Termination:

This Agreement shall come into effect on the date it is signed by both Parties and shall continue until the Data Processing services are terminated.

12. Annexes:

Annex 1: Details of Processing Activities

Annex 2: Approved Sub-processors

Annex 1: Details of Processing Activities

The Purpose of the Data Processor's processing of personal data on behalf of the Data Controller is as part of or in reference to the Parties' agreement concerning the supply of one or more business-critical IT solutions by the Data Processor to the Data Controller.

The Nature of the processing includes storage, collection, registration, systematization, interconnection, deletion, archiving, etc., necessary to provide the services stipulated in the Agreement.

Types of Personal Data processed include ordinary personal information such as name, address, email, phone number, date of birth, gender, pictures, IP, and cookie information.

Categories of Data Subjects include employees, users, patients, citizens, customers, clients, or similar.

The Duration of the processing concludes as part of the termination of the SaaS Agreement between the parties.

Annex 2: Approved Sub-processors

At the inception of these Clauses, the Data Controller authorizes the engagement of the following sub-processors to carry out specific processing activities:

Microsoft

- Service provided: Cloud-based data hosting system service
- Transfer to Third Country: Yes

Webflow, Inc.

- Service provided: Website hosting service
- Transfer to Third Country: Yes

Fiken AS

- Service provided: Cloud based accounting system
- Transfer to Third Country: No

Sub-processor Authorization and Changes:

The Data Controller grants general approval for the use of the listed sub-processors. The Data Processor is obligated to notify the Data Controller of any planned changes regarding the addition or replacement of sub-processors at least 30 days in advance, allowing the Data Controller to object to such changes. In case of objection, the Data Processor will address the Data Controller's concerns or may terminate the SaaS Agreement for the specific services involving the disputed sub-processor, with other agreement provisions remaining effective.