Splashtop Cloud-Produkte

Sicherheitsübersicht

Aktualisiert am 17. April 2026

Inhalt

Einleitung

Dieses Whitepaper bietet einen technischen Überblick über die Cloud-Business-Produkte von Splashtop aus sicherheitstechnischer Perspektive. Es umfasst die Architektur, Protokolle, Infrastruktur und Komponenten der Splashtop-Produkte. Das Dokument kann Technik- und Sicherheitsexperten dabei helfen, den Aufbau von Splashtop aus sicherheitstechnischer Sicht zu verstehen. Außerdem kann es ihnen dabei helfen, die Produkte so einzusetzen, dass sie den Sicherheitsanforderungen ihrer Organisationen entsprechen und diese ergänzen.

Hinweis für Nutzer aus der Europäischen Union (EU)
Standardmäßig werden EU-Nutzer dazu geleitet, ihre Benutzerkonten in der EU-basierten Cloud-Infrastruktur von Splashtop anzulegen, die sich in Deutschland befindet. Dabei handelt es sich um eine eigenständige Infrastruktur, die von der in den USA ansässigen Infrastruktur getrennt ist, die Splashtop-Nutzer im Rest der Welt bedient. Diese Trennung ermöglicht es den Nutzern, etwaige Anforderungen an die Datensouveränität zu erfüllen.

Produkte

Dieses Whitepaper bezieht sich auf die Suite der **cloudbasierten** Splashtop-Fernzugriffsprodukte für Unternehmen (siehe unten). Diese Produkte ermöglichen es Privatpersonen und Unternehmen, Computer und mobile Geräte aus der Ferne zu steuern und zu verwalten, um die Produktivität zu steigern und Supportleistungen zu erbringen.

Diese Produkte wurden unter Berücksichtigung von Sicherheitsaspekten entwickelt, um sicherzustellen, dass nur autorisierte Nutzer Zugriff haben, Daten durchgängig geschützt sind und Nutzer alle Aktivitäten lückenlos nachverfolgen können.

Die Suite der cloudbasierten Remote-Desktop-Produkte von Splashtop umfasst drei Produkte:

- *Splashtop Enterprise*. Für Unternehmen, die Remote-Zugriff und Support auf Unternehmensniveau benötigen, mit Single Sign-On, detaillierten Kontrollmöglichkeiten, umfangreichen Protokollierungsfunktionen einschließlich SIEM-Export und Cloud-Aufzeichnung, Service-Desk-Workflow, ITSM-Integration, zeitgesteuertem Zugriff, offenen APIs, RDP-/VNC-/SSH-Zugriff und vielem mehr.

- *Splashtop Remote Support*. Für MSPs und IT-Experten, um remote auf die von ihnen verwalteten Computer zuzugreifen. Die Agent-Software ist auf den Computern vorinstalliert. Die Zugriffsberechtigungen werden streng kontrolliert. Helpdesk-Techniker können ihre Benutzer zudem ad hoc unterstützen – ohne dass eine Vorinstallation erforderlich ist und mit einem einfachen „Download-und-Ausführen"-Vorgang.
- *Splashtop Remote Access*. Für Berufstätige oder kleine Teams, um jederzeit und von überall aus per Fernzugriff auf ihre Arbeitscomputer zuzugreifen. Die Agent-Software ist auf den Computern vorinstalliert. Die Zugriffsberechtigungen werden streng kontrolliert.

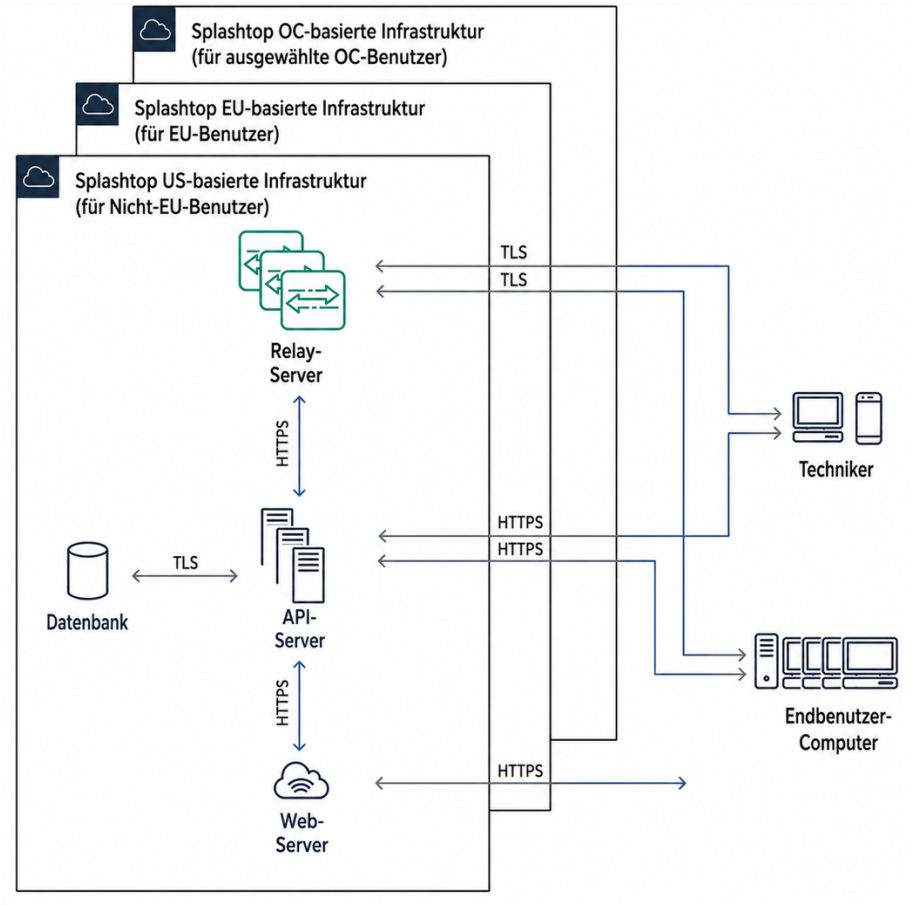
Architekturübersicht

Die Architektur der cloudbasierten Splashtop-Produkte besteht aus den folgenden Hauptkomponenten:

- Agent-Software, die auf den Geräten der Endbenutzer installiert ist („*Splashtop* Streamer")
- Techniker-App, die auf den Geräten der Techniker installiert ist („*Splashtop Business* App")
- API-Server
- Relay-Server
- Webserver
- Datenbank

Splashtop unterhält drei Cloud-Infrastrukturen: eine für Nutzer in der EU, eine für Nutzer außerhalb der EU und eine für ausgewählte Kunden in Ozeanien. Jede Cloud-Infrastruktur verfügt über eigene API-Server, Webserver und eine eigene Datenbank. Die Nutzerdaten sind zwischen den drei Infrastrukturen vollständig voneinander getrennt. Gespeicherte Daten werden verschlüsselt in der jeweiligen Hoheitsregion gespeichert.

Das folgende Diagramm veranschaulicht die Hauptkomponenten der Splashtop-Cloud-Infrastruktur, ihre Kommunikationswege und die verwendeten Protokolle.



Die Kommunikation zwischen allen oben genannten Komponenten ist verschlüsselt.

Webserver verwenden Standard-HTTPS über Port 443 mit TLS 1.2. API-

Server verwenden Standard-HTTPS über Port 443 mit TLS 1.2.

Relay-Server verwenden TCP über Port 443 mit TLS 1.2 und AES-256-Verschlüsselung.

Protokolle und Komponenten„ “
(aus Sicht der Sicherheit)

Die Splashtop-API-Server sind für die US-Infrastruktur über Kalifornien und Oregon, für die EU-Infrastruktur über Deutschland und für die Ozeanien-Infrastruktur über Australien lastverteilt.
Relay-Server befinden sich an mehreren Standorten weltweit, um in unmittelbarer Nähe zu sein und die Leistung für Nutzer in ganz Nordamerika, Südamerika, Europa, dem Nahen Osten, Afrika, Asien und Australien zu verbessern.
Die Webserver befinden sich in Oregon für die US-Infrastruktur, in Deutschland für die EU-Infrastruktur und in Australien für die Ozeanien-Infrastruktur.
Die Datenbank befindet sich ebenfalls in Oregon für die US-Infrastruktur, in Deutschland für die EU-Infrastruktur und in Australien für die Ozeanien-Infrastruktur, mit regionenübergreifenden Backups und Notfallwiederherstellung.

API-Server
Die Endpunkte (*Splashtop-Streamer* und *Splashtop Business*-App) kommunizieren über Standard-HTTPS mit den API-Servern. HTTPS schützt alle übertragenen Informationen.
Jeder API-Server verfügt über ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat (2048-Bit-RSA-SHA-2), um seine Identität zu gewährleisten und Man-in-the-Middle-Angriffe zu verhindern.
Der API-Server verwendet TLS 1.2.

Relay-Server
Die Endpunkte (*Splashtop-Streamer* und *Splashtop* Business-App) bauen jeweils eigenständig TLS-Verbindungen über TCP mit den Relay-Servern auf. Der Relay-Server vermittelt anschließend einen End-to-End-Tunnel zwischen den beiden entsprechenden Endpunkten. Die beiden Endpunkte handeln den TLS- und den AES-256-Verschlüsselungsschlüssel direkt miteinander aus. Der daraus resultierende verschlüsselte Tunnel überträgt die Daten der Remote-Sitzung. Die Daten sind durchgehend geschützt und können nur an den Endpunkten der Benutzer entschlüsselt werden.
Jeder Relay-Server verfügt über ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat (2048-Bit-RSA-SHA-2).
Der Relay-Server verwendet TLS 1.2.

Webserver
Webserver stellen den Kunden die webbasierte Verwaltungsoberfläche zur Verfügung. Dort können Kunden alle Computer, Benutzer, Techniker und Audit-Protokolle einsehen und verwalten.
Der Zugriff auf die Webkonsole ist ausschließlich über HTTPS mit TLS 1.2 möglich, wodurch alle übertragenen Informationen gesichert werden. Jeder Webserver verfügt über ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat (2048-Bit-RSA-SHA-256).

Datenbank
Die Datenbank ist ein verschlüsselter (AES-256) Datenbankcluster. Sie wird täglich in mehreren Regionen gesichert. Die Sicherungen sind ebenfalls verschlüsselt.
Die Datenbank speichert Hashwerte der Benutzerkennwörter, nicht die Kennwörter selbst. Die Hashwerte werden mit SHA-512 unter Verwendung eines für jedes Kennwort einzigartigen 20-Zeichen-Salts generiert.

Endpunkt-Software
Die Endpunkt-Software besteht aus der *Splashtop* Business-App, *dem Splashtop-Streamer* und der *Splashtop* SOS-App (für Ad-hoc-Support). Sie werden über HTTPS von den Splashtop-Websites heruntergeladen, wodurch die Legitimität der Quelle gewährleistet ist.
Die Binärdateien sind mit den entsprechenden Zertifikaten kodsigniert, um ihre Integrität zu gewährleisten.
Windows-Ausführungsdateien sind mit X.509-Zertifikaten mit erweiterter Validierung (EV)
X.509-Zertifikaten signiert.
Ausführbare Dateien für macOS sind gemäß den Anforderungen von Apple für Entwickler mit einem X.509-Zertifikat signiert.

Sicherheitsfunktionen

Die Designmerkmale von Splashtop, die die Sicherheit der Benutzer gewährleisten, lassen sich grob in **Authentifizierung**, **Autorisierung** und **Protokollierung** unterteilen.

Splashtop wurde mit strengen Authentifizierungsanforderungen entwickelt, um sicherzustellen, dass Benutzer tatsächlich die sind, für die sie sich ausgeben.

Zudem gibt es eine Reihe robuster Autorisierungskontrollen, um die Rechte und Zugriffsberechtigungen authentifizierter Benutzer fein abzustimmen. Die Autorisierung kann die SSO-Funktionen (Single

Sign-On), SCIM (System for Cross-domain Identity Management) und JIT (Just-in-Time) des Unternehmens für eine zentralisierte Steuerung und bessere Automatisierung nutzen.

Schließlich ist eine umfassende Protokollierung vorhanden, um die Überwachung und **das Auditing** zu ermöglichen.

Authentifizierung
Es stehen verschiedene Mechanismen zur Verfügung, um sicherzustellen, dass Benutzer, die sich bei Splashtop anmelden, tatsächlich die sind, für die sie sich ausgeben.

- *Splashtop-Anmeldedaten*. Die Grundlage der Authentifizierung bilden die Splashtop-Anmeldedaten: die Splashtop-ID und das Passwort. Die Splashtop-ID ist eine verifizierte E-Mail-Adresse. Das Passwort muss bestimmte Anforderungen an die Komplexität erfüllen.
  Single Sign-On (SSO) ist mit *Splashtop Enterprise* verfügbar, um die Authentifizierung über das Verzeichnis der Organisation zu zentralisieren. Splashtop unterstützt SSO über SAML 2.0 und OpenID Connect. Für die meisten gängigen Identitätsanbieter stehen vorgefertigte Konnektoren zur Verfügung.
- *Geräteauthentifizierung*. Immer wenn sich ein Benutzer bei Splashtop anmeldet – sei es über die Webkonsole oder die *Splashtop* Business-App –, wird eine obligatorische Geräteauthentifizierung durchgeführt. Ist das Gerät oder der Browser neu, muss der Benutzer einen Geräteauthentifizierungsprozess durchlaufen. Dabei wird überprüft, ob der Benutzer tatsächlich Eigentümer der mit seiner Splashtop-ID verknüpften E-Mail-Adresse ist.
  Administratoren und Benutzer können die Liste der authentifizierten Geräte einsehen und Geräte jederzeit über die Webkonsole deaktivieren. Der Teambesitzer kann zudem die Dauer festlegen, für die Geräte authentifiziert bleiben.
  Darüber hinaus haben Administratoren die Möglichkeit, festzulegen, dass die E-Mails zur Geräteauthentifizierung aller Benutzer ausschließlich an die Administratoren gesendet werden, um die volle Kontrolle darüber zu behalten, welche Geräte Benutzer für den Fernzugriff verwenden dürfen.
- *Zwei-Faktor-Authentifizierung*. Ein Benutzer kann die Zwei-Faktor-Authentifizierung einrichten. Die Zwei-Faktor-Authentifizierung basiert auf TOTP und erfordert die Registrierung eines Mobilgeräts und einer Authentifikator-App. Zu den Authentifikator-Apps, die TOTP unterstützen, gehören *Google Authenticator*, *Cisco Duo Mobile* und *Microsoft Authenticator*. Sobald die Zwei-Faktor-Authentifizierung aktiviert ist, erfordert die Anmeldung mit dem Splashtop-Konto in der Webkonsole oder in der *Splashtop* Business-App die Eingabe eines
  Zeitbasierten Einmalpasswort aus der Authentifizierungs-App

auf dem registrierten Mobilgerät.
Der Teambesitzer hat die Möglichkeit, von jedem Benutzer im Team die Verwendung der Zwei-Faktor-Authentifizierung zu verlangen.
Der Teambesitzer hat außerdem die Möglichkeit, die vertrauenswürdigen Geräte der Benutzer zu verwalten und festzulegen, wie lange diese Geräte als vertrauenswürdig gelten.

- *IP-Adressen-Zulassungsliste*. Der Teambesitzer kann die IP-Adressen einschränken, von denen aus auf die *Splashtop* Business-App und die Webkonsole zugegriffen werden darf. So kann beispielsweise ein Callcenter die Nutzung von Splashtop darauf beschränken, dass die Techniker sich vor Ort befinden.

Berechtigungen

Der Teambesitzer und die Administratoren können festlegen, welche Benutzer oder Benutzergruppen Zugriff auf genau welche Computer oder Computergruppen haben.
Der Teambesitzer und die Administratoren können über die Webkonsole Benutzer einladen, aktivieren, deaktivieren und löschen.
Unternehmen mit SSO und Identitätsanbietern, die SCIM oder JIT unterstützen, können den Arbeitsablauf weiter optimieren, indem sie über ihre Verzeichnisse Benutzer bereitstellen, gruppieren und Berechtigungen festlegen und diese Konfigurationsänderungen dann automatisch an Splashtop weiterleiten.
Die Zugriffsberechtigung wird an mehreren Stellen überprüft, unter anderem beim Aufbau einer Verbindung.
Bei einem Verbindungsversuch kann eine zusätzliche Autorisierung erforderlich sein. Beispielsweise kann der Benutzer aufgefordert werden, die Windows- oder Mac-Anmeldedaten des Zielcomputers oder einen für den Zielcomputer spezifischen benutzerdefinierten Sicherheitscode einzugeben.
Der Zielcomputer kann außerdem so konfiguriert werden, dass in der letzten Phase des Verbindungsaufbaus eine ausdrückliche Genehmigung des Benutzers erforderlich ist, der sich gerade vor dem Computer befindet (in Form einer Popup-Eingabeaufforderung mit einem Countdown-Timer).
Im Falle eines Ad-hoc-Supports über *Splashtop Remote Support* oder *Splashtop Enterprise* wird der Fernzugriffsprozess vom Endbenutzer am Zielcomputer initiiert. Der Endbenutzer muss ausdrücklich auf einen URL-Link klicken, eine App herunterladen, die App ausführen usw., um dem Techniker den Fernzugriff zu ermöglichen.
Der Team-Inhaber hat die Möglichkeit, bestimmte Funktionen vollständig zu deaktivieren, falls dies zur Einhaltung der Sicherheitsanforderungen der Organisation erforderlich ist. Zu diesen Funktionen gehören Dateiübertragung, Kopieren und Einfügen, Remote-Druck, Remote-Befehle, Sitzungsaufzeichnung, Neustart und mehr. Mit *Splashtop Enterprise* lassen sich verschiedene Funktionen

sehr detailliert gesteuert werden, bis hinunter auf die Ebene einzelner Benutzer oder Benutzergruppen.
Wenn ein Benutzer per Fernzugriff auf einen Zielcomputer zugreift (um eine Fernsteuerung, eine Dateiübertragung im Hintergrund oder einen Befehl im Hintergrund auszuführen), wird auf dem Zielcomputer eine obligatorische Benachrichtigung angezeigt. Dies trägt zum Schutz vor unbefugter Überwachung bei und gewährleistet die Privatsphäre der Benutzer.
Der Zielcomputer kann so konfiguriert werden, dass eine Remote-Sitzung automatisch beendet wird, wenn er eine bestimmte Zeit lang inaktiv war.
Der Zielcomputer kann außerdem so konfiguriert werden, dass er nach Beendigung einer Sitzung automatisch zum Sperrbildschirm des Betriebssystems zurückkehrt.
Der Zielcomputer kann so konfiguriert werden, dass sein Bildschirm automatisch ausgeblendet wird, wenn eine Remote-Desktop-Sitzung läuft. Dies trägt dazu bei, die Privatsphäre der Aktionen des Remote-Benutzers zu schützen.

