Data protