Last modified: May 22, 2018

Data Processing Agreement

The Customer agreeing to these terms ("**Customer**") and Fastpool Sweden AB (as applicable, "**Fastpool**") have entered into an Agreement about providing a Service (**"Agreement"**). This Data Processing Agreement (**"DPA"**) reflects the parties agreement with respect to the terms governing the processing and security of Customer Data under the applicable Agreement.

1. **Definitions**.

1.1. Capitalized terms used but not defined in this DPA have the meanings given in Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 ("GDPR"). In this Agreement, unless stated otherwise:

"**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR.

"**Customer Data**" means data submitted, stored, sent or received via the Service by Customer and its End Users.

"**Customer Personal Data**" means personal data contained within the Customer Data.

"**Data Incident**" means a breach of Fastpool's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Fastpool. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016.

"**Model Contract Clauses**" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

"**Non-European Data Protection Legislation**" means data protection or privacy legislation other than the European Data Protection Legislation.

"**Notification Email Address**" means the email address(es) designated by Customer to receive certain notifications from Fastpool.

"**Security Measures**" has the meaning given in Section 6.1.1 (Fastpool's Security Measures).

"**Service**" means the following services, as applicable: Fastpool.

"**Subprocessors**" means third parties authorized under this Agreement to have logical access to and process Customer Data in order to provide parts of the Service and related technical support.

1.2. The terms “personal data”, “data subject”, “processing”, “controller”, “processor” and “supervisory authority” as used in this Agreement have the meanings given in the GDPR, and the terms “data importer” and “data exporter” have the meanings given in the Model Contract Clauses, in each case irrespective of whether GDPR (European Data Protection Legislation) or Non-European Data Protection Legislation applies.

2. Duration of Data Processing Agreement.

2.1. This DPA will take effect on the May 25 2018 and remain in effect until, and automatically expire upon, deletion of all Customer Data by Fastpool as described in this DPA.

3. Scope of Data Protection Legislation.

3.1. Application of European Legislation (GDPR). The parties acknowledge and agree that GDPR (the European Data Protection Legislation) will apply to the processing of Customer Personal Data if, for example the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA and/or the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering them services in the EEA.

3.2. Application of Non-European Legislation. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

3.3. Application of Data Processing Agreement. Except to the extent this Agreement states otherwise, the terms of this Agreement will apply irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies to the processing of Customer Personal Data.

4. Processing of Data.

4.1. Roles and Regulatory Compliance; Authorization.

- 4.1.1. Processor and Controller Responsibilities. The parties acknowledge and agree that:
  - 4.1.1.1. the subject matter and details of the processing are described in Appendix 1;
  - 4.1.1.2. Fastpool is a processor of that Customer Personal Data under GDPR;
  - 4.1.1.3. Customer is a controller or processor, as applicable, of that Customer Personal Data under GDPR;
  - 4.1.1.4. each party will comply with the obligations applicable to it under the GDPR with respect to the processing of that Customer Personal Data.
- 4.1.2. Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party’s processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

4.2. Scope of Processing.

- 4.2.1. Customer’s Instructions. By entering into this Agreement, Customer instructs Fastpool to process Customer Personal Data only in accordance with applicable law:
  - 4.2.1.1. to provide the Service and related technical support;

4.2.1.2. as further specified via Customer's use of the Service and related technical support;

4.2.1.3. as further documented in any other written instructions given by Customer and acknowledged by Fastpool as constituting instructions for purposes of this Data Processing Agreement.

4.2.2. Fastpool's Compliance with Instructions. As from the Full Activation Date, Fastpool will comply with the instructions described in Section 4.2.1 (Customer's Instructions)

5. **Data Deletion**.

5.1. Deletion During Term. Fastpool will enable Customer and/or End Users to delete Customer Data during the applicable term in a manner consistent with the functionality of the Service. If Customer or an End User uses the Service to delete any Customer Data and the Customer Data cannot be recovered by Customer or an End User, this use will constitute an instruction to Fastpool to delete the relevant Customer Data from Fastpool's systems in accordance with applicable law. Fastpool will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

5.2. Deletion on Term Expiry. Subject to Section 5.3 (Deferred Deletion Instruction), on expiry of the applicable Term Customer instructs Fastpool to delete all Customer Data (including existing copies) from Fastpool's systems in accordance with applicable law. Fastpool will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 7.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain afterwards.

5.3. Deferred Deletion Instruction. To the extent any Customer Data covered by the deletion instruction described in Section 5.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 5.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Agreement will continue to apply to such Customer Data until its deletion by Fastpool.

6. **Data Security**.

6.1. Fastpool's Security Measures, Controls and Assistance.

6.1.1. Fastpool's Security Measures. Fastpool will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Fastpool's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Fastpool may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service.

6.1.2. Security Compliance by Fastpool Staff. Fastpool will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.2. Data Incidents.

6.2.1. Incident Notification. If Fastpool becomes aware of a Data Incident, Fastpool will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

6.2.2. Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Fastpool recommends Customer take to address the Data Incident.

6.2.3. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Fastpool's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

6.2.4. No Assessment of Customer Data by Fastpool. Fastpool will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

6.2.5. No Acknowledgment of Fault by Fastpool. Fastpool's notification of or response to a Data Incident under this Section 6.2 (Data Incidents) will not be construed as an acknowledgement by Fastpool of any fault or liability with respect to the Data Incident.

6.3. Customer's Security Responsibilities and Assessment.

6.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Fastpool's obligations under Section 6.1 (Fastpool's Security Measures, Controls and Assistance) and Section 6.2 (Data Incidents):

6.3.1.1. Customer is solely responsible for its use of the Services, including:

6.3.1.1.1. making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;

6.3.1.1.2. securing the account authentication credentials, systems and devices Customer uses to access the Services;

6.3.1.2. Fastpool has no obligation to protect Customer Data that Customer elects to store or transfer outside of Fastpool's and its Subprocessors' systems (for example, offline or on-premise storage).

7. **Data Subject Rights, Data Export**.

7.1. Access; Rectification; Restricted Processing; Portability. During the applicable term, Fastpool will, in a manner consistent with the functionality of the Service, enable Customer to access, rectify and

restrict processing of Customer Data, including via the deletion functionality provided by Fastpool as described in Section 5.1 (Deletion During Term), and to export Customer Data.

7.2. Data Subject Requests.

7.2.1. Customer's Responsibility for Requests. During the applicable Term, if Fastpool receives any request from a data subject in relation to Customer Personal Data, Fastpool will advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

7.2.2. Fastpool's Data Subject Request Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) Fastpool will assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in Section 7.1 (Access; Rectification; Restricted Processing; Portability) and Section 7.2.1 (Customer's Responsibility for Requests).

8. **Data Transfers**.

8.1. Data Storage and Processing Facilities. Customer agrees that Fastpool may, subject to Section 8.2 (Transfers of Data Out of the EEA), store and process Customer Data in any country in which Fastpool or any of its Subprocessors maintains facilities.

8.2. Transfers of Data Out of the EEA. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA and GDPR applies to the transfers of such data ("Transferred Personal Data"), Fastpool will:

8.2.1. ensure that Fastpool as the data importer of the Transferred Personal Data enters into Model Contract Clauses as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or

8.2.2. offer an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

8.3. Data Center Information. Information about the locations of Fastpool data centers is available at Fastpool GDPR information page (as may be updated by Fastpool from time to time).

8.4. Disclosure of Confidential Information Containing Personal Data. If Customer has entered into Model Contract Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), Fastpool will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

9. **Subprocessors**.

9.1. Consent to Subprocessor Engagement. Customer generally authorizes the engagement of any other third parties as Subprocessors ("Third Party Subprocessors"). If Customer has entered into Model Contract Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Fastpool of the processing of Customer Data if such consent is required under the Model Contract Clauses.

9.2. Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at Fastpool GDPR information page (as may be updated by Fastpool from time to time in accordance with this DPA).

9.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Fastpool will:

9.3.1. ensure via a written contract that:

9.3.1.1. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this DPA) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Fastpool as described in Section 8.2 (Transfers of Data Out of the EEA); and

9.3.1.2. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Agreement, are imposed on the Subprocessor; and

9.3.2. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

9.4. Opportunity to Object to Subprocessor Changes.

9.4.1. When any new Third Party Subprocessor is engaged during the applicable Term, Fastpool will, at least 30 days before the new Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

9.4.2. Customer may object to any new Third Party Subprocessor by terminating the applicable Agreement immediately upon written notice to Fastpool, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 9.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

10. **Processing Records**.

10.1. Customer acknowledges that Fastpool is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Fastpool is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Fastpool means provided by Fastpool, and will ensure that all information provided is kept accurate and up-to-date.

11. **Liability**.

11.1. This DPA will not affect applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

12. **Effect of Amendment**.

12.1. To the extent of any conflict or inconsistency between the terms of this DPA and the remainder of the applicable Agreement, the terms of this DPA will govern. Subject to the amendments in this DPA, such Agreement remains in full force and effect. For clarity, if Customer has entered more than one Agreement, this DPA will amend each of the Agreements separately.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter
Fastpool's provision of the Service and related technical support to Customer.
Duration of the Processing
The applicable term plus the period from expiry of such term until deletion of all Customer Data by Fastpool in accordance with the Agreement.
Nature and Purpose of the Processing
Fastpool will process Customer Personal Data submitted, stored, sent or received by Customer, or End Users via the Service for the purposes of providing the Service and related technical support to Customer in accordance with the Agreement.
Categories of Data
Personal data submitted, stored, sent or received by Customer and/or End Users via the Service may include the following categories of data: user IDs, email, addresses, phone numbers, images, calendar entries and other data.
Data Subjects
Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; and any other person who transmits data via the Service, including individuals collaborating and communicating with Customer.

Appendix 2: Security Measures

Fastpool will implement and maintain the Security Measures set out in this Appendix 2 to the Agreement. Fastpool may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. Data Center & Network Security.
    1.1. Data Centers.
        1.1.1. Infrastructure. Fastpool stores all production data in secure data centers (Digital Ocean at this moment), geographically distributed if need.
        1.1.2. Server Operating Systems. Fastpool servers use a Linux based Operating Systems (Debian).
    1.2. Networks & Transmission.
        1.2.1. Data Transmission. Fastpool transfers data via Internet standard protocols.
        1.2.2. Incident Response. Fastpool monitors a variety application points and communication channels for security incidents, and Fastpool's personnel will react promptly to known incidents.

1.2.3. Encryption Technologies. Fastpool uses HTTPS encryption (also referred to as SSL or TLS connection).

2. Access and Site Controls.
   2.1. Access Control.
      2.1.1. Infrastructure Security Personnel. Fastpool has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel.
      2.1.2. Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Service. The Service checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.
      2.1.3. Internal Data Access Policy. Fastpool's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Fastpool aims to design its services to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. Fastpool employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Fastpool requires the use of unique user IDs and strong passwords to minimize the potential for unauthorized account use. Access to Service is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

3. Personnel Security.
   3.1. Fastpool personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Fastpool conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
   3.2. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Fastpool's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Fastpool's personnel will not process Customer Data without authorization.

4. Subprocessor Security.
   4.1. Before onboarding Subprocessors, Fastpool conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Fastpool has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 9.3 (Requirements for Subprocessor

Engagement) of this Agreement, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.