DATA PROCESSING AGREEMENT

1. Background and Interpretation

1.1 In order to fulfil the subscription or partnership agreement (the “**Agreement**”) between the parties, CarbonZero AB (the “**Processor**”) will process personal data on behalf of the Customer or Partner (as defined in the Agreement) (the “**Controller**”) in the capacity as the Controller’s data processor.

1.2 This data processing agreement (the “**DPA**”) forms an integral part of the Agreement. The purpose of this DPA is to ensure a secure, correct and legal processing of personal data and to comply with applicable requirements for data processing agreements as well as to ensure adequate protection for the personal data processed within the scope of the Agreement.

1.1 In cases where the Controller acts as a data processor on behalf of another entity (for example, a partner to the Controller or Customer or a company within the Controller's corporate group) that is a data controller, the Processor instead acts as a sub-processor. If another legal entity within the Controller's corporate group is the data controller for personal data that the Processor processes under the DPA, the Processor's obligations towards the Controller shall also apply to such legal entity acting as data controller to the extent necessary to comply with applicable data protection laws.

1.2 The GDPR and a supervisory authority's binding decisions, recommendations and guidelines, practices in the field of data protection, supplementary local adaptation and legislation as well as sector-specific legislation in relation to data protection are collectively referred to as the “**Data Protection Rules**”.

1.3 Any terms used in this DPA, e.g. *processing*, *personal data, data subjects, supervisory authority*, etc., shall primarily have the meaning as stated in the GDPR and otherwise in accordance with the Agreement, unless otherwise clearly indicated by the circumstances. The terms “processing” and “personal data” refer exclusively to such processing and such personal data that the Processor processes on behalf of the Controller in accordance with this DPA. In addition, the definitions used in the Agreement shall have the same meaning in this DPA unless otherwise is expressly stated or indicated by the circumstances.

2. Instructions and Responsibilities

1.1 The categories of personal data and categories of data subjects processed by the Processor under this DPA as well as the purpose, nature, duration and objects of this processing, are described in the instructions on processing of personal data in **Appendix A**.

1.2 The Controller undertakes to comply with the Data Protection Rules. The Controller shall in particular:

(a) be contact person towards data subjects and respond to their inquiries regarding the processing of their personal data;

(b) ensure the lawfulness of the processing of personal data, provide information to data subjects pursuant to Articles 13 and 14 of the GDPR and maintain a record of processing activities under its responsibility;

(c) provide the Processor with documented instructions for the Processor's processing of personal data, including instructions regarding the subject-matter, duration, nature and purpose of the processing as well as the type of personal data and categories of data subjects;

(d) immediately inform the Processor of changes that affect the Processor's obligations under this DPA;

(e) immediately inform the Processor if a third-party takes action or lodges a claim against the Controller as a result of the Processor's processing under this DPA; and

(f) immediately inform the Processor if anyone else is the data controller or joint data controller with the Controller for processing of personal data according to this DPA.

1.3 When processing personal data, the Processor shall:

(a) only process personal data in accordance with the Controller's documented instructions, which at the time of the parties entering into this DPA are set out in Appendix A, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor, or a party that process personal data as sub-processor to the Processor ("**Sub-processor**"), is subject to. In such a case, the Processor or the Sub-processor shall inform the Controller of that legal requirement before the processing, unless the law prohibits such information on important grounds of public interest;

(b) ensure that persons authorized to process the personal data on behalf of the Processor have committed themselves to confidentiality for such processing or are under an appropriate statutory obligation of confidentiality;

(c) maintain an adequate level of security for the personal data by implementing all technical and organizational measures set out in Article 32 of the GDPR in the manner set out in section 3 below;

(d) respect the conditions referred to in paragraphs 2 and 4 in Article 28 of the GDPR for engaging a Sub-processor;

(e) taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(f) assist the Controller in ensuring compliance with the obligations pursuant to Articles 32-36 of the GDPR, taking into account the nature of the processing and the information available to the Processor;

(g) at the choice of the Controller, delete or return all the personal data to the Controller after the end of the Agreement, and delete existing copies, unless Union law or applicable national law of an EU Member State requires storage of the personal data; and

(h) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor agreed upon by the parties.

1.4 The Processor shall notify the Controller without undue delay, if, in the Processor’s view, an instruction infringes the Data Protection Rules. In addition, the Processor shall without undue delay inform the Controller of any changes affecting the Processor’s obligations pursuant to this DPA.

2. Security

2.1 The Processor shall implement technical and organisational security measures in order to protect the personal data against destruction, alteration, unauthorised disclosure and unauthorised access. The measures shall ensure a level of security that is appropriate considering the state of the art, the costs of implementation, the nature, scope, context and purpose of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The Processor may amend its technical and organisational measures.

2.2 The Processor shall notify the Controller of accidental or unauthorised access to personal data or any other personal data breach without undue delay after becoming aware of such data breach and pursuant to Article 33 of the GDPR. Such notification shall not in any way imply that the Processor has committed any wrongful act or omission, or that the Processor shall become liable for the personal data breach.

2.3 If the Controller during the term of this DPA requires that the Processor takes additional security measures, the Processor shall as far as possible meet such requirements provided that the Controller pays and takes responsibility for any and all costs associated with such additional measures.

3. Confidentiality and disclosure of information

3.1 In addition to what follows from the Agreement concerning confidentiality, the Processor shall not without the Controller's prior written consent, disclose or otherwise make available personal data to any third-party, except (i) to the Sub-processors that have been engaged in accordance with this DPA, or (ii) if the personal data is ordered to be shared with the supervisory authority or should be disclosed according to the Data Protection Rules or another statutory obligation.

In the event that the Processor is required to disclose personal data according to the Data Protection Rules or other applicable legislation, the Processor shall take all actions to request confidentiality in connection with the requested information and immediately inform the Controller of the disclosure, in so far as the Processor is not prevented from doing so under the Data Protection Rules or other legislation.

3.2 If the Processor receives a request from a data subject, supervisory authority or any other third-party regarding obtaining access to personal data that the Processor processes on behalf of the Controller, the Processor shall immediately forward the request to the Controller.

3.3 The Processor shall without undue delay inform the Controller of any contacts from supervisory authority regarding the processing of personal data and provide the Controller, to the extent permitted by law, with all information relevant in this regard. The Processor is not entitled to represent or act on the Controller's behalf in relation to supervisory authority.

4. Sub-processors and transfers to Third Countries

4.1 The Controller hereby grants the Processor with a general authorisation to engage Sub-processors. Sub-processors engaged at the time of the conclusion of the Agreement are listed in the list of Sub-processors in **Appendix B**. The Processor shall enter into a data processing agreement with each Sub-processor, according to which, the corresponding data protection obligations as set out in this DPA, are imposed upon the Sub-processor. The Processor is responsible towards the Controller for Sub-processors' performance of its undertakings in relation to the Controller.

4.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors by maintaining an updated list of Sub-processors at https://www.eandox.com/legal-documents, which the Controller may access from time to time, thereby giving the Controller the opportunity to object to such changes. Such objection shall be made in writing. If the Controller objects to the Processor engaging a Sub-processor and the parties are unable to agree within a reasonable time, the Processor shall have the right to terminate the DPA and/or relevant parts of the Agreement in whole or in part with thirty (30) days' notice. If the Processor would choose to adapt to such objection from the Controller, the Processor shall be entitled to reasonable compensation from the Controller for the costs that the Processor incurs as a result of the adaptation.

4.3 Upon the Controller's request, the Processor shall provide the Controller with a correct and up-to-date list containing the Sub-processors that have been engaged in the processing of personal data, the Sub-processors' contact information, the geographic location of the Sub-processor's processing and which processing of personal data each Sub-processor performs.

4.4 If the Processor and/or Sub-processors transfers personal data outside the EU/EEA, such transfer shall always comply with the applicable data protection requirements according to the Data Protection Rules. The Processor shall keep the Controller informed about the legal grounds for the transfer.

5. Liability

5.1 The liability of each party is limited in accordance with what is stated in the Agreement.

5.2 Each party shall be fully and solely responsible for compensating any damages and administrative fines imposed on it under Articles 82 and/or 83 of the GDPR.

6. Term and Termination

6.1 The DPA is valid from the time the Agreement is entered into.

6.2 Upon termination of the Agreement without undue delay, the Processor shall either delete or return all personal data, in accordance with the Controller's instructions to the Processor and ensure that each Sub-processor does the same. If the Controller does not instruct the Processor to return the personal data, the Processor shall promptly delete the personal data, including any existing copies, unless the Controller provides timely instructions to the contrary. In any case, the Processor shall ensure that the personal data is no longer available or retrievable for the Processor. The Processor shall ensure this no later than thirty (30) days after the processing discontinues. Upon the Controller's request, the Processor shall confirm in writing that deletion has occurred and provide a written description of the measures taken in this regard.

6.3 This DPA remains in force as long as the Processor processes personal data on behalf of the Controller, including by deletion or returning of personal data according to section 7.2 above. This DPA shall thereafter cease to apply.

6.4 Sections which by their nature apply after the termination of this DPA and the following sections shall also apply after the termination of this DPA, such as but not limited to sections 4 (Confidentiality and disclosure of information), 6 (Liability), 8 (Amendments), 9 (Miscellaneous) and 10 (Governing Law and Dispute resolution).

7. Amendments

7.1 If the Data Protection Rules are changed so that this DPA does not meet the requirements for a data processing agreement pursuant to the GDPR, either party shall be entitled to request changes to this DPA in order to meet such new, changed or clarified requirements.

7.2 The Processor shall have the right to propose a new version of the DPA from time to time by notifying the Controller.

7.3 Changes in accordance with section 8.1 or 8.2 above shall enter into effect no later than thirty (30) days after a party's amendment notification, unless the other party has objected to such proposed change or new version of the DPA. If a party makes such an objection and the parties are unable to agree within a reasonable time, the Processor shall have the right to terminate the DPA and/or relevant parts of the Agreement in whole or in part with thirty (30) days' notice.

7.4 If the Processor would choose to adapt to the Controller's objection, the Processor shall be entitled to reasonable compensation from the Controller for the costs that the Processor incurs as a result of such adaptation.

8. Miscellaneous

8.1 The Processor is not entitled to any additional compensation for the processing of personal data in accordance with this DPA. However, the Processor is entitled to compensation in accordance with the Agreement for any work performed by the Processor in relation to personal data breaches or other measures that goes beyond the Processor's ordinary processing of personal data on behalf of the Controller.

8.2 In the event of deviating provisions between the Agreement and this DPA, the provisions of this DPA shall prevail with regard to processing of personal data and nothing in the Agreement shall be deemed to restrict or modify obligations set out in this DPA, to the extent that this results in the Controller not complying with the requirements of the Data Protection Rules, and notwithstanding anything to the contrary in the Agreement.

8.3 This DPA supersedes and replaces any eventual prior existing data processing agreements between the parties.

8.4 If a party assigns the Agreement (according to the terms of the Agreement), this DPA shall also be deemed assigned to the assignee of the Agreement. However, this DPA may still apply between the original parties. No party shall assign this DPA separately from the Agreement.

9. Governing Law and Dispute Resolution

9.1 Swedish law, without regard to its choice of law provisions, shall under all circumstances apply to this DPA. Any disputes arising out of or in connection with this DPA shall be resolved in accordance with the dispute settlement provision of the Agreement.

Appendix A – instructions on processing of personal data

Handling of personal data:

Purposes	● To manage user access within the platform ● To manage permissions within the platform ● To enrich deliverables within the platform (e.g. improve credibility of an asset by specifying contact details) ● To support users within the platform ● To improve quality within the platform ● To troubleshoot within the platform
Types of personal data	● Name ● Email ● (Possibly others, if specified in free-text fields, but not mandated or explicitly encouraged by the software)
Categories of data subjects	● Users operating the software within the scope of a customer account, partner account or supplier account
Retention time	● For the duration necessary to fulfill the purposes for which it was collected (i.e. if a user is created within the software, their data will be retained for as long as they remain a user). All personal data will be removed at latest when the Agreement is terminated.
Processing operations	● Storing ● Erasing

Information security measures:

Access control	● Access to customer data is restricted to authorized personnel only. ● Access permissions are granted based on the principle of least privilege, ensuring that individuals have access only to the data necessary for their roles. ● Access to customer data is logged and monitored for security purposes. ● Login and subsequent access of personal data is protected behind MFA login procedures
Back-up	● Snapshot backup every 4 hours
Logging of access to personal data	● As EandoX is a single-tenant solution, every customer account has their own repository for personal data. Access to data is

	provided on a need-to-know basis for bug resolution and incident handling purposes only
Authorisation and permissions	● Access permissions are granted based on the principle of least privilege, ensuring that individuals have access only to the data necessary for their roles.
Encryption of data communication	● All customer data is encrypted both in transit and at rest using industry-standard encryption algorithms. ● Encryption keys are securely managed and rotated periodically to mitigate the risk of unauthorized access.
Firewalls, separation of environments and antivirus protection	● As EandoX is a single-tenant solution, every customer account is its own environment separated from other entities on the platform ● Continuous monitoring and threat detection mechanisms are implemented to identify and respond to security incidents promptly ● Incident response procedures are documented and regularly tested to ensure readiness in the event of a security breach ● EandoX relies on security measures provided by external database providers (e.g. AWS)

Appendix B – Sub-processors

The following Sub-processors are engaged by the Processor to perform parts of the processing assignment at the time of the conclusion of the DPA.

Company name	Company organisation number (or similar)	Geographical location	Task in the services	If personal data is transferred outside of EU/EEA - Mechanism for transfer to third country	Comments
Mouseflow ApS	CVR: 32837330	*Denmark (EU)*	*Troubleshooting, Quality assurance, Analytics*	*N/A (Inside EU)*	
Amazon Web Services (AWS)	*B186284 (Luxembourg)*	*Frankfurt, Stockholm*	*Cloud Infrastructure & Hosting*	*N/A (Inside EU) (On the rare occasion any personal data should be accessed from USA, the transfer would be based on the EU-US Data Privacy Framework)*	
Google	*IE 6388047V*	*Ireland (HQ) / Global*	*Cloud Services / Analytics / Workspace*	*EU-US Data Privacy Framework (DPF)*	
Mongodb	*06663503 (UK)*	*Dublin*	*Database management*	*EU-US Data Privacy Framework (DPF)*	
Hubspot	*505777*	*Ireland / USA*	*CRM & Marketing Automation*	*EU-US Data Privacy Framework (DPF)*	
OneTrust	*10462551 (UK)*	*UK / USA*	*Privacy Management / Cookie Consent*	*Adequacy decision / EU-US Data Privacy Framework (DPF)*	