Data Processing Agreement

This document constitutes an attachment to the General Terms and Conditions for Position Green and the Service Agreement or Advisory Agreement (for the purposes of this document, any reference to "Service Agreement" shall be interpreted to include both Service Agreement and Advisory Agreement). Terms that are not defined in this attachment shall possess the meaning that is stated in the General Terms and Conditions. This Data Processing Agreement, ("Agreement"), is part of the General Terms and Conditions for the Platform and has been met between:

A. Customer, ("**Controller**"), and

B. Position Green Denmark ApS, (**"Position Green"** and "**Processor**"),

(each respectively a "**Party**" and together as "**Parties**").

This Agreement sets out the rights and obligations of the Controller and of the Processor, when the Processor is processing Personal Data on behalf of the Controller.

The Agreement shall take priority over any similar provisions contained in other agreements between the Parties.

The Agreement along with appendices shall be retained in writing, including electronically, by both Parties.

The Agreement shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (the "GDPR") or other legislation relating to data protection ("Data Protection Legislation").

1. Background

1.1 Position Green provides the Platform with the same name. The Platform aims to help organizations collect, manage, visualize, and report environmental and sustainability data. With the help of the Platform, organizations will achieve an easier, smarter and more efficient way to manage their sustainability and environmental data reporting. The Controller has chosen to be a licensee of the Platform. As a licensee the Controller will report data to the Platform. Position Green will process the personal data that has been reported by the Controller (or by a third party, on the Controller's behalf), as a Data Processor. Position Green may perform Personal Data Processing, as specified in Appendix 2a, to provide the services defined in the Service Agreement or other possible separate agreements between the Parties, ("Services").

1.2 In light of what is stated in section 1.1 above and section 5 in the General Terms and Conditions for the Platform the Parties have agreed on the following Agreement.

2. Personal Data Processing

2.1 Within the context of providing the Services the Processor may process Personal Data, as defined in article 4.1 in the Data Protection Regulation (EU 2016/679), ("GDPR"), which will be processed for purposes decided by the Controller, ("Personal Data"). The Controller is the Controller for such processing of Personal Data per the GDPR, and is thereby responsible for ensuring that the processing of Personal Data takes place in compliance with the GDPR, Data Protection Legislation and the Agreement, e.g. by ensuring that the processing of Personal Data, which the processor undertakes per the agreement has a legal basis.

2.2 The Processor commits to process the Personal Data in accordance with the Agreement or other written agreements between the Parties and only in accordance with the Controller's documented instructions, Appendix 2a, as well as in agreement with the GDPR and any other relevant Data Protection Legislation.

2.3 For the case in which the Processor lacks instructions which the Processor assesses necessary to perform the commitment or commitments the Processor has received from the Controller, within the context of the Services, the Processor shall, without undue delay, inform the Controller about their position and await instructions from the Controller.

2.4 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR.

2.5 Access to the Personal Data within the Processor's organization shall be limited to individuals who require the data to perform the Services and who are obliged to treat information with secrecy or who are legally bound to work under confidentiality.

2.6 The Processor shall undertake certain technical and organizational measures to protect the Personal Data. The measures should achieve a level of security that is reasonable within the consideration of available technology and the cost of the measures, as well as take into consideration whether there are any certain risks with the processing and how sensitive the Personal Data is. Such measures include e.g.:

(a) the ability to continuously assure confidentiality, integrity, accessibility and resilience within the context of the processing;

(b) the ability to restore availability and access to the Personal Data within a reasonable time in the event of a physical or technical incident;

(c) pseudonymization and encryption of the Personal Data when the processing so requires according to applicable law or legislation;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

A detailed description of the technical and organizational security measures to be undertaken by the Processor is included in Appendix 2b.

2.7 The Processor undertakes to, at all times, assure that relevant personnel in its organization act in accordance with this Agreement and the instructions provided by the Controller and to assure that they are informed about the current Data Protection Legislation.

2.8 Furthermore, the Processor shall assist the Controller in ensuring compliance with its obligations pursuant to Article 32 GDPR, by *inter alia* providing the Controller with information concerning the technical and organizational measures already implemented by the Processor pursuant to Article 32 GDPR along with all other information necessary for the Controller to comply with the Controller's obligation under Article 32 GDPR.

2.9 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Processor shall, insofar as this is possible, assist the Controller in the Controller's compliance with fulfilling requests relating to data subject's rights laid down in Chapter III GDPR:

2.10 The Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

(a) The Controller's obligation to without undue delay and not later than 72 hours after having become aware of it, notify the personal data breach to the

competent Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, meaning that the Processor is required to assist in obtaining the information required in order for the Controller to make a notification to the Data Protection Authority. In case of a personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach;

(b) the Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

(c) the Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (data protection impact assessment);

(d) the Controller's obligation to consult the competent Data Protection Authority, prior to processing of Personal Data where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk (prior consultation).

