

DATA PROCESSING AGREEMENT “CLIMAX”

This is the Data Processing Agreement for Climax (the "DPA"), a software as a service solution offered by Sparqing B.V., having its office at Aert van Nesstraat 45 (3012 CA) in Rotterdam, The Netherlands, and registered with the Dutch Chamber of Commerce under number 80769519, in the role of a 'processor' and in this DPA hereafter referred to as "Climax".

1. DEFINITIONS

- 1.1 In this DPA words written with capitals and not defined elsewhere will have the following meaning:
 - 1.1.1 Customer: means the legal person, that is interested in the Service and/or has accepted these Terms in order to access and make use of the Service;
 - 1.1.2 Customer Data: means all data, documents and materials uploaded or transmitted to the Service by the Customer or generated as a result of the use of the Service by the Customer, excluding Aggregate Data and Anonymous Data;
 - 1.1.3 GDPR: means the General Data Protection Regulation (Regulation (EU) 2016/679);
 - 1.1.4 Personal Data: any information relating to an identified or identifiable natural person that Climax processes on behalf of the Customer;
 - 1.1.5 Service: means the software products and solutions known under the name 'Climax' and provided by Climax to the Customer 'as a service' in accordance with these Terms;
 - 1.1.6 Support: means support in relation to the use of, and the identification and resolution of Errors in the Service, but not including the provision of development and/or consultancy services in connection with the creation of (additional) modules or functionality in the Service;
 - 1.1.7 Terms: the [SaaS Terms and Conditions](#) for Climax available via the [website](#).

2. GENERAL

- 2.1 The Climax Service allows Customer to measure, monitor and report on its carbon footprint. An activity for which Customer has tasked Climax to perform. Climax does not require Personal Data to perform the Service however Customer Data that is being transferred by Customer may include personal data for which the effort by Customer to exclude such data is disproportionately challenging. Accordingly, for the purpose of providing and maintaining the Service and providing Support or additional services, Climax may have access to Personal Data of the Customer, its employees and/or customers of the Customer. Climax processes such Personal Data on behalf of the Customer to perform the Service, therefore Climax qualifies as the 'processor' and the Customer as the 'controller' as defined in the GDPR.
- 2.2 A copy of the Customer Data that is transferred by Customer to Climax, is stored by Climax for audit purposes. Climax does not process Personal Data to calculate carbon footprints nor does it visualise Personal Data through its dashboard.
- 2.3 Customer is fully responsible for the Personal Data that it processes when making use of Service provided by Climax. Customer guarantees vis-à-vis Climax that the content, use and/or processing of the Personal Data are not unlawful and do not infringe any data subject's right. Customer indemnifies Climax against any claims by a third party instituted, for whatever reason, in connection with these data or the performance of the Agreement.
- 2.4 Climax applies a [Privacy Statement](#) that can be consulted on Climax' [website](#). In addition to accepting these Terms, Customer declares to agree with the content of Climax' Privacy Statement.
- 2.5 This DPA is an integral part of the Terms as applicable between the Parties. For the avoidance of doubt,

the liability as agreed upon in the Terms is applicable to this DPA.

- 2.6 In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.

3. PROCESSING OF PERSONAL DATA

- 3.1 The Customer provides large bulks of data to Climax. The categories of Personal Data therefore vary depending on the data provided by the Customer. The categories of Personal Data include, but are not limited to, names, contact details (e-mail address, phone number, address), license plate number, travel/employee expenses, hourly rates and financial data (bank account numbers, management fees).
- 3.2 The categories of Data Subjects vary depending on the data provided by the Customer. The categories of data subjects from whom Personal Data can be processed by Climax include, but are not limited to, employees, customers and suppliers of the Customer.
- 3.3 The Personal Data will be processed for the duration of the Agreement and no longer than five years after the Personal Data has been transferred by Customer to Climax.
- 3.4 Climax' services are not intended for processing special categories of personal data or data relating to convictions under criminal law or criminal offences. Customer is responsible not to share these categories with Climax.