Protokollierung
Alle Remote-Desktop-Sitzungen werden mit den folgenden Informationen protokolliert:

- Startzeit, Endzeit und Dauer
- Name des Zielcomputers, auf den zugegriffen wird, und dessen IP-Adresse
- Splashtop-ID des Benutzers, der den Fernzugriff durchgeführt hat, Name des für den Fernzugriff verwendeten Geräts und IP-Adresse des Geräts
- Derzeit laufende Remote-Desktop-Sitzungen werden in der Webkonsole entsprechend gekennzeichnet.

Alle Dateiübertragungen werden mit den folgenden Informationen protokolliert:

- Zeitstempel
- Name des Zielcomputers, auf den zugegriffen wird, und dessen IP-Adresse
- Splashtop-ID des Benutzers, der den Fernzugriff durchgeführt hat, Name des für den Fernzugriff verwendeten Geräts und IP-Adresse des Geräts
- Dateiname und -größe
- Richtung der Übertragung

Fernsteuerungssitzungen, Chat-Sitzungen und andere Sitzungstypen werden ebenfalls protokolliert, gegebenenfalls einschließlich des vollständigen Sitzungsprotokolls.
Alle oben genannten Protokolle können in der Splashtop-Webkonsole für die letzten 90 Tage eingesehen werden.

Der Verlauf der Teamverwaltung (Verwaltung von Benutzern, Änderungen an Berechtigungen, Hinzufügen und Entfernen von Computern, Anmeldungen auf neuen Geräten, fehlgeschlagene Anmeldeversuche usw.) kann in der Splashtop-Webkonsole für die letzten drei Jahre eingesehen werden.
Protokolle der letzten 12 Monate können archiviert werden, indem sie aus der Webkonsole im CSV-Format exportiert werden. Mit *Splashtop Enterprise* können Protokolle zudem kontinuierlich und automatisch über eine SIEM-Integration oder eine offene API-Integration abgerufen werden.
Wird das Splashtop-Produkt in Verbindung mit einem unterstützten Ticketingsystem verwendet, werden die Protokolle direkt in die entsprechenden Tickets im Ticketingsystem eingefügt.
Remote-Desktop-Sitzungen können aufgezeichnet werden, wobei die Aufzeichnungen lokal auf dem Arbeitsplatzrechner des Technikers gespeichert werden. Die Aufzeichnung kann jederzeit über die Symbolleiste innerhalb der Sitzung gestartet und gestoppt werden. Der Team-Inhaber kann zudem die automatische, obligatorische Aufzeichnung aller Sitzungen aktivieren sowie den Speicherpfad und die maximale Größe der Aufzeichnungen konfigurieren. *Splashtop Enterprise* bietet zusätzlich die Option der Aufzeichnung in der Cloud(†) an, was aus Gründen der Benutzerfreundlichkeit und der Compliance wichtig sein kann. Cloud-Aufzeichnungen werden 90 Tage lang gespeichert und können über die Webkonsole wiedergegeben oder heruntergeladen werden.

Infrastruktur

Die Splashtop-Infrastruktur nutzt Infrastructure-as-a-Service-Anbieter (IaaS) wie Amazon Web Services (AWS), Google Cloud Platform (GCP) und Oracle Cloud Infrastructure (OCI).

Diese Anbieter gewährleisten eine hohe Verfügbarkeit und physische Sicherheit ihrer Infrastruktur. Splashtop hat zusätzliche Redundanzebenen und Failover-Logik über die verschiedenen Anbieter hinweg eingerichtet, um die Zuverlässigkeit weiter zu verbessern. Wie bereits erwähnt, verfügt Splashtop über zahlreiche Präsenzpunkte weltweit, um durch die Nähe zu den Nutzern eine gute Leistung zu gewährleisten und regionenübergreifende Redundanz zu schaffen.

Splashtop nutzt neben den Standard-Recheninstanzen auch verschiedene Dienste dieser Infrastrukturanbieter. Zu den zusätzlich genutzten Diensten gehören verwaltete Datenbanken, Cloud-Speicher, Edge-Caching, Lastverteiler, DNS-Dienste und eine Vielzahl von Überwachungstools.

