GREENBYTE DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") supplements the Greenbyte Master Services Agreement and the Greenbyte General Terms and Conditions.

By entering into the Agreement, on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, on behalf of its Affiliates, the Customer acknowledges and accepts the terms and conditions set forth in this DPA and its incorporation into the Agreement.

This version of the DPA was published on 30 March 2020.

All capitalized terms not defined herein shall have the same meaning as defined in the Agreement.

1 DEFINITIONS

"Agreement" shall have the meaning ascribed to it in the Master Services Agreement or the Trial Services Agreement as entered into by the Customer and Greenbyte.

"Controller" means the entity which determines the purposes and means of the processing of Personal Data.

"Customer Personal Data" means any Personal Data processed by the Processor or a Subprocessor on Controller's behalf pursuant to or in connection with the Services.

"Data Protection Laws and Regulations" means the laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, and the United States of America, which are applicable to the processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Customer Personal Data relates.

"EEA" means the European Economic Area.

"EU" means the European Union.

"EU Data Protection Laws" means the GDPR and laws implementing or supplementing the GDPR.

"GDPR" means EU General Data Protection Regulation 2016/679.

"Data Transfer" means:

(a) a transfer of Customer Personal Data from the Controller to a Processor or a Subprocessor; or

(b) an onward transfer of Customer Personal Data from a Processor to a Subprocessor, or between two establishments of a Processor.

"Personal Data" means any information relating to an identifiable person who can be directly or indirectly identified in particular with reference to a personal identifier. Examples of personal identifiers collected within the Services include, but are not limited to, first name and last name, title, phone number, mobile number, email address and location information.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

"Processor" means the entity which processes Customer Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the contractual clauses issued by the European Commission by the decision 2010/87/EU for international transfers of Personal Data, or any subsequent legal instrument permitting the lawful transfer of Personal Data to international organizations and countries not part of the EEA or EU.

"Subprocessor" means any person or entity appointed by or on behalf of the Processor to process Customer Personal Data on behalf of Controller in connection with the Agreement.

2 HOW THIS DPA APPLIES

The terms of Part I of this DPA shall apply to all Customers.

For Customers within the EEA or EU or Customers of the Swedish corporation Greenbyte AB, the terms of Part II of this DPA shall apply in addition to the terms of Part I.

PART I

---

3 PROCESSING OF PERSONAL DATA

3.1 Role of the Parties

The Parties acknowledge and agree that with regard to the processing of Customer Personal Data, Customer is the Controller, Greenbyte is the Processor, and that Greenbyte or its Affiliates may engage Subprocessors in accordance with the GDPR provisions.

3.2 Protection of Customer Data and Customer Personal Data

Processor shall maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Personal Data, to include, but not be limited to:

(a) encryption of Personal Data;

(b) restoration of availability and access to Personal Data in a timely manner in the event of a Personal Data Breach or other unexpected event interrupting Processor's processing of Customer Personal Data; and

(c) regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing.

In the event the Customer Data or Customer Personal Data require protections under specific law, regulations, rules, or orders applicable to Customer, or under specific contractual obligations owed by Customer to third parties, it shall be the Customer's responsibility to timely inform Greenbyte of such additional specific requirements prior to Processor's processing of such Customer Data or Customer Personal Data. Such additional requirements shall be addressed by the Parties in a separate SoW (defined in the Agreement) pursuant to the Agreement and subject to such fees as agreed by the Parties in writing.

3.3 Refusal to Process Data

The Processor is entitled to refuse further processing of Customer Personal Data on behalf of the Controller if the Processor regards that such continued data processing would be in violation of applicable laws. The change in the Processor's performance of its obligations under the Agreement as such refusal would mean, shall not give the Controller the right to claim deficiency in the Processor's performance under the Agreement.

4 CONTROLLER DATA INCIDENT MANAGEMENT AND NOTIFICATION

4.1 Incident Response

Processor shall notify Controller without undue delay upon Processor becoming aware of an actual Personal Data Breach affecting Customer Personal Data, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects or relevant regulators of the Personal Data Breach as required by applicable law, such notification to contain at least the following:

(a) a description of the nature of the Personal Data Breach including the categories and approximate number of Data Subjects concerned, and the categories and approximate number of data records concerned;

(b) the name and contact details of the person responsible for Processor's data protection matters;

(c) a description of likely consequences and/or realized consequences of the Personal Data Breach; and

(d) a description of the measures taken to address the Personal Data Breach and to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases.

4.2 Investigation of Breach

Processor shall cooperate with Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

5 LIMITATION OF LIABILITY

5.1 Limitation of Liability

Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and the DPA.

5.2 Total Liability

For the avoidance of doubt, Processor's and its Affiliates' total liability for all claims from the Controller and all of its Affiliates arising out of or related to the Agreement and the DPA shall apply in the aggregate for all claims under both the Agreement and the DPA, including by Controller and its Affiliates, and, in particular, shall not be understood to apply individually and severally to Controller and/or to any Affiliate that is a contractual party to the DPA.

5.3 Indemnity

In case of a claim from any Data Subject directly against the Processor or any of its Affiliates or Subprocessors, the Controller shall indemnify and hold harmless the

Processor and its Affiliates and Subprocessors for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that the Processor has notified the Controller about the claim and given the Controller the opportunity to cooperate with the Processor in the defence and settlement of the claim. Subject to the terms of the Agreement, the Controller may claim from the Processor amounts paid to a Data Subject or for a violation of applicable laws caused by the Processor's or any of its Affiliates or Subprocessors breach of its obligations under this DPA.

5.4 Compensation

In addition to what is otherwise stated in this DPA or in the Agreement, the Processor is entitled to receive reasonable compensation for:

(a) the work and additional costs incurred by the Controller's amendment of its instructions regarding the Processor's processing of Customer Personal Data on behalf of the Controller;

(b) the work and additional costs arising from the supervision of a supervisory authority or similar measures;

(c) the work and additional costs inflicted upon the Processor due to violation of the Controller of its obligations hereunder;

(d) the work and additional costs incurred by the Processor when the Processor assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

6 DELETION OR RETURN OF PERSONAL DATA

6.1 Deletion of Personal Data

Subject to this Section 6, Processor shall promptly in accordance with the Controller's instructions and at the expense of the Controller, return or delete and procure the deletion of all copies of Customer Personal Data within thirty (30) business days of the date of termination of the Services involving the processing of Customer Personal Data, unless Customer Personal Data storage is required under law. However, the above requirements for deletion do not apply to deletion of backups, which occurs in accordance with the Processor's current backup routine, provided such routines are in accordance with industry standards.

6.2 Certification of Deletion

Processor shall provide written certification to Controller that it has fully complied with this Section 6.

7 GENERAL TERMS

7.1 Confidentiality

Each Party must keep any information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law; or

(b) the relevant information is already in the public domain.

Nothing herein obligates Processor to disclose information and reports about internal investigations, operations, and audits that may contain confidential information, trade secrets, or privileged information of Processor or Processor's other customers.

7.2 Amendments

Greenbyte shall be entitled to amend this DPA from time to time by notifying the Customer via e-mail at least one hundred twenty (120) days prior to such change coming into effect. In the event that an amendment is not acceptable to the Customer, the Customer shall be entitled to terminate this DPA effective from the date the amendment comes into effect by giving written notice to Greenbyte within thirty (30) days from receiving the notice of the amendment from Greenbyte. If the Customer exercises its right to terminate this DPA, Greenbyte shall be entitled to suspend or terminate the Services affected by termination of this DPA without incurring any liability or obligation to refund any advance payments made by Customer. Where the DPA is not terminated by Customer within the aforementioned time, Customer shall be deemed to have accepted the amendment.

7.3 Notices

All notices and communications given under this DPA must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Agreement. Processor shall be notified by email sent to the address: privacy@greenbyte.com.

7.4 Order of Precedence

This DPA is governed by the terms of conditions of the Agreement. In the event of a conflict between this DPA and the Agreement, the DPA shall prevail, and Section II shall prevail over Section I.

7.5 Governing Law and Jurisdiction

All disputes or controversies arising from the terms and conditions of this DPA shall be governed by Section 17 of the Agreement.

PART II

---

8 PROCESSING OF PERSONAL DATA

8.1 Disclosure of Personal Data

Customer shall, in its use of the Services, disclose Customer Personal Data in accordance with the requirements of Data Protection Laws and Regulations. The Controller shall provide up to date and accurate information about the Customer Personal Data processed by the Processor on behalf of the Controller. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which they acquired the Customer Personal Data and ensure that the Customer does not provide or enable the provision of other Personal Data than set out herein for processing by the Processor. The Controller undertakes to ensure that the Users and other Data Subjects receive information about how their Personal Data is processed by the Processor.

8.2 Instructions

The Controller is required to provide clear and documented instructions to the Processor regarding the processing of Customer Personal Data by the Processor. The Controller's instructions to the Processor as of the date hereof are set out below. The Data Controller has the right and obligation to adjust its instructions to ensure their correctness and provide modified or supplementary instructions to the Processor when required. The Controller shall clearly and in advance inform the Processor in writing of any such changes. The Controller is responsible for ensuring that the instructions provided by the Controller to the Processor are in accordance and compliance with the requirements of the Data Protection Laws and Regulations.

8.3 Purpose of Processing Personal Data

Processor shall treat Personal Data as Confidential Information and shall only process Customer Personal Data on behalf of and in accordance with Controller's documented instructions for the following purposes:

(a) processing in accordance with the Agreement;

(b) processing initiated by Users in their use of the Services; and

(c) processing to comply with other documented reasonable instructions provided by Controller where such instructions are consistent with the terms of this DPA and the Agreement.

In the event that the Processor processes Customer Personal Data in addition to or in violation of the Controller's instructions, due to being required to do so by Data Protection Laws and Regulations to which the Processor is subject, then the Processor shall inform the Controller of that legal requirement before processing, unless such law or regulation prohibits such information on important grounds of public interest.

8.4 **Subject Matter**

The subject-matter of processing of Customer Personal Data by Processor is the performance of the Services pursuant to the Agreement.

8.5 **Term**

Processor will process Customer Personal Data for the duration of the Agreement and as long as required to fulfill its obligations hereunder, unless otherwise agreed in writing.

8.6 **Data Subject Categories**

Customer Personal Data submitted by the Controller or its Users may relate to the following categories of Data Subjects:

(a) Customers, business partners, and vendors of Customer (who are natural persons);

(b) Employees, agents, advisors, and freelancers of Customer (who are natural persons);

(c) Customer's Users authorized by Customer to use the Services.

8.7 **Categories of Personal Data**

The Data Subjects and Users may submit Customer Personal Data to the Services, the extent of which is determined and controlled by the User in its sole discretion, and which may include the following categories of Customer Personal Data:

(a) First and last name

(b) Position

(c) Employer

(d) Contact information (company, email, phone, physical business address)

(e) Usage information

(f) Cookies data

9 PROCESSOR AND SUBPROCESSOR PERSONNEL

9.1 Personnel Confidentiality

Processor shall take reasonable steps to ensure the reliability of any employee, agent, or contractor of any Subprocessor who may have access to Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with the Applicable Laws in the context of that individual's duties to the Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

10 SUBPROCESSING

10.1 Controller Consent to Subprocessors

Controller acknowledges and agrees that:

(a) Processor's Affiliates may be retained as Subprocessors; and

(b) Processor and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services only if Processor or its Affiliate(s) have previously entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor.

10.2 Subprocessor List Access

Processor shall make the list of Subprocessors for the Services available to the Controller upon request.