2.11 Any transfer of Personal Data to third countries by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

In case of transfers to third countries, which the Processor has not been instructed to perform by the Controller, and is required under EU or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to the transfer unless that law prohibits such information. Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Agreement:

(a) transfer Personal Data to a controller or a processor in a third country

(b) transfer the processing of Personal Data to a sub-processor in a third country

(c) have the Personal Data processed in by the Processor in a third country

2.12 Should the Controller in conflict with the GDPR not inform the data subject about a personal data breach and the competent Data Protection Authority submits to the Processor to amend the error, the Controller is obliged to compensate the Processor for the costs related to fulfilling the decision of the competent Data Protection Authority.

2.13 The Processor commits to undertake written records over the processing of Personal Data with the content specified in article 30.2 GDPR.

2.14 The Controller hereby gives the Processor a general written authorization to appoint another Processor (so-called "Sub-processor") to process Personal Data.

The Processor has the Controller's general authorization for the engagement of Sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning Sub-processors at least 14 calendar days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned Sub-processor(s). Should the Controller object against the appointment of a new Sub-processor, after having been notified about which according to this section 2.14, and before the appointment has taken place, the Processor is not allowed to make use of the

Sub-processor to process Personal Data, as long as the Controller had a legitimate reason for objecting.

Legitimate reason in this section refers to circumstances on the Sub-processor's side that to a significant extent effect, or with probability risk to affect, the protection of the registered individual's personal integrity, as if for example the new Sub-processor does not satisfy the requirements under the GDPR, or in other Data Protection Legislation.

The list of Sub-processors already authorized by the Controller can be found in Appendix 2a.

Where the Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the Agreement shall be imposed on that Sub-processor.

A copy of such a Sub-processor agreement shall – at the Controller's request – be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in the Agreement are imposed on the Sub-processor. Clauses on business related issues shall not require submission to the Controller.

If the Sub-processor does not fulfil the data protection obligations placed upon the Sub-processor, the Processor shall remain fully liable to the Controller as regards the fulfilment of the data protection obligations of the Sub-processor.

2.15 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and the Agreement, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Should the Controller wish to perform an inspection, the Controller must inform the Processor of this at least 60 calendar days in advance and simultaneously specify the content and extent of the inspection. The Processor holds the right to be compensated for reasonable costs in connection with such an inspection or other audit.

2.16 An inspection following section 2.15 assumes that the Controller, or the Controller-appointed auditor, has entered into necessary secrecy requirements and is following the Processor's safety regulations at the place where the inspection is performed and that the inspection is performed without risking hindering the Processor's operation or the protection of other Processor's information and/or personal data. Information that has been collected as part of an audit, including inspections, must be erased after the completed audit or otherwise when it is no longer required for the purpose of the audit.

2.17 The Processor must be prepared to follow the decision of the relevant Data Protection Authority regarding measures to ensure the fulfillment of applicable Data Protection Legislation.

2.18 The Processor must without undue delay inform the Controller about any potential contact with a Data Protection Authority regarding the Processor's processing of Personal Data. The Processor does not hold the right to represent the Controller or to act on behalf of the Controller towards a Data Protection Authority.

2.19 Upon termination of the provision of Services, the Processor shall be, upon the Controller's request, under obligation to delete all Personal Data processed on behalf of the Controller and certify to the Controller that it has done so or to return all the Personal Data to the Controller and delete existing copies unless Union or Member State law requires storage of the Personal Data.

2.20 The Processor shall compensate the Controller for direct damage in the

event of any damages that can be assigned to the Processor's processing of the Personal Data that goes directly against the Agreement, the GDPR or Data Protection Legislation. The responsibility of the Processor according to this Agreement is limited per breach to what the Controller has paid to the Processor during the 12 months directly preceding the event causing the damage.

3. Other

3.1 This Agreement becomes effective when the Service Agreement has been signed by authorized representatives from both Parties. This Agreement expires simultaneously with the Service Agreement between the Parties, although at the earliest when the Processor has ceased all processing of the Personal Data.

3.2 Should the Data Protection Legislation be altered during the time of this Agreement, or if the authorized regulator issue guidelines, decisions or provisions around the application of the Data Protection Legislation that prompts this Agreement to not meet the requirements of a data processing agreement under Article 28 GDPR, or if the Service Agreement is being altered, this Agreement must be amended to meet any new or added requirements and/or alterations. An alteration of such becomes effective 30 days after the Controller informs the Processor about the alterations. The Processor holds the right to be fairly compensated for reasonable costs arising out of such an alteration of this Agreement that requires modification to the Service to comply with a direct requirement from the Controller.

3.3 Beyond what applies according to the agreement(s) regulating the Services, the Processor commits to, during the time of the Agreement and thereafter, not disclose any Personal Data to a third party. The Personal Data is only allowed to be disclosed to employees of the Processor requiring the data to perform their work, an authorized regulator, or otherwise when disclosure of the Personal Data is required in order to provide the Services under the Service Agreement or by law.

3.4 This Agreement shall be interpreted and applied under Swedish law to the extent that mandatory Data Protection Legislation does not require otherwise. Disputes arising regarding the interpretation or implementation of this Agreement shall be settled per the Service Agreement.

Controller's instructions

Presented below is the processing which the Controller instructs the Processor to execute per the Agreement. Further, instructions referring to the Agreement will replace what is here stated.

Categories of individuals	**Customers and employees at Suppliers and other partners.**
Type of Personal Data	Personal details such as Name, Address, Phone number, Work Title in the company, and Email.
Purpose of processing	The Personal Data is only allowed to be processed for the following purposes and only on account of the Controller: Provide the Position Green Platform and the Advisory Services, including support and other required communication about the Services.
Type and nature of processing	Storage, structuring, reading and deletion.
Storage period	As long as the Controller is a licensee of Position Green, although at the longest until the Controller instructs the Processor to erase Personal Data (which can be referring to some Personal Data or all Personal Data).
Sub-processors	The Processor is currently employing the following Sub-processor(s):

All Personal Data in Position Green Platform are processed within the EU/EEA. Below is a list of approved sub-processors.

Main sub-processors

Service	**Purpose of processing**	**Data Hosting Region**	**Reference**
Bahnhof AB	Data center	Sweden, EU	Sveavägen 41 111 34 Stockholm, Sweden gdpr@bahnhof.net https://bahnhof.cloud/

Cleura AB	Backup provider	Sweden, EU	Blekingegatan 1 371 57 Karlskrona, Sweden privacy@cleura.com https://cleura.com/
Startdeliver AB	Project management tool	Germany, EU	Klarabergsgatan 60 111 21 Stockholm, Sweden support@startdeliver.com https://www.startdeliver.com/

Customer support and/or service

All Personal Data according to below, related to customer support and/or service, are processed in EU/EEA. Below is a list of approved sub-processors.

Service	**Purpose of processing**	**Data Hosting Region**	**Reference**
Hubspot Inc.	Administration of customer relations, support to customers.	Germany, EU	HubSpot Germany GmbH AM Postbahnhof 17 10243 Berlin https://legal.hubspot.com/dpa
Google Cloud EMEA Limited (Ireland)	Information and dialogue regarding service and support. Used for sharing files e.g. project plans.	Ireland, EU	Google Building Gordon House, Barrow St, Grand Canal Dock, Dublin 4, D04 V4X7, Ireland data-access-requests@google.com https://policies.google.com/privacy/
Microsoft Ireland Operations Ltd	Reporting and dialogue concerning discovered bugs and improvement suggestions	Ireland, EU	South County Business Park, One Microsoft Place, Carmanhall And Leopardstown, Dublin, D18 P521, Ireland

			https://aka.ms/privacyresponse
Fortnox AB	Accounting system	Sweden, EU	Box 427 351 06 Växjö, Sweden dpo@fortnox.se https://www.fortnox.se/
Dealhub Inc.	Facilitation of sales workflows, including contract management and document generation.	US	815a Brazos St Austin, Texas 78701 US privacy@dealhub.io https://dealhub.io/privacy-policy/
Chilipiper Inc.	Scheduling and management of meetings, including automated booking and rescheduling.	US	228 Park 78136, New York City, New York, 10003, United States support@chilipiper.com https://www.chilipiper.com/

Technical and organizational security measures

The Processor shall implement the following technical and organizational measures to ensure the security of the Personal Data processed when providing the Services:

- Access Control Policies
- Change Control Policies
- Anti-Virus / Malware policies
- Business Continuation and Disaster recovery plans
- Vulnerability tests and assessments performed

Access control to premises and facilities
Unauthorized access (in the physical sense) must be prevented.
Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

- Access control system
- Door locking (electric door openers etc.)
- Alarm system

Access control to systems
Unauthorized access to IT systems must be prevented.
Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, change of password)
- MFA - Multi Factor Authentication
- Automatic blocking
- Encryption of data media
- MDM - Mobile Device Management

Access control to data
Activities in IT systems not covered by the allocated access rights must be prevented.
Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights. These measures include:

- Differentiated access rights (profiles and roles)
- Automated log of user accesses to:
    - Reports
    - Access
    - Change
    - Restrictions
    - Deletion

Disclosure control
Aspects of the disclosure of Personal Data must be controlled: electronic transfer, data transport, transmission control, etc.
Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Encryption/tunneling (VPN = Virtual Private Network)
- Logging
- Transport-layer security with forward secrecy

Input control
Full documentation of data management and maintenance must be maintained.
Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

- Logging and reporting systems

Availability control
The data must be protected against accidental destruction or loss.
Measures to assure data security (physical/logical):

- Backup procedures
- Uninterruptible power supply (UPS)
- Remote storage
- Regular patches
- Anti-virus/firewall systems
- Intrusion Detection systems
- Independent Network Penetration

Segregation control
Data collected for different purposes must also be Processed separately.
Measures to provide for separate Processing (storage, amendment, deletion, transmission) of data for different purposes:

- "Internal client" concept / limitation of use
- Segregation of functions (production/testing)

Sweden	Norway	Denmark	UK	US	Belgium	Germany
Malmö Stockholm Gothenburg	Oslo	Copenhagen	London	New York Houston	Brussels	Berlin