



9920 Jefferson Blvd
Culver City, CA 90232
844-4-PKTFAB (toll free)
+1-424-207-1300 (direct)
www.packetfabric.com

Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is incorporated into and made a part of the Master Service Agreement ("**MSA**"), or Terms and Conditions Agreement, as applicable, between PacketFabric, Inc. ("**PacketFabric**") and Customer. Unless otherwise defined herein, capitalized terms in this Addendum shall have the meanings given in the MSA. This Addendum shall apply to all Services ordered by Customer.

WHEREAS, Customer acts as a data controller as defined by Article 4.7 of GDPR (as defined below);

WHEREAS, Customer wishes order certain Services with PacketFabric wherein, PacketFabric does not extract, compile, store, synthesize or analyze any Customer Data which traverses through PacketFabric's network during Customer's use of the Service;

WHEREAS, the Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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 referred to as "**GDPR**"); and

WHEREAS, the Parties wish to delineate their rights and obligations.

NOW, THEREFORE, in consideration of the premises and mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. Data Processing. PacketFabric does not extract, compile, store, synthesize or analyze any Customer Data which traverses through PacketFabric's network during Customer's use of the Service. PacketFabric, however, expressly acknowledges that Customer Data is Confidential Information and exclusively owned by Customer. No title to or ownership of any of Customer Data or other Confidential Information of Customer, is transferred to PacketFabric under this Addendum. PacketFabric represents and warrants to Customer that it will comply, at its sole expense, with all federal, state, and local laws, regulations, codes, executive orders, and other legal requirements, that apply to PacketFabric and the MSA, including without limitation all applicable privacy and data security laws.
2. Ownership and Rights in Customer Data. Customer is solely responsible for the content of all Customer Data. Customer will encrypt, secure and maintain all rights in its data. PacketFabric does not assume any obligations with respect to Customer Data other than as expressly set forth in the MSA or as required by applicable law. As a general matter, PacketFabric will not have access to, and will not attempt to have access to, the Customer Data traversing through PacketFabric's network during Customer's use of the Service, and therefore will not copy, modify or disclose the Customer Data, except if required by law.
3. Portal. Although PacketFabric does not have access to the Customer Data which traverses through PacketFabric's network during Customer's use of the Service, PacketFabric will have user accounts, contact information, configuration and history data in the event Customer uses PacketFabric's online Portal ("**Customer Account Data**"). PacketFabric will use, at a minimum, industry standard encryption, technical and organizational security measures to transfer Customer Data in a manner designed to protect the integrity and privacy of Customer Data and guard against unlawful or unauthorized access or use.
4. Security of Portal. PacketFabric will maintain sufficient procedures to detect and respond to any unauthorized, access, possession, modification, disclosure, use or other security breaches involving its Portal. PacketFabric will: (a) notify Customer as soon as reasonably practicable, but in no event, more than forty-eight (48) hours after it becomes aware of any actual or reasonably suspected security breaches or unauthorized or attempted access to Customer Data within the Portal or control of PacketFabric; and (b) furnish Customer with all details of the unauthorized or attempted access, possession, disclosure, use or knowledge of such breach. PacketFabric will fully cooperate with Customer in investigating such breach or

unauthorized access and preventing the recurrence of any unauthorized or attempted possession, use of the Customer Data. PacketFabric will take all action to identify, mitigate and remediate the effects of such breach and implement any other reasonable and appropriate measures in response to the breach. PacketFabric will also provide Customer with all available information regarding such breach to assist Customer in implementing its information security response program, and if applicable, in notifying its customers. In the event of a breach or threatened breach of this Addendum by PacketFabric, Customer shall, in addition to any other rights or remedies it may have, be entitled to obtain equitable relief, including an injunction, without the necessity of posting any bond or surety.

5. Privacy and Data Security. In connection with this Addendum, PacketFabric represents, warrants and covenants that PacketFabric, including without limitation PacketFabric personnel and any authorized subcontractors, will not access nor otherwise process any Personally Identifiable Information. If at any time PacketFabric determines that it has accessed Personally Identifiable Information, or may require access to Personally Identifiable Information in connection with this Addendum, PacketFabric shall: (i) notify Customer immediately in writing; (ii) maintain strict confidentiality and security measures to protect the Personally Identifiable Information; (iii) not disclose the Personally Identifiable Information to any other party; (iv) notify Customer immediately if there is any potential or actual breach of security involving the Personally Identifiable Information; and (v) execute additional privacy and data security contractual terms with Customer and any of its Affiliates as required in Customer's sole judgment to comply with applicable privacy and data security laws in all relevant jurisdictions, including but not limited to the following, in each case, as amended or supplemented: the Gramm-Leach-Bliley Act ("**GLBA**"), the Dodd-Frank Act, the Fair Credit Reporting Act, the Equal Credit Opportunity Act, the Truth in Lending Act, the Service members Civil Relief Act, the Telephone Consumer Protection Act, the Fair Debt Collection Practices Act, the CAN-SPAM Act, California Financial Information Privacy Act, the Federal Trade Commission Act, state data breach and data security laws, international data protection and security laws, including but not limited to Directive 95/46/EC of the European Parliament and of the Council and, when effective, the General Data Protection Regulation (the "**EU Data Law**"), and analogous local, state, federal, and international laws relating to the processing, privacy, usage, protection and security of PII. If, in Customer's reasonable judgment, the performance of the Services would violate any applicable law, or in the event the Parties are unable to reach agreement on additional contractual terms required by subpart (v) above, Customer may require PacketFabric to immediately suspend the Services. In the event PacketFabric needs to suspend Customer's use of the Service, such action shall not constitute a default under the MSA. In such event, the Parties will use commercially reasonable efforts to implement an alternative method of performing the Services. If an alternative method cannot be reasonably implemented, the MSA will be terminated and PacketFabric will refund any fees pre-paid by Customer for Services not performed or not delivered.
 - a. Personally Identifiable Information. As used in this Section, the term "**Personally Identified Information**" or "**PII**" means any (a) information that identifies or can be used to identify an individual either alone or in combination with other readily available data; (b) personally identifiable financial or insurance information, including but not limited to "non-public personal information" as that term is defined in GLBA; and (c) any other combination of data that, if compromised, would require notice or reporting under any applicable Privacy Laws.
6. Full Force and Effect. This Addendum attaches to and is incorporated into the MSA. Nothing contained in this Addendum supersedes, replaces, or modifies the MSA. The MSA remains in full force and effect.