10.3 Processor Notification

Processor shall notify the Controller if it engages a Subprocessor to process the Customer Personal Data. Controller may object to Processor's engagement of a new Subprocessor by notifying Processor promptly in writing within ten (10) business days after receipt of Processor's notice. In the event Controller objects to a new Subprocessor, as permitted in the preceding sentence, Processor will use reasonable

efforts to make available to Controller a change in the Services or recommend a commercially reasonable change to Controller's configuration or use of the Services to avoid processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening the Controller.

10.4 **Termination**

If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Controller may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Processor without the use of the objected-to new Subprocessor by providing written notice to Processor.

10.5 **Processor Liability for Subprocessor Actions**

Processor shall be liable for the acts and omissions of its Subprocessors to the same extent Processor would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

11 RIGHTS OF DATA SUBJECTS

11.1 **Data Subject Request Notifications**

Processor shall, to the extent legally permitted, promptly notify Controller if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request".

11.2 **Assistance by Processor**

Taking into account the nature of the processing, Processor shall assist Controller by taking appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

11.3 **Commercially Reasonable Response Efforts**

To the extent Controller, in its use of the Services, does not have the ability to address a Data Subject Request, Processor shall, upon Controller's request, provide commercially reasonable efforts to assist Controller in responding to such Data Subject Request, to the extent Processor is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Controller shall be responsible for any costs arising from Processor's provision of such assistance.

12 SECURITY AND RECORD

12.1 Security Measures

Processor shall maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Personal Data, to include, but not be limited to:

(a) encryption of Personal Data;

(b) restoration of availability and access to Personal Data in a timely manner in the event of a Personal Data Breach or other unexpected event interrupting Processor's processing of Customer Personal Data; and

(c) regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing.

12.2 Record

The Processor shall maintain a record in an electronic form ("Record") of all Customer Personal Data processing carried out under this DPA and the Agreement on behalf of the Controller, containing at least:

(a) the name and contact details of the Processor;

(b) the categories of processing carried out on behalf of the Controller;

(c) information on any transfers of Customer Personal Data outside of the EU/EEA made in accordance with this DPA and the documentation of appropriate safeguards implements;

(d) a description of the technical and organizational security measures taken in accordance with this Section 12;

(e) a list of Subprocessors used for Customer Personal Data processing; and

(f) a report of any known audits performed by Processor or a third party, which shall include information on execution of this DPA and requests of the relevant supervisory authority and the Data Subjects and the measures taken on the basis of those requests.

12.3 Reporting Obligation

Processor shall provide Controller with the Record without undue delay but no later than 5 (five) business days from the Controller's request.

13 DATA PROTECTION IMPACT ASSESSMENT

13.1 Assessment

Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with competent data privacy authorities, which Controller reasonably considers to be required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law and Regulation, in each case solely in relation to processing of Customer Personal Data by, and taking into account the nature of the processing and information available to, the Processor and Subprocessors.

14 AUDIT RIGHTS

14.1 Compliance with Audit Requests

Subject to this Section 14, Processor shall make all information necessary to demonstrate compliance with this DPA available to Controller by request and at Controller's expense, and shall allow for and contribute to audits and inspections by Controller or any auditor mandated by Controller in relation to the processing of the Customer Personal Data by the Subprocessors. All audits initiated by Controller shall be at its expense.

14.2 Occurrence of Audit

Information and audit rights of Controller only arise under Section 14.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws and Regulations.

15 DATA TRANSFER

15.1 Data Transfer

Processor shall ensure that no Customer Personal Data is transferred, released, assigned, disclosed, or otherwise made available to any third party without Controller's specific prior written consent or acknowledgement under the Agreement.

15.2 Transfers Outside the EU/EEA

Processor may not transfer or authorize the transfer of Customer Personal Data to countries outside the EU and/or the EEA without the prior written consent of the Controller. If Customer Personal Data processed under this DPA is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that the

Customer Personal Data is adequately protected. To achieve this, the Parties shall rely on EU approved Standard Contractual Clauses for the transfer of Personal Data.