Splashtop Corporate Customer Data Processing Agreement

Splashtop Inc. ("SPLASHTOP" or "us" or "our") serves enterprises, public sector entities and other organizations ("Customers") and protects Customer Data in compliance with the terms of this Corporate Customer Data Processing Agreement ("DPA"). Customer Data means personal data relating to named or identifiable individuals that Customer's authorized users ("Authorized Users") upload to our servers in compliance with applicable law and our applicable service agreement or other commercial contract terms ("Contract") when Customers use our remote access software-as-a-service offerings and related data processing services as described in our data sheets, service specifications, and other technical documentation, as amended from time to time ("Services").

1. Control and Ownership. As between Customer and SPLASHTOP, Customers own and control all Customer Data. Customer is a Controller under the General Data Protection Regulation in the EU ("GDPR") and a Business under the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act ("CCPA"). SPLASHTOP is a processor under GDPR and a service provider under CCPA. SPLASHTOP does not use Customer Data, except: (a) in the interest and on behalf of the Customer; (b) as necessary to provide the Services, (c) as instructed by the Customer, including in the Contract, this DPA or otherwise, or (d) as otherwise required by law. SPLASHTOP returns or deletes Customer Data at Customer's request, as agreed in the Contract, or after the Contract expires or is terminated. SPLASHTOP reserves all rights to the Services, SPLASHTOP's technology and SPLASHTOP's data, including any information that SPLASHTOP discovers, creates or derives as it provides Services, except Customer Data.

2. Security. SPLASHTOP applies technical, administrative and organizational data security measures that meet or exceed the requirements described in SPLASHTOP's Technical and Organizational Measures - (TOMs"), details of which are available at: [https://www.splashtop.com/security/practices/technical-and-organizational-measures]. SPLASHTOP may update and modify the TOMs from time to time, provided that SPLASHTOP must not reduce the level of security provided thereunder, except with Customer's consent or with 90 days prior written notice.

3. Cooperation with Compliance Obligations. At Customer's reasonable request, SPLASHTOP will reasonably assist Customer with data access, deletion, portability and other requests, at Customer's expense where any custom efforts are required of SPLASHTOP. At Customer's request, SPLASHTOP will agree to EU Standard Contractual Clauses for cross-border transfers to processors. If Customer can no longer legally use SPLASHTOP's products due to changes in law or technology, SPLASHTOP shall allow Customer to terminate certain or all contracts and provide transition or migration assistance as reasonably required, subject to termination charges and fees as mutually agreed in good faith by the parties.

4. Submit to Audits. SPLASHTOP will make available to Customer all information necessary to demonstrate compliance with the obligations of Article 28 GDPR, and will submit to reasonable data security and privacy compliance audits and shares audit report results with Customer. SPLASHTOP also offers a customer audit program subject to reasonable precautions and safeguards as follows:

(a) Audits conducted by Customers representative (i) shall be limited to Customer Data or information pertaining to the Services performed under the Terms of Service agreed upon by Customer and SPLASHTOP; (ii) shall respect the confidentiality obligations of SPLASHTOP's other customers (iii) shall be conducted at Customer's sole expense and (iv) shall be performed not more than once annually.

(b) Customer may only mandate an auditor that is approved by SPLASHTOP in writing, such approval not to be unreasonably withheld.

(c) Customer shall work with SPLASHTOP to schedule a mutually agreed upon time for audit to be conducted.

(d) SPLASHTOP will not permit access to SPLASHTOP owned premises for any individual unless he or she produces reasonable evidence of identity and authority; or outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to SPLASHTOP that this is the case before attendance outside those hours begins; or for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits which: (i) Customer reasonably considers necessary because of genuine concerns as to SPLASHTOP's compliance with this DPA or after a security breach; or (ii) Customer is required to carry out by a Supervisory Authority under the GDPR, where Customer has identified its concerns or the relevant requirement or request in its notice to SPLASHTOP of the audit.

5. Breach Notification. If SPLASHTOP becomes aware of a confirmed Security Incident or has a reasonable suspicion of unauthorized access to Customer Data, SPLASHTOP will inform Customer without undue delay, and at any rate within 72 hours and will provide reasonable information and cooperation to Customer so that Customer can fulfil any Personal Information/ Personal Data Security Incident reporting obligations it may have under the applicable Privacy/Data Protection Laws. SPLASHTOP will take reasonably necessary measures to remedy and mitigate the effects of the Security Incident and will keep Customer informed of all material developments with the Security Incident.

