FASTCOMET

Managed Cloud Hosting

Customer GDPR Data Processing Agreement

Version October 2022

This Customer Data Processing Agreement reflects the requirements of the European Data Protection Regulation ("GDPR") as it comes into effect on May 25, 2018. FastComet's products and services offered in the European Union are GDPR ready, and this DPA provides you with the necessary documentation of this readiness.

This Data Processing Agreement ("DPA") is an addendum to the Customer Terms of Service https://www.fastcomet.com/terms ("Agreement"), Privacy Policy (https://www.fastcomet.com/terms/privacy-policy) or other written or electronic agreement between FastComet Inc. ("FastComet") and Client hereafter named the "Customer" for the purchase of Web Hosting services from FastComet (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. The customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorized Affiliates (defined below).

This DPA includes:

- Standard Contractual Clauses
- List of Sub-Processors attached hereto as Annex A.
- FastComet Statement on Security attached hereto as Annex B.

1. Data Processing Terms

1.1 Definitions. For the purposes of this Addendum, the following definitions apply and shall prevail as to any conflict with definitions under the Agreement:

"**Affiliates**" means any entity which is controlled by, controls or is in common control with FastComet.
"**Applicable Data Protection Law**" means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms "process", "processes" and "processed" will be construed accordingly.
"**Covered Services**" any hosted services we offer you that could involve our Processing of Personal Data.
"**Customer**" means the Customer that has executed the FastComet Web Hosting Order.

"**Customer Data**" means what is defined in the Agreement as "Customer Data" or "Your Data." "Customer Data" means the Personal Data of any Data Subject Processed by FastComet within the FastComet Infrastructure on behalf of Customer pursuant to or in connection with the Terms of Service.
"**Data Controller**" means the Customer, as the entity which determines the purposes and means of the Processing of Personal Data.
"**Data Processor**" means FastComet, as the entity which Processes Personal Data on behalf of the Data Controller.
"**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.
"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.
"**End-users**" means Customer's own customers and Affiliates whose Personal Data is Processed by FastComet through the provision to, or use by, the Customer of the Services.
"**EU Data Protection Law**" means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (in each case, as may be amended, superseded or replaced).
"**GDPR**" means the General Data Protection Regulation (EU) 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).
"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), where for each (i) or (ii), such data is Customer Data.
"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"**Processing**" means any operation or set of operations which is performed upon

Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.
"**Services**" means any product or service provided by FastComet to Customer pursuant to and as more particularly described in the Agreement.
"**Sub-processor**" means any Processor engaged by FastComet or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or any FastComet Affiliate.
"**Technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Scope and Applicability of this DPA

If Customer entering into this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the FastComet entity that is party to the Agreement is party to this DPA.

If Customer's Affiliate entering into this DPA has executed an Order with FastComet or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order and applicable renewal Orders, and the FastComet entity that is party to such Order is party to this DPA.

3. Processing of Personal Data and Parties Obligations

3.1 Scope of Processing. This DPA applies where and only to the extent that FastComet processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

Personal data may be processed for the following purposes: (a) to provide the Web

Hosting Service (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the FastComet End-User Terms of Services, Privacy Policy and Service Level Agreement.

3.2 Roles of the Parties. The parties agree that, in respect to any Processing of Customer Personal Data through the provision or use of the Services: Customer may be either of the following (i) a Controller of Customer Personal Data, or (ii) a Processor when it Processes Customer Personal Data on behalf of its End-users. Consequently, FastComet is a Processor where Customer is Controller or Processor, a sub-processor when Customer is acting as a Processor on behalf of its End-users.

3.3 FastComet Processing of Personal Data. As a Processor, FastComet shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order(s); (ii) Processing initiated by Users in their use of the Web Hosting Services; and (iii) Processing to comply with other reasonable instructions provided by Customer to the extent they are consistent with the terms of this Agreement and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to FastComet in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and FastComet.

3.4 Customer's Processing of Personal Data. Customer shall, in its provision of the FastComet Web Hosting Services, comply with their respective obligations under the GDPR, to the extent applicable to the Processing of any User Personal Data in the context of the provision of the FastComet Services. Customer shall (i) comply with all applicable privacy and data protection laws with respect to Customer's Processing of User Personal Data and any Processing instructions that Customer issues to FastComet, and (ii) ensure that Customer has obtained (or shall obtain) all consents and rights under Data Protection Laws for FastComet to process Personal Data and provide the Services pursuant to the Agreement and this DPA. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including but not limited to the proper notice and consent required for such Personal Data.

3.5 Details of the Processing. The subject matter of processing of Customer Data by FastComet is the performance of the Covered Services pursuant to the Terms of Service and product-specific agreements. FastComet shall only Process Customer Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Terms of Service or

applicable product-specific agreement; (ii) Processing initiated by end users in their use of the Covered Services; (iii) Processing to comply with other documented, reasonable instructions provided by Customers (ex. via email) where such instructions are consistent with the terms of the Agreement. FastComet shall not be required to comply with or observe Customer's instructions if such instructions would violate the GDPR or any other applicable data privacy laws.

FastComet will Process Personal Data during the effective date of the Terms of Service, but will abide by the terms of this Addendum for the duration of the Processing if in excess of that term, and unless otherwise agreed upon in writing.

3.6 Compliance with Laws. Each party shall comply with all laws, rules and regulations applicable to it and bind on it in the performance of this Addendum, including all statutory requirements relating to data protection.

3.7 Access or Use. FastComet will only Process User Personal Data on behalf of and in accordance with the Customer's prior written instructions and for no other purpose. FastComet is hereby instructed to Process User Personal Data to the extent necessary to enable FastComet to provide the FastComet Service Offerings in accordance with the Agreement.

3.8 Nature of the Data. FastComet handles Customer Data provided by Customer. Such Customer Data may contain special categories of data depending on how the Services are used by Customer. The Customer Data may be subject to the following process activities: (i) storage and other processing necessary to provide, maintain and improve the Services provided to Customer; (ii) to provide customer and technical support to Customer; and (iii) disclosures as required by law or otherwise set forth in the Agreement.

3.9 FastComet Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that FastComet shall have a right to use and disclose data relating to and/or obtained in connection with the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, FastComet is the Controller of such data and accordingly shall process such data in compliance with Data Protection Laws.

3.10 Customer Controls. The Service Offerings provide Customer with controls to enable Customer to retrieve, correct, delete, or block Customer Data as described in the Documentation. FastComet makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for properly (a) configuring the Service Offerings, (b) using the controls available in connection

with the Service Offerings (including the security controls), and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Customer Data, which may include use of encryption technology to protect Customer Data from unauthorized access and routine archiving of Customer Data.

3.11 Categories of Data Subjects

Customer may upload Personal Data in the course of its use of the Covered Services, the extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Covered Services

3.12 Type of Personal Data. Customer may upload Personal Data in the course of its use of the Covered Services, the type of and extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data of Data Subjects:

- Name
- Address
- Telephone number
- Date of birth
- Email address
- Other data collected that could directly or indirectly identify you.

4. Subprocessing

4.1 Authorized Sub-processors. Customer agrees that FastComet may engage Sub-processors to process Personal Data on Customer's behalf. The Sub-processors currently engaged by FastComet and authorized by Customer are listed in Annex A.

4.2 Sub-processor Obligations. FastComet shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data

Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause FastComet to breach any of its obligations under this DPA.

4.3 Changes to Sub-processors. FastComet shall provide Customer reasonable advance notice (for which email shall suffice) if it adds or removes Sub-processors.

4.4 List of Current Sub-processors. FastComet shall make available to Customer the current list of Sub-processors for the Services identified in Annex 1 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("Infrastructure and Sub-processor Documentation").

4.5 Objection to Sub-processors. Customer may object in writing to FastComet's appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying FastComet promptly in writing within five (5) calendar days of receipt of FastComet's notice in accordance with Section 4.3. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If this is not possible, either party may terminate the applicable Services that cannot be provided by FastComet without the use of the objected-to-new Sub-processor.

