Datenschutz-Infoblatt für die Nutzung von TeamDrive

1. Einleitung

Datensicherheit und Datenschutz sind Bereiche mit hoher Relevanz für jedes Unternehmen, aber ebenso wichtig für jeden Anwender oder auch Privatpersonen, die mit Daten im Internet arbeiten. Wir möchten Ihnen mit diesem Infoblatt notwendige Informationen und Maßnahmen zum Umgang mit Daten in Verbindung mit unserem Produkt TeamDrive vermitteln.

Bei Datensicherheit, als Teil der IT-Sicherheit, geht es vornehmlich darum, dass Daten vor unberechtigtem Zugriff und vor Verlust geschützt werden. Hier bietet TeamDrive die technischen Voraussetzungen, um diese Anforderungen zu erfüllen. Der Anwender muss allerdings selber dafür Sorge tragen die richtigen Einstellungen und Konfigurationen gemäß seinen persönlichen Anforderungen einzustellen.

Beim Datenschutz geht es vor allem um den Schutz personenbezogener Daten, die seit Mai 2018 in der Datenschutzgrundverordnung (DSGVO) geregelt werden. Ein Verstoß gegen die die Regeln der DSGVO kann durch die zuständigen Behörden mit hohen Bußgeldern geahndet werden. In diesem Infoblatt vermitteln wir Ihnen einen Überblick über wichtige Fragen, Entscheidungen und Konfigurationen die Sie selber entsprechend Ihrer Anforderungen vornehmen sollten.

2. Grundlagen

In diesem Dokument wird auf datenschutzrechtliche Anforderungen verwiesen, die beim Einsatz des Produktes „TeamDrive“ beachten werden sollen. Dieses Dokument soll als Basisinformation für die Einsatzplanung eines Produktes wie „TeamDrive“ dienen. Die Datenschutzgesetze und Richtlinien des Bundes bzw. der jeweiligen Länder sind zusätzlich zu beachten.

TeamDrive unterstützt datenschutzrechtliche Anforderungen durch technische Maßnahmen, um beiden Seiten (Sicherheitsbedürfnis des Betreibers und Wahrung der Persönlichkeitsrechte) hinreichend zu unterstützen. **Privacy by Default** und **Privacy by Design** im Sinne von Art. 25 DSGVO sind Grundlagen der Entwicklung.

Die TeamDrive Software und die Cloud Services basieren auf einer **Zero Knowledge Architektur**. Das bedeutet, dass der Service Anbieter (z.B. unsere Firma TeamDrive) und auch der Betreiber des Cloud Rechenzentrums niemals Einblick in die in TeamDrive gespeicherte Dokumente, Ordner Namen und andere Metadaten erhält. Alle Daten werden vor dem Hochladen in die Cloud beim Anwender verschlüsselt und der Anwender behält die Schlüssel. Diese Schlüssel werden niemals dem Serviceanbieter in lesbarer Form zugänglich gemacht. Diese Lösung wird **„Ende-zu-Ende-Verschlüsselung“** genannt. Weiterhin werden keine Informationen gespeichert, welche Personen Zugriff auf die jeweiligen verschlüsselten Daten haben. Zu Abrechnungs- und Verwaltungszwecken ist lediglich bekannt, wer den Space (Datenraum) angelegt hat und wer die Kosten hierfür übernimmt.

Alle TeamDrive Services sind auf eine minimale Datenspeicherung der Nutzerdaten konzipiert. Datensparsamkeit bedeutet das Server Logdaten nach kurzer Zeit gelöscht werden, kein Restore nach dem Löschen der Daten mehr möglich ist.

Das Produkt wird in einer datenschutzfreundlichen Voreinstellung ausgeliefert.
Bei der Anlage neuer Benutzer werden BSI-konforme Kennworte (siehe 9.weitere Dokumente) erzwungen.
Kennwortrichtlinien und Verschlüsselungsmodus sind im live-Betrieb weder vom Benutzer noch vom Administrator des Systems änderbar.

TeamDrive speichert alle Daten in Deutschland in ISO 27001 zertifizierten Rechenzentren ab. Sämtliche Anforderungen der DSGVO und von Berufsgeheimnisträgern gemäß § 203 Strafgesetzbuch (StGB) werden erfüllt. Für jeden zahlenden Kunden von TeamDrive halten wir einen Auftragsverarbeitungsvertrag bereit.
Soweit Berufsgeheimnisträger TeamDrive nutzen, ist die Nutzung regelmäßig auch nach den Vorgaben der DSGVO zulässig, zumal wir als Anbieter keine Kenntnis von den von Berufsgeheimnisträgern verarbeiteten Daten erhalten. Es findet insbesondere damit keine unbefugte Offenbarung i.S.d. § 203 StGB statt.

Wichtiger Hinweis: Neben den Konfigurationen und Sicherheitseinstellungen gemäß den Anforderungen der DSGVO, liegt in dem sorgfältigen Umgang mit den persönlichen Passworten, Sicherheitsschlüsseln und den Space Schlüsseln die persönliche Verantwortung.

3. Konfigurationseinstellungen (Defaults)

Alle im Folgenden beschriebenen Voreinstellungen können individuellen Anforderungen und Wünschen angepasst werden. Einige Anpassungen erfordern optionale Lizenzerweiterungen.

Jeder Nutzer von TeamDrive benötigt ein TeamDrive Benutzerkonto. Dazu benötigt jeder Benutzer eine Email Adresse. Diese dient zur Authentifizierung und für Benachrichtigungen. Seine Email Adresse kann jeder Benutzer selber ändern und sein Benutzerkonto kann jeder Benutzer selber löschen. Mit dem Löschen des Benutzerkontos werden sämtliche Daten des Benutzers gelöscht. Ausgenommen hiervon sind ausschließlich gesetzlich geforderte Daten, wie z.B. Angebote oder Rechnungen, die gemäß der Aufbewahrungsfristen nach deren Ablauf gelöscht werden.

TeamDrive Nutzer, die mit Hilfe einer selbstgehosteten Enterprise Installation angebunden sind, sind dem TeamDrive System nicht namentlich bekannt. (auch nicht die Email Adresse). Diese Nutzer werden über einen anonymisierten Hash verwaltet.

Jeder Benutzer benötigt ein Passwort mit einer Mindestlänge von 8 Zeichen. Eine Änderung des Passworts ist nur über eine Email Bestätigung oder Authentifizierung möglich. Neu installierte Endpoints (Client/Software Installationen) müssen durch einen Email Bestätigung aktiviert werden.

Jeder Nutzer kann einen Space anlegen. Ein Space ist in der Regel ein überwachter Ordner, deren Inhalte (Ordner und Dateien) verschlüsselt über die Cloud Services synchronisiert werden. Derjenige der einen Space anlegt ist der Administrator und Besitzer des Spaces. Nur er verfügt über die Schlüssel des Spaces. Diese werden lokal auf seinem Rechner gespeichert und mit seinen Credentials (Benutzername und Passwort) verschlüsselt in einer zentralen Schlüsselverwaltung (Key-Repository) hinterlegt. **Wenn der Benutzer sein Passwort vergisst, dann kann er seine Schlüssel aus der Schlüsselverwaltung nicht mehr entschlüsseln und riskiert einen Datenverlust.** Für den Fall das der Nutzer im laufenden Betrieb seines Clients das Passwort ändert, so werden seine Schlüssel mit dem neuen Passwort und seinen Credentials neu

in die Schlüsselverwaltung hochgeladen.

Die lokale Datenspeicherung ist bei den unterschiedlichen TeamDrive Clients unterschiedlich voreingestellt.

Desktop Clients (WIN/MAC/LINUX) : Vollständige Synchronisation aller Daten in das lokale Dateisystem.

Mobile Clients (IOS/ANDROID) : Nur die Metadaten, Verzeichnisnamen und Dateinamen werden heruntergeladen (Dateisystem) und angezeigt.

WebClient (HTML BROWSER) : Nur die Metadaten, Verzeichnisnamen und Dateinamen werden heruntergeladen (Datenbank) und angezeigt. Es werden niemals lesbare Daten im Docker Container gespeichert.

Diese Einstellungen können von dem Anwender individuell je Spaces geändert werde. So kann bei Bedarf die lokale Speicherung der Daten in den Desktop Clients ausgeschaltet werden. Oder in den Mobilen Clients eingeschaltet werden. Damit wird die offline Verfügbarkeit und die Nutzbarkeit der Daten ohne Internetverbindung beeinflusst.

In den Desktop Clients (WINDOWS/MAC) gibt es zusätzlich die Möglichkeit ein virtuelles Laufwerk zu konfigurieren. Damit kann der Anwender komfortabel wie im lokalen Dateisystem mit seinen Daten arbeiten, ohne das die Daten auf seinem Rechner dauerhaft gespeichert bleiben. Diese Einstellung ist sinnvoll wenn es sich bei den Daten in den Spaces um personenbezogene Daten handelt, die nicht verteilt auf verschiedenen Rechnern gespeichert werden dürfen und somit immer in der verschlüsselten Cloud verbleiben.

Die gewünschten Verhaltensweisen und Speicherorte können voreingestellt werden, so das die Datenhaltung immer automatisch den Anforderungen und Compliance Richtlinien genügt.

Spaces lassen sich bei der Space Anlage individuell konfigurieren. Dabei gibt es Konfigurationen die sich im Nachhinein nicht mehr ändern lassen. Hierzu zählen Funktionen wie die Überwachung von Aufbewahrungsfristen. Aufbewahrungsfristen lassen sich vom Administrator des Spaces nur verlängern und eine Löschsperre eines Spaces lässt sich nicht aufheben. In geforderten Fällen ist hier eine dokumentierte Neuanlage eines Spaces erforderlich. Auf diese Weise ist die Archivierung von Daten in den entsprechend konfigurierten TeamDrive Spaces **GoBD compliant**. Damit können Angebote, Rechnungen und andere finanzrelevante Unterlagen gemäß den Anforderungen der Finanzbehörden nach den Richtlinien der GoBD in TeamDrive gespeichert und archiviert werden.

Entsprechend konfiguriert, funktioniert die Arbeit mit TeamDrive überwiegend automatisiert. Der Anwender muss sich dann wenig mit Prozessen wie Datensicherung, Backups, Verschlüsselung etc. beschäftigen. Er kann bei Bedarf über jeden seiner Rechner oder Mobilen Endgeräte jederzeit und von jedem Ort aus sicher auf seine Daten zugreifen und an seinen Dokumenten arbeiten.

4. Datenschutzrichtlinien

Folgende Datenschutzrichtlinien müssen Sie als Anwender berücksichtigen, wenn Sie ihre Daten in TeamDrive speichern. Die folgenden Fragen müssen Sie für sich beantworten, wenn Sie mit personenbezogenen Daten arbeiten.

a) Rechtsgrundlage

Die Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 DSGVO zulässig:

- wenn eine Einwilligung der betroffenen Person vorliegt,
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
- zur Erfüllung einer rechtlichen Verpflichtung
- zum Schutze lebenswichtiger Interessen,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder
- aufgrund einer Interessenabwägung erforderlich ist.

Die Datenverarbeitung ist bereits dann rechtmäßig, wenn einer der genannten Tatbestände vorliegt.

b) Grundsätze der Datenverarbeitung

Nach Art. 5 DSGVO sind bei der Verarbeitung personenbezogener Daten folgende Grundsätze einzuhalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Näheres können Sie Art. 5 DSGVO entnehmen.

c) Datenlöschung

Die DSGVO verlangt eine sichere Datenlöschung.

Dieses wird durch TeamDrive sehr transparent abgebildet und in vorbildlicher Weise erfüllt. Löschprozesse können konfiguriert und automatisiert werden. Damit lässt sich das Vergessen von Löschanforderungen vermeiden.

Bitte beachten Sie auch das jede betroffene Person das Recht hat, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden.

d) Betroffenenrechte

Die Betroffenenrechte wurden durch die DSGVO gestärkt und beinhalten neben dem Recht auf Löschung personenbezogener Daten) insbesondere auch erweiterte Informationspflichten.

e) Test und Freigabe

Bitte denken Sie bei dem Einsatz von Datenverarbeitungssoftware immer daran, dass diese Software geeignet sein muss alle Anforderungen der DSGVO einzuhalten. Sprechen Sie mit Ihrem Datenschutzbeauftragten oder Verantwortlichen und lassen sich die Nutzung der Software freigeben.

5. Datenschutzfolgenabschätzung

Mit der DSGVO wird das Instrument der Datenschutz-Folgenabschätzung (DSFA) eingeführt (Art. 35 EU-DSGVO). Dabei handelt es sich um die Pflicht für den Verantwortlichen, vor Beginn einer geplanten Datenverarbeitung eine Abschätzung der Folgen vorzunehmen und zu dokumentieren. Grundsätzlich ist die Datenschutz-Folgenabschätzung immer dann durchzuführen, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Hier senkt TeamDrive die von Ihnen zu berücksichtigenden Risiken ganz erheblich, denn alle Daten, die Sie in TeamDrive speichern sind und bleiben immer hoch verschlüsselt. Die Verschlüsselung ist „State of the Art“ und selbst bei einem Datenleck im Rechenzentrum, in dem die Daten liegen, sind Sie aufgrund der hohen Verschlüsselung von der Meldepflicht befreit.

6. Verschlüsselungsmechanismen

TeamDrive verschlüsselt sämtliche Daten vor der Übertragung in die Cloud AES-256. Für die Übertragung wird zusätzlich das HTTPS/SSL Verfahren verwendet. Alle Mitteilungen und sonstigen Kommunikationen sind über ein Public/Private Key Verschlüsselungsverfahren gesichert.

Eine ausführliche Dokumentation aller verwendeter Schlüssel und Verfahren steht auf Anfrage als Dokument zur Verfügung.

7. Passwortrichtlinien

Sämtliche in TeamDrive benutzten Passworte den Anforderungen an den Stand der Technik genügen. Passworte müssen mindestens 8 Zeichen lang sein. Passworte können von Administratoren jederzeit zurückgesetzt werden. Damit werden die Nutzer gezwungen ein neues Passwort zu vergeben. Zu keiner Zeit werden Passworte irgendwo im Klartext übertragen oder gespeichert. Passwortänderungen benötigen immer einen zweiten Faktor (z.B. eine E-Mail Bestätigung). Es stehen optional 2-Faktor Authentifizierungen zur Verfügung und über das Software-Modul externe Authentifizierung können beliebige andere Authentifizierungsverfahren genutzt werden.

8. Technische und organisatorische Maßnahmen

TeamDrive trifft angemessene Maßnahmen, um den Schutz von Daten bei uns bzw. unseren Unterauftragsverarbeitern zu gewährleisten.

Treffen Sie bitte technische und organisatorische Maßnahmen für den Datenschutz im Umgang mit dem Produkt:

- Definieren Sie, welche Mitarbeiter für welche Vorgänge auf dem System berechtigt sind.
- Kontrollieren Sie die Einhaltung des Berechtigungskonzepts regelmäßig.
- Geben Sie keine Daten an unberechtigte Personen weiter.
- Achten Sie bitte darauf, dass Unbefugte keine Einsicht in Monitore erhalten, während Sie im System arbeiten.

- Sofern Sie externe Dienstleister für die Datenverarbeitung oder Wartung und Pflege der EDV einsetzen, kontrollieren Sie diese regelmäßig und nachweisbar auf Einhaltung des Datenschutzes.

Für den Fall das ein Client-Gerät (PC/SmartPhone/Tablet) auf dem TeamDrive installiert ist, als kompromittiert definiert wird, kann der Account Administrator einzelne Devices löschen (löschen und wipen). Damit werden die Schlüssel des Clients gelöscht und der Client nicht weiter synchronisieren. Sollte der Client online erreichbar sein, werden sämtliche TeamDrive Daten auf dem Client bei dem ersten Kontaktversuch gelöscht. Damit wird sichergestellt, dass verloren gegangene Rechner oder infizierte Systeme keinen Zugang mehr zu Space Inhalten erlangen können.

9. Auftragsverarbeitungsvertrag

Wir halten einen Auftragsverarbeitungsvertrag für Sie bereit. Diesen Vertrag können Sie mit TeamDrive auf einfache Weise in einem digitalen Prozess über unsere Webseite abschließen. Loggen Sie sich mit Ihrem Benutzernamen auf unserer Webseite ein. Dann finden Sie in Ihrem Benutzerkonto als Erstes den Punkt DSGVO. Dort können Sie durch Eingabe Ihrer Kunden- oder Rechnungsnummer und Vervollständigung der Vertragsdaten den Vertrag mit uns online abschließen. Sie erhalten Ihre Vertragskopie per PDF an die von Ihnen angegebenen E-Mail-Adresse.

10. Weitere Informationen zum Thema Datenschutz und Datensicherheit

https://privacy.teamdrive.net/de/index.html (TeamDrive Datenschutzhinweise)
https://teamdrive.com/datenschutzerklaerung/
https://teamdrive.com/zertifizierung/

**** Stand Dezember 2019 *****