Compliance

Aktuelle Informationen zu Splashtop im Hinblick auf Branchenstandards finden Sie unter https://www.splashtop.com/compliance.

ISO/IEC 27001:2022
ISO/IEC 27001 ist ein international anerkannter Maßstab für die Einrichtung und Aufrechterhaltung eines robusten Informationssicherheits-Managementsystems. Mit seinen umfassenden und strengen Anforderungen unterstützt der Standard einen ganzheitlichen Ansatz für die Informationssicherheit, indem er Personen, Richtlinien und Technologien durch strenge Tests und Audits gründlich bewertet. Splashtop unterzieht sich jährlichen ISO/IEC 27001-Audits.

Service Organization Control 2 (SOC 2)
SOC 2 ist ein umfassendes Berichtsrahmenwerk, das vom American Institute of Certified Public Accountants (AICPA) entwickelt wurde.
Die SOC-2-Bescheinigung belegt, dass bei Splashtop Kontrollmaßnahmen vorhanden sind und ordnungsgemäß angewendet werden, um die Sicherheit und den Datenschutz der Kundendaten zu gewährleisten.
Splashtop unterzieht sich jährlichen SOC-2-Audits und erfüllt sowohl die Anforderungen von SOC 2 Typ 2 als auch von SOC 3.

Health Insurance Portability and Accountability Act (HIPAA)
Die HIPAA-Konformität ist für Splashtop nicht relevant, da Splashtop keine Computerdaten der Nutzer verarbeitet, speichert oder darauf zugreift. Splashtop ermöglicht die Übertragung von Video, Audio und Daten und speichert die Streams nicht.
Die Übertragung erfolgt durchgehend verschlüsselt.
Die Splashtop-Produkte helfen den Nutzern bei ordnungsgemäßer Verwendung in Verbindung mit den zuvor beschriebenen Sicherheitsmaßnahmen dabei, die HIPAA-Anforderungen ihrer Organisationen zu erfüllen.

Gesetz über die Rechte der Familie auf Bildung und Datenschutz (FERPA)
Ähnlich wie oben gilt die FERPA-Konformität nicht für Splashtop, da Splashtop keine Bildungsunterlagen von Schülern verarbeitet, speichert oder darauf zugreift.
Die Splashtop-Produkte helfen den Benutzern bei ordnungsgemäßer Verwendung in Verbindung mit den zuvor beschriebenen Sicherheitsmaßnahmen dabei, die FERPA-Anforderungen ihrer Bildungseinrichtungen zu erfüllen.

Datenschutz-Grundverordnung (DSGVO)
Splashtop erfüllt als Verantwortlicher und Auftragsverarbeiter die Anforderungen der DSGVO für Nutzer in der Europäischen Union. Nutzer haben das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten.

California Consumer Privacy Act (CCPA)
Splashtop erfüllt die Anforderungen des CCPA für Einwohner Kaliforniens. Nutzer haben das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten.

---

† Besonderer Hinweis zur Aufzeichnung von Cloud-Sitzungen: Wir sind uns bewusst, dass die Aufzeichnung von Sitzungen ein äußerst sensibler und privater Vorgang ist, und haben daher entsprechende strenge Sicherheitsvorkehrungen getroffen. Splashtop-Mitarbeiter haben keinen Zugriff auf die Sitzungsaufzeichnungen. Der Zugriff erfolgt ausschließlich von Gerät zu Gerät und dient ausschließlich dem Zweck, unseren Nutzern die Möglichkeit zu geben, ihre eigenen Aufzeichnungen über die Webkonsole abzuspielen und herunterzuladen. Die einzige Ausnahme bildet ein vorübergehender, überwachter Zugriff zu Zwecken der Fehlerbehebung, der einer Genehmigung auf Führungsebene bedarf.