5. Rights of Data Subjects

Data Subject Access Request ("SAR"). FastComet will grant Customer electronic access to Customer's Web Hosting Services environment that holds Personal Data to permit Customer to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). To the extent such electronic access is not available to Customer, FastComet will follow Customer's detailed written instructions to access, delete, release, correct or block access to Personal Data held in Customer's Web Hosting Services environment.

Customer agrees to pay FastComet's reasonable fees that may be associated with FastComet's performance of any such access, deletion, release, correction or blocking of access to Personal Data on behalf of Customer. FastComet will pass on to the Customer any requests of an individual Data Subject to access, delete, release, correct or block Personal Data Processed under the Agreement. FastComet will not be responsible for responding directly to the request, unless otherwise required by law.

6. Obligations of Processor

6.1 FastComet Personnel and Employees

Confidentiality. FastComet guarantees that its personnel engaged in the Processing of Personal Data are informed of the confidentiality obligations nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements (whether contractual or statutory). FastComet ensures that such confidentiality obligations survive the termination of the personnel engagement.
Reliability. FastComet takes commercially reasonable steps to ensure the reliability of any FastComet personnel engaged in the Processing of Personal Data.
Limitation of Access. FastComet ensures that FastComet's access to Personal Data is limited to that personnel performing Services in accordance with the Agreement. A subset of FastComet's employees has access to the products and services and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Access is enabled through "just in time" requests for access; all such requests shall be logged. Employees shall be granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.
Background checks. All new FastComet employees that have access to customer data undergo a 3rd party background check prior to being extended an employment offer, as local laws allow. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.
Data Protection Officer. FastComet Inc. has appointed a data protection officer. The appointed person may be reached at privacy@fastcomet.com

6.2 Security

Controls for the Protection of Customer Data. FastComet has implemented and maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Personal Data.

Such measures include, as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the 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; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. At a minimum, such measures shall include those set out in Annex 2 to this Addendum, Security Standards.

Confidentiality of Processing. FastComet shall ensure that any person who is authorized by FastComet to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that FastComet 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 Services purchased by the Customer.

7. Security Reports and Audits

Independent Determination. The customer is responsible for reviewing the information made available by FastComet relating to data security and its Security Standards and making an independent determination as to whether the Covered Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum. The information made available is intended to assist Customer in complying with Customer's obligations under applicable privacy laws, including the GDPR, in respect of data protection impact assessments and prior consultation.
Upon Client's written request, FastComet shall provide Client with the most recent certifications and/or summary audit report(s) concerning the security measures for the FastComet Cloud Hosting environment used to provide the Web Hosting Services.

Customer Audit Rights. Customer has the right to confirm FastComet's compliance with this Addendum as applicable to the Covered Services, including specifically FastComet's compliance with its Security Standards, by exercising a reasonable right to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by making a specific request of FastComet in writing to the address set forth in its Terms of Service. If FastComet declines to follow any instruction requested by Customer regarding a properly requested and scoped audit or inspection, Customer is entitled to terminate this Addendum and the Terms of Service. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. This Section will also apply insofar as FastComet carries out the control of Sub-processors on behalf of the Customer.

8. International Transfers

8.1 Processing Locations. FastComet stores and processes EU Data (defined below) in data centers located inside and outside the European Union. All other Customer Data may be transferred and processed in the United States and anywhere in the world where Customer, its Affiliates and/or its Sub-processors maintain data processing operations. FastComet shall implement appropriate safeguards to protect the Personal Data, wherever it is processed, in accordance with the requirements of Data Protection Laws.

8.2 FastComet shall not transfer any Customer Personal Data outside of the European Economic Area unless it has taken steps to ensure Transfer Protections, but subject to such Transfer Protections Customer agrees that Customer Personal Data may be Processed in countries where the Applicable FastComet Entity or its subprocessors maintain facilities or personnel as necessary so that FastComet may fulfill its obligations under the Agreement;

9. Personal Data Incident Management and Notification

9.1 Security Incident. FastComet evaluates and responds to any Personal Data Breach that creates suspicion of or indicates unauthorized access to or handling of Personal Data (“Incident”). FastComet Operations staff is instructed on responding to Incidents where processing of Personal Data may have been unauthorized, including prompt and reasonable internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence. Depending on the nature of the Incident, FastComet defines escalation paths and response teams to address the Incident.