4. RIGHTS AND OBLIGATIONS

- 4.1 Climax will process the Personal Data solely upon written instruction and on behalf of Customer, unless required to do so by law. In this case, Climax will inform the Customer of this legal requirement unless prohibited by law.
- 4.2 Climax ensures that the obligation to observe confidentiality is imposed on any person processing Personal Data under Climax' responsibility.
- 4.3 Customer warrants that the instructions and related processing activities under this DPA are not unlawful and indemnifies Climax against any claims of third parties (including data subjects and data protection authorities) arising from or in connection with a breach of this warranty.
- 4.4 Climax is entitled to appoint third parties (e.g. sub-processors) for the processing of the Personal Data. Climax' shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in this DPA. In the event Climax intends to replace or add a [sub-processor](#), Climax will inform Customer of the intended change via its [website](#). Customer may substantially object to the intended change within five (5) Business Days after receiving the notice, in which event Climax and Customer will discuss a solution or termination of the Service.
- 4.5 As far as legally required and reasonably possible, Climax will provide assistance to Customer in the compliance with its legal obligations to take appropriate security measures, handling data breaches, carrying out data protection impact assessments (DPIA) including prior consultations and/or data subject requests. Climax may charge Customer its reasonable costs for providing such assistance.
- 4.6 If Climax receives a data subject request for the Personal Data, it will timely and adequately handle such request. If relevant Climax will forward the request to the Customer.
- 4.7 If, further to a request or a lawfully issued order by a public authority or in the context of a statutory obligation, Climax is requested to perform activities with relation to Customer Data, involving Personal Data, Climax may charge Customer its reasonable costs involved in such performance.
- 4.8 Climax will process the Personal Data in countries within the European Economic Area (EEA). Climax may

transfer the Personal Data to a country outside the EEA, provided that the legal requirements for such transfer have been met.

- 4.9 Climax will take adequate technical and organisational measures to protect the Personal Data against loss or any form of unlawful processing (such as the unauthorised access to or alteration or disclosure of the Personal Data), thereby taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the Personal Data to be protected as included in Schedule 1. Customer may request Climax to implement additional security measures. Climax may charge Customer for the costs involved in implementing such adjustments as requested by Customer.
- 4.10 Climax does not guarantee that the security measures are effective in all circumstances. In the event of a data breach at Climax or any sub-processors, Climax will inform Customer about the data breach without undue delay after becoming aware of the breach, thereby including all relevant details regarding the breach. Customer shall at all times remain responsible for the notification of a data breach to the relevant data protection authority and/or data subject(s). Where requested by Customer, Climax will provide assistance to Customer to comply with its legal obligations under the GDPR.
- 4.11 At Customer's substantiated and reasonable request, Climax provides all information that is reasonably required to demonstrate its compliance with the arrangements laid down in this DPA with respect to Personal Data processing, for example by means of a certificate, an audit report or third party memorandum or by means of other information to be provided by Climax. If Customer nevertheless has substantiated reasons to assume that the Personal Data are not processed in accordance with this DPA and/or GDPR, Customer is entitled, with a maximum of once per calendar year and with prior notification to Climax of at least two weeks, to – at its own cost - have an audit carried out by an independent IT auditor who will be bound to confidentiality, in order to verify Climax' compliance with this clause, more specifically the security measures. Customer shall ensure that any such audit will be carried out in a manner that has the least effect as possible on the normal business operations of Climax.
- 4.12 Climax and Customer will discuss the findings of a report as soon as possible and comply with proposed improvement measures insofar this can be reasonably expected from them, thereby taking into account processing risks and intended use in connection with the Service, state of the art and implementation costs.

5. TERMINATION

- 5.1 In the event this DPA ends, Climax will, within a reasonable time, return and/or deletes any existing copies of Personal Data processed on behalf of the client in such a way that they can no longer be used and are rendered inaccessible.
- 5.2 The provision of article 5.1 does not apply if statutory provisions should prohibit Climax to delete the Personal Data or return these, in part or in full. In such an event Climax only continues to process the Personal Data insofar as required under its statutory obligations.

SCHEDULE 1 - TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Climax has implemented technical and organisational measures in accordance with the ISO/IEC 27001 standard.

More specifically we've take the following measures:

- *The source data transferred by Customer to Climax that can contain Personal Data will be kept separate and secure. Only one or two persons can access the source data (access restriction) with a special security. Regarding the data that does not contain any personal data, no further restrictions will be included.*
- *Measures of pseudonymisation and encryption of personal data.*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.*
- *Measures for user identification and authorisation.*
- *Measures for the protection of data during transmission.*
- *Measures for the protection of data during storage.*
- *Measures for ensuring event logging.*