6. No Information Selling or Sharing for Cross-Context Behavioral Advertising. SPLASHTOP does not accept or disclose any Customer Data as consideration for any payments, services or other items of value. SPLASHTOP does not sell or share any Customer Data, as the terms "sell" and "share" are defined in CCPA. SPLASHTOP processes Customer Data only for the business purposes specified in the written Contract. Splashtop does not retain, use, or disclose Customer Data (a) for cross-context behavioral advertising, or (b) outside the direct business relationship with the Customer. SPLASHTOP does not combine Customer Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA.

7. EEA Personal Data: With respect to any Customer Data that is subject to the EU General Data Protection Regulation (GDPR) or similar laws of other countries including the UK as "personal data," SPLASHTOP accepts the following obligations as a data importer, processor or subprocessor of Customer and warrants that SPLASHTOP

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or EU Member State law to which Splashtop is subject; in such a case, Splashtop shall inform the controller of that legal requirement before processing, unless prohibited by law from doing so;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32 of the GDPR (security of processing);
(d) respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controller's obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects)
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data. By default, on termination of services, controller's data will be deleted; encrypted backups will be retained until they are cycled out, over a 2-year cycle.
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

For Customers based in the EU, SPLASHTOP will process their Customer Data in the EU. For Customers based outside of the EU, SPLASHTOP will process their Customer Data in the USA.

SPLASHTOP notes that Customer Data from Customers based outside of the EU may at times include the personal data of EU individuals. To the extent that SPLASHTOP processes personal data of EU individuals in the USA, the transfer of personal data to the USA will be pursuant to the Standard Contractual Clauses for international transfer ("SCCs") (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN). For purposes of the SCCs, module 2 (controller to processor) shall apply. Clause 7 is opted out. In Clause 9 option 2 (general written authorisation) will apply, authorization period will be 14 days; a list of approved subprocessors is available at

[https://www.splashtop.com/subprocessors] and Customer may at its discretion sign up there for notifications of changes to that list. In Clause 11 the optional language will not apply. In Clause 17 governing law will be Dutch law; In Clause 18 disputes shall be resolved by the courts of Netherlands. In Annex I Customer is the 'Data exporter', SPLASHTOP is the 'Data importer'; the 'Data subjects', 'Categories of data', 'Frequency of the transfer', 'Nature of processing', 'Purpose', 'Retention period' and 'Subject matter, nature and duration of the processing' are as described in Annex 1. The 'competent supervisory authority' is the Dutch data protection authority.

To the extent that SPLASHTOP processes personal data of UK individuals in the USA, the transfer of Customer Data to SPLASHTOP is made on the basis of the UK's International Data Transfer Addendum to the EU SCCs ("UK Addendum") dated, March 21, 2022 (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), hereby incorporated by the parties into this DPA. The UK Addendum shall incorporate the EU SCCs, as described above, excluding the amendments and exceptions included in the UK Addendum.

8. Integration. This DPA is binding on SPLASHTOP if and to the extent it is expressly agreed or incorporated by reference in a duly signed Contract. This DPA shall not create third party beneficiary rights. SPLASHTOP does not accept or submit to additional requirements relating to Customer Data, except as specifically and expressly agreed in writing with explicit reference to the Contract and this DPA.

ANNEX I

Description of the processing

Categories of data subjects whose personal data is processed

Trial users, freemium users, subscribed users, website visitors .....

Categories of personal data processed

Email address (Splashtop Account ID [SPID]), password, device information.....

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A.....

Nature of the processing

To provide, maintain services, analytics, provide marketing information, perform transactions, send communication regarding Splashtop services, provide technical and sales services .....

Purpose(s) for which the personal data is processed on behalf of the controller

For customers to gain account access and use the services and provision of account support and expansion.....

Duration of the processing

Duration of contract, proceeded by 2-year data retention of backups after termination of the contract .....

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

Company	Location	Services	Principle for Transfers
Amazon Web Services	USA	Database (hosting) and infrastructure for EU stack.	SCC
Google Cloud Platform	Global (regionally based)	Infrastructure (Relay servers) Does not process or store customer data.	SCC
Oracle Cloud Infrastructure	Global (regionally based)	Infrastructure (Relay servers) Does not process or store customer data.	SCC
Salesforce	USA	Customer Relationship Manager	SCC
Zendesk	USA	Service support platform	SCC
Intercom.io	USA	Website live chat	SCC
Microsoft	USA	Email platform	SCC
HubSpot	USA	Marketing platform	SCC
RingCentral	USA	Phone provider	SCC
Osano	USA	Cookie Consent	SCC
Splashtop Taipei	Taipei, Taiwan	Support team for off hours	SCC