If FastComet becomes aware of either (a) any unlawful access to any Customer Data stored on FastComet servers; or (b) any unauthorized access to FastComet facilities, where in either case such access results in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), FastComet will without undue delay: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

9.2 Failed Security Incidents. Customer agrees that:
(i) an unsuccessful Security Incident will not be subject to this Section. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of FastComet's facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) FastComet's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgment by FastComet of any fault or liability of FastComet with respect to the Security Incident.

9.3 Communication. Notification(s) of Security Incidents, if any, will be delivered to the Customer's account administrative emails. It is Customer's sole responsibility to ensure account owner maintains accurate contact information on the FastComet Client area and secure transmission at all times.

10. Obligation after the termination of personal data-processing services

FastComet shall enable Customer to retrieve and/or delete Customer Personal Data before any termination of the Agreement. Upon termination of the Agreement, FastComet will promptly initiate its purge process to delete or anonymize the Personal Data. If you request a copy of such Personal Data within 30 days of termination, FastComet will provide you with a copy of such Personal Data.

Customer instructs FastComet, after the end of the provision of the Services, to delete all Customer Personal Data in FastComet's possession or control, including existing copies thereof, but this requirement shall not apply to the extent FastComet is required by applicable law to retain all or some of the Customer Personal Data or to Customer Personal Data FastComet has archived on backup systems, which data FastComet shall securely isolate and protect from any further processing except to the extent required by such law until such time as the relevant back-up is destroyed in accordance with FastComet's standard backup destruction policies;

11. Legally Required Disclosures

FastComet will not disclose Customer Data to any government or any other third party, except as otherwise required to comply with the law or a valid and binding order of a law enforcement agency such as subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority (“Demand”) that it receives and which relates to the Processing of Personal Data. If a law enforcement agency sends FastComet a demand for Customer Data, FastComet will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, FastComet may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then FastComet will give Customer reasonable notice of the demand to allow Customer to seek a protective order or another appropriate remedy unless FastComet is legally prohibited from doing so. Customer acknowledges that FastComet has no responsibility to interact directly with the entity making the Demand.

12. Service Analyses

FastComet may (i) compile statistical and other information related to the performance, operation and use of the Cloud Services, and (ii) use data from the Web Hosting Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (collectively "Service Analyses"). FastComet may make Service Analyses publicly available. However, Service Analyses will not incorporate Customer's Content, Personal Data or Confidential Information in a form that could identify or serve to identify Customer or any Data Subject. FastComet retains all intellectual property rights in Service Analyses.

13. Miscellaneous

Termination of the Addendum. This Addendum will continue in force until the termination of our processing in accordance with the Terms of Service (the "Termination Date").

Return or Deletion of Customer Data. As described in the Covered Services, the Customer may be provided controls that may use to retrieve or delete Customer Data. Any deletion of Customer Data will be governed by the terms of the particular Covered Services.

14. Liability

The liability of each party under this Addendum will be subject to the exclusions and limitations of liability set out in the Terms of Service. Customer agrees that any regulatory penalties incurred by FastComet in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Addendum and any applicable privacy laws will count towards and reduce FastComet's liability under the Terms of Service as if it was liability to the Customer under the Terms of Service.

15. Entire Terms of Service; Conflict

This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and FastComet, whether written or verbal, regarding the subject matter of this Addendum, including any data processing addenda entered into between FastComet and Customer with regard to the processing of personal data and on

the free movement of such data. Except as amended by this Addendum, the Terms of Service will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Terms of Service and this Addendum, the terms of this Addendum will control.

Annex A - List of FastComet Sub-processors

Available upon request

Annex B – Security Measures

Available upon request