General Data Processing Agreement

General Data Processing Agreement

THIS GENERAL DATA PROCESSING AGREEMENT ("DPA") is entered into by OpenVPN Inc., a Delaware corporation ("OpenVPN") and the person or persons to whom OpenVPN has granted a license to use a service described below (the "Customer") and sets forth the terms under which OpenVPN will process Customer Data in connection with that service.

All capitalized terms not defined in this DPA shall have the meanings set forth in the License Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA.

1. Definition of Terms.
    - "Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.
    - "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly."Customer Data" means personal data that OpenVPN processes on behalf of Customer via the Service, as more particularly described in this DPA.
    - "Data Protection Laws" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, European Data Protection Laws and Non-European Data Protection Laws.

General Data Processing Agreement

- “European Data Protection Laws” means all data protection laws and regulations applicable to Europe, including (i) 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”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, “UK Data Protection Laws”); and (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance (“Swiss DPA”).
- “Europe” means, for the purposes of this DPA, the European Economic Area and its member states (“EEA”), Switzerland and the United Kingdom (“UK”).
- “Non-European Data Protection Laws” means the California Consumer Privacy Act (“CCPA”); the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); the Brazilian General Data Protection Law (“LGPD”), Federal Law no. 13,709/2018; and the Privacy Act 1988 of Australia, as amended (“Australian Privacy Law”).
- “Principal Agreement” means the agreement pursuant to which OpenVPN provides the Service to the Customer, including OpenVPN Access Server End User License Agreement, 2 OpenVPN Cloud End User License Agreement, and the OpenVPN Connect End User License Agreement.

General Data Processing Agreement

- “Service” means OpenVPN Cloud, Access Server, OpenVPN Connect, or other computer software or service that OpenVPN provides to the Customer under the License Agreement.
- “Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by OpenVPN.
- “Sensitive Data” means an individual’s (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) information concerning a person’s race, ethnicity, political or religious affiliation, trade union membership, sexual life or sexual orientation, or criminal record.
- “Sub-Processor” means any processor engaged by OpenVPN or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the License Agreement or this DPA. Sub-Processors may include third parties or Affiliates of OpenVPN but shall exclude OpenVPN employees, contractors, or consultants.The terms “personal data”, “controller”, “data subject”, “processor” and “processing” shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and “process”, “processes" and “processed”, with respect to any Customer Data, shall be interpreted accordingly.

General Data Processing Agreement

2. Roles and Responsibilities
    - a. Parties' Roles. If European Data Protection Laws apply to either party's processing of Customer Data, the parties acknowledge and agree that with regard to the processing of Customer Data, OpenVPN is a processor acting on behalf of the Customer (whether itself a controller or a processor).
    - b. Purposes. OpenVPN will process Customer Data for the purposes described in Exhibit A and only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law and to perform the Service, or as OpenVPN and Customer otherwise agreed in writing ("Permitted Purposes"). The License Agreement, including this DPA, along with the Customer's configuration of or use of any settings, features, or options in the Service (as the Customer may be able to modify from time to time) constitute the Customer's complete and final instructions to OpenVPN in relation to the processing of Customer, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.
    - c. Prohibited Data. Unless Sensitive Information is listed in Exhibit A as being among the categories of Customer Data OpenVPN will process, Customer will not provide (or cause to be provided) any Sensitive Data to OpenVPN for processing or storage. OpenVPN will have no obligations with respect to any Sensitive Data or liability for any access or destruction of 3 any Sensitive Data, whether in connection with a Security Incident or otherwise, that Customer provides or makes available to OpenVPN in violation of this Section 2c.

General Data Processing Agreement

- d. Customer Compliance. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to OpenVPN; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for OpenVPN to process Customer Data for the purposes described in the License Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data.e. Lawfulness of Customer's Instructions. Customer will ensure that OpenVPN's processing of the Customer Data in accordance with Customer's instructions will not cause OpenVPN to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. OpenVPN shall promptly notify Customer in writing, unless prohibited from doing so under applicable law, if it becomes aware or believes that any data processing instruction from Customer violates European Data Protection Laws. Customer shall serve as the sole point of contact for OpenVPN and OpenVPN need not interact directly with (including to provide notifications to or seek authorization from) any third-party controller other than through regular provision of the Service to the extent required under the License Agreement. Customer shall be responsible for forwarding any notifications received under this DPA to the relevant controller, where appropriate.

General Data Processing Agreement

3. Sub-Processing
    - a. Authorized Sub-Processors. Customer agrees that OpenVPN may engage Sub-Processors to process Customer Data on Customer's behalf. OpenVPN shall notify Customer if it adds or removes Sub-Processors at least 10 days prior to any such changes if Customer opts in to receive such notifications.
    - b. Sub-Processor Obligations. OpenVPN shall: (i) enter into a written agreement with each Sub-Processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-Processor; and (ii) remain responsible for such SubProcessor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause OpenVPN to breach any of its obligations under this DPA. Customer acknowledges and agrees that OpenVPN may be prevented from disclosing Sub-Processor agreements to Customer due to confidentiality restrictions but OpenVPN shall, upon request, use reasonable efforts to provide Customer with all relevant information it reasonably can in connection with Sub-Processor agreements.

General Data Processing Agreement

4. Security and Confidentiality
    - a. Security Measures. OpenVPN shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Data from Security 4 Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with OpenVPN's security standards, which shall be no less stringent than those that are generally applied in the industry in the United States ("Security Measures").
    - b. Confidentiality of Processing. OpenVPN shall ensure that any person who is authorized by OpenVPN to process Customer Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
    - c. Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that OpenVPN 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 provided to Customer. Customer is responsible for reviewing the information made available by OpenVPN relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws.

General Data Processing Agreement

- d. Security Incident Response. Upon becoming aware of a Security Incident, OpenVPN shall: (i) notify Customer without undue delay, and where feasible, in any event no later than forty-eight (48) hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. OpenVPN's notification of or response to a Security Incident under this Section 4d shall not be construed as an acknowledgment by OpenVPN of any fault or liability with respect to the Security Incident.
- e. Customer Responsibilities. Notwithstanding the above, Customer agrees that it, and not OpenVPN, is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data that is uploaded to the Service.
- f. Government Audit. If a government regulatory authority requires an audit of the data processing facilities of OpenVPN in order to ascertain or monitor Customer's compliance with Data Protection Laws, OpenVPN will cooperate with such audit. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time OpenVPN expends for any such audit, in addition to the rates for services performed by OpenVPN.

General Data Processing Agreement

5. Provisions for Specific Customers and Data.
    - a. Data Center Locations. Customer acknowledges that OpenVPN may transfer and process Customer Data to and in the United States and anywhere else in the world where OpenVPN, its Affiliates or its Sub-Processors maintain data processing operations provided that such transfer is in accordance with applicable law. OpenVPN shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.
    - b. Provisions Applicable to Certain Jurisdictions.
        - i) If OpenVPN is a recipient of Customer Data protected by the Australian Privacy Law, the parties acknowledge and agree that OpenVPN may transfer such Customer Data outside of Australia as permitted by the terms agreed upon by the parties and subject to OpenVPN complying with this DPA and the Australian Privacy Law.
        - ii) To the extent that OpenVPN receives Customer Data from the states and countries listed in Exhibit C, the provisions of Exhibit C will apply to OpenVPN's obligations under this Agreement with respect to that Customer Data.
        - iii) If OpenVPN receives Customer Data from Brazil, the Customer agrees that OpenVPN may process that data outside of Brazil, and represents and warrants that such transfer of Customer Data is in compliance with LGPD.

General Data Processing Agreement

- c. International Transfers from Designated Countries. The parties obligations with respect to Customer Data that originates in the European Area will be governed by the following Addenda to this DPA. To the extent that there is any conflict between the provisions of this DPA and any Addendum that is applicable to the Customer Data from that country or region so designated, that Addendum will control.
  - i) For Customer Data that is transmitted from the EEA and is processed by OpenVPN outside of the EEA, the Data Processing Agreement Addendum, Module 2, (attached as Exhibit D) will govern.
  - ii) For Customer Data that is transmitted from the UK and is processed by OpenVPN outside of the UK, the United Kingdom Data Processing Agreement Addendum (attached as Exhibit E) will govern.
  - iii) For Customer Data that is transmitted from Switzerland and is processed by OpenVPN outside of Switzerland, the Data Processing Agreement Addendum under Switzerland Data Protection (attached as Exhibit F) will govern.
- d. HIPAA Data. If OpenVPN has entered into an agreement with Customer pursuant to which it processes Customer Data that is subject to the Health Insurance Portability and Accountability Act of 1996 and the regulations of the Department of Health and Human Services promulgated thereunder, that agreement will govern all rights and obligations of OpenVPN and the Customer with respect to that data.

General Data Processing Agreement

6. Return or Deletion of Data
    - a. Deletion or Return on Termination. Upon termination or expiration of the Agreement, OpenVPN shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent OpenVPN is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data OpenVPN shall securely isolate, protect from any further processing and eventually delete in accordance with OpenVPN's deletion policies, except to the extent required by applicable law.
    - b. Return or Removal of Customer Data. OpenVPN will promptly delete Customer Data pursuant to an instruction from Customer, whether pursuant to a written request from the data subject or otherwise, provided that such request was in accordance with applicable law. Promptly following Customer's request OpenVPN will provide Customer with evidence of the deletion of that Customer Data.

General Data Processing Agreement

7. Data Subject Rights and Cooperation
    - a. Data Protection Impact Assessment. To the extent required under applicable Data Protection Laws, OpenVPN shall (considering the nature of the processing and the information available to OpenVPN) provide all reasonably requested information regarding the Service to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. OpenVPN shall comply with the foregoing by: (i) complying with Section 4; (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing clauses (i) and (ii) are insufficient for Customer to comply with such obligations, providing additional reasonable assistance (at Customer's expense) upon Customer's request.
8. Limitation of Liability
    - a. Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA shall be subject to the exclusions and limitations of liability set forth in the License Agreement.
    - b. Any claims made against OpenVPN or its Affiliates under or in connection with this DPA shall be brought solely by the Customer.
    - c. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

General Data Processing Agreement

9. Relationship with the License Agreement
    - a. This DPA shall remain in effect for as long as OpenVPN carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 6.a.
    - b. The parties agree that this DPA replaces in its entirety any existing data processing agreement or similar document into which the parties may have previously entered into in connection with the Service.
    - c. In the event of any conflict or inconsistency between this DPA and the License Agreement with respect to Customer Data, the provisions of this DPA will prevail.
    - d. Except for any changes made by this DPA, the License Agreement remains unchanged and in full force and effect.
    - e. No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

General Data Processing Agreement

- f. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the License Agreement, unless required otherwise by applicable Data Protection Laws.g. This DPA may only be amended by means of a writing signed by OpenVPN and Customer; however, if, in the good faith judgment of OpenVPN, any provision of this DPA is required to be amended to comply with a Data Processing Law applicable to the Customer Data, OpenVPN may amend effect such amendment by delivering notice of that amendment to Customer. Such amendment will enter into effect thirty (30) days after notice of that amendment is provided to Customer unless OpenVPN determines in good faith that the amendment is required to enter into effect earlier to comply with that Data Processing Law, in which case that amendment will enter into effect immediately upon OpenVPN providing notice of the same to Customer.

General Data Processing Agreement

EXHIBIT A – DETAILS OF DATA PROCESSING

(a) Categories of Data Subjects: Individual customers of OpenVPN

(b) Categories of Personal Data: Customer may upload, submit, or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data: For OpenVPN's Access Server and OpenVPN Cloud Solution: Data Importer may process certain information about how a User uses the Subscriber Websites or Apps, including a User's Internet Protocol (IP) address and other user engagement and interaction metrics and other statistics. For subscriber processing, Data Importer may process name, email address, usernames, passwords and other login credentials as necessary to manage the user's account.

(c) Sensitive Data Processed (if applicable): No sensitive data is processed by OpenVPN

(d) Frequency of Processing: OpenVPN shall process Personal Data in its provision of Services on a continuous basis pursuant to the terms of the Agreement.

(e) Subject Matter and Nature of the Processing: Storage and other processing necessary to provide, maintain, and improve the Service provided to Customer pursuant to the License Agreement.

General Data Processing Agreement

(f) Purpose of the Processing: OpenVPN shall process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the License Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the License Agreement.

(g) Duration of Processing and Period for which Personal Data will be retained: OpenVPN will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

General Data Processing Agreement

EXHIBIT B – SECURITY MEASURES

The Security Measures applicable to the Service are described here (as updated from time to time in accordance with Section 4.c of this DPA).

MFA is required to access stored data. Access is limited based on least privilege and limited to a small number of importer employees who require access. All data transfer is performed over encrypted connections. Only minimum necessary data is collected. Information Security program is overseen by certified individual (CISSP, CISM, GPEN, GXPN.)

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Sub-processors that are certified in PCI-DSS are used to process credit card transactions. Required transaction information is transferred to importer over encrypted connections.

General Data Processing Agreement

EXHIBIT C - JURISDICTION-SPECIFIC TERMS

Europe: Objection to Sub-Processors. Customer may object in writing to OpenVPN's appointment of a new Sub-Processor within five (5) calendar days of receiving notice in accordance with Section 3.a of the DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, OpenVPN will, at its sole discretion, either not appoint such Sub-Processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

General Data Processing Agreement

Government data access requests. As a matter of general practice, OpenVPN does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about OpenVPN accounts (including Customer Data). If OpenVPN receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a OpenVPN account (including Customer Data) belonging to a data subject whose primary contact information indicates that the data subject is located in Europe, OpenVPN shall: (i) review the legality of the request; (ii) inform the government agency that OpenVPN is a processor of the data; (iii) attempt to redirect the agency to request the data directly from Customer; (iv) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy; and (v) provide the minimum amount of information permissible when responding to the agency or authority based on a reasonable interpretation of the request. As part of this effort, OpenVPN may provide the data subject's primary and billing contact information to the agency. OpenVPN shall not be required to comply with this paragraph if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, the OpenVPN website, OpenVPN's computer network and other assets, or to the Service.

General Data Processing Agreement

California: Except as described otherwise, the definitions of: “controller” includes “Business”; “processor” includes “Service Provider”; “data subject” includes “Consumer”; “personal data” includes “Personal Information”; in each case as defined under the CCPA.

For this “California” section of Exhibit C only, “Permitted Purposes” shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer’s documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for “service providers” under the CCPA.

OpenVPN’s obligations regarding data subject requests, as described in Section 7 of this DPA, extend to rights requests under the CCPA. Notwithstanding any use restriction contained elsewhere in this DPA, OpenVPN shall process Customer Data to perform the Service, for the Permitted Purposes and/or in accordance with Customer’s documented lawful instructions, or as otherwise permitted or required by applicable law.

Notwithstanding any use restriction contained elsewhere in this Exhibit C, OpenVPN may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.

General Data Processing Agreement

Where Sub-Processors process the Personal Information of Customer contacts, OpenVPN takes steps to ensure that such Sub-Processors are Service Providers under the CCPA with whom OpenVPN has entered into a written contract that includes terms substantially similar to this “California” section of Exhibit or are otherwise exempt from the CCPA’s definition of “sale”. OpenVPN conducts appropriate due diligence on its Sub-Processors.

Canada: OpenVPN takes steps to ensure that OpenVPN’s Sub-Processors are third parties under PIPEDA, with whom OpenVPN has entered into a written contract that includes terms substantially similar to this DPA. OpenVPN conducts appropriate due diligence on its SubProcessors.

OpenVPN will implement technical measures set forth in Section 4 of the DPA.

Addendums for EEU, UK, and Switzerland available upon request

Rev. 9.19.2022