DATA PROCESSING AGREEMENT

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Between the Customer (“You”, “the data controller”)

and

BEWO ApS (“The Company”, “BeWo”, “Us”, “the data processor”)
CVR 42630888
Prags Boulevard 49E, 3
2300 København S
Denmark

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation).

3. In the context of the provision of BeWo services and products (collectively the "Services") the data processor will process personal data on behalf of the data controller in accordance with the Clauses. Please refer to BeWo Terms of Service document for information regarding the Services.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Three appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure 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.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

   The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

   The data controller may object to the use of a sub-processor if such objection is relevant and reasoned in regard to data protection issues. If the objection is relevant and reasoned, BeWo may suggest a new sub-processor in order for the Controller to accept that one or give the data controller the right to cancel the Service Agreement (at BeWo's sole discretion). For avoidance of doubt, the discontinuance of sub-processors do not require written notices to the data controller.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such

a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

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

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data 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 data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall apply for the duration of the provision of personal data processing services and remains in force until terminated by one of the Parties. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

1. You may contact BeWo using the following email: contact@bewo.io

Appendix A Information about the processing

A.1. The nature and purpose of the data processor's processing of personal data on behalf of the data controller

BeWo will process Personal Data as necessary to provide the Services under the Agreement. BeWo does not sell Customer Data (or end user information within such Customer Data) and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

a. BeWo provides a sustainability reporting software platform and other related services, as described in the Agreement. BeWo will process Customer Data as a data processor in accordance with Customer's instructions as outlined in Appendix C of this Agreement.

b. The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of BeWo's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

A.3. The processing includes the following categories of data subjects and types of personal data about data subjects:

Any individual and/or information system accessing and/or using the Services through the Customer's account ("Users"); third parties with whom Customer or Customer's Users have a commercial or business relationship ("Third Parties").

Types of Customer Data:

a. Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (payment information); information used for sustainability reporting (name, contact details);

b. Third Parties: Contact details included in documents processed for the purpose of sustainability reporting; identity information (name, email address, title, contact details) submitted to BeWo by Customer or Customer's Users.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

As between BeWo and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF SERVICE	PROCESSING LOCATION
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin, Ireland	Hosting services / Email domain provider	Ireland, France Netherlands (backup location)
Hotjar Limited	Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta	User experience optimization	EU
Hubspot Inc.	2 Canal Park Cambridge, MA 02141 United States	Customer Relationship Management system	US based
Stripe, Inc.	South San Francisco, 354 Oyster Point Blvd, United States	Payment processing	US based
Slack Technologies Limited	Salesforce Tower 60 R801, North Dock Dublin	Internal communications	EU
Twilio Ireland Limited	3 DUBLIN LANDING NORTH WALL QUAY DUBLIN, D01C4E0 Ireland	Email provider	EU

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

Customer Processing of Customer Data: Customer agrees that (i) it shall comply with its obligations as a data controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to BeWo, and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for BeWo to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

Customer Instructions: BeWo shall process Customer Data in accordance with Customer's instructions. By entering into the Agreement, Customer instructs BeWo to Process Customer Data to provide the Services and pursuant to any other written instructions given by Customer and acknowledged in writing by BeWo as constituting instructions for purposes of this Agreement. Customer acknowledges and agrees that such instruction authorizes BeWo to Process Customer Data (a) to perform its obligations and exercise its rights under the Agreement; (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; and (c) to provide the service as described in the Terms of Service, including but not limited to billing, account management, technical support and product development.

BeWo Processing of Customer Data: BeWo shall process Customer Data for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Master Service Agreement set out the Customer's complete and final instructions to BeWo in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and BeWo.

C.2. Security of processing

BeWo shall maintain appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of Customer Data, as described in BeWo IT Security Policy provided below. Security Measures shall include appropriate administrative, technical, and physical controls, as defined by industry standards. Customer is responsible for determining whether BeWo's Security Measures meet Customer's requirements and legal obligations under Data Protection Laws.

Customer Responsibilities: Customer agrees that, except as provided by this DPA, it is responsible for its secure use of the Services, including securing credentials and encrypting Customer Data in transit to the Services. Customer is additionally responsible for securing and backing up copies of Customer Data that are exported and stored outside the Services.

Confidentiality of processing: BeWo shall ensure that any person who is authorized by BeWo to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty), adhere to all safeguards prescribed by law and have received appropriate training on their responsibilities.

See BeWo IT Security Policy for handling the Controller's personal data on BeWo website: https://www.bewo.io/legal

C.4. Storage period/erasure procedures

BeWo shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed including but not limited to providing the Services. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

C.5. Processing location

Data center locations: BeWo may transfer and process Customer Data where BeWo, its Affiliates or its sub-processors maintain data processing operations, in accordance with Appendix B. BeWo shall proceed to such transfers only when it is deemed absolutely necessary to provide the Services as described in the Terms and Services and only the personal data that is absolutely necessary. BeWo shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

C.6. Instruction on the transfer of personal data to third countries

Where a transfer of personal data occurs between BeWo and a sub-data processor located outside of the EEA, the transfer of personal data will include one of the following appropriate safeguards, as applicable:

(i) The adoption by the parties of the EU model clauses resulting from the EU Commission implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(ii) Any other appropriate safeguards recognized by the European Data Protection Regulation 2016/679 such as an adequacy decision, an approved code of conduct or an appropriate certification mechanism.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

BeWo accepts and agrees to the data controller being able to conduct audits in the manner chosen by the data controller. The audits may be conducted as written audits or as inspections at BeWo's location. The data controller must give BeWo 30 days prior written notice of inspections at BeWo's location.

The data controller is entitled at its own cost to appoint an independent expert who shall have access to BeWo's location and receive the necessary information in order to be able to audit whether BeWo complies with its obligations under the Agreement, including ensuring that the appropriate technical and organisational security measures have been implemented. The expert shall upon BeWo's request sign a customary non-disclosure agreement, and treat all information obtained or received from BeWo confidentially, and may only share the information with the data controller and BeWo.

BeWo shall cooperate with the Controller without undue delay and provide the Controller with requested signed declarations, statements and similar to verify the compliance with this DPA and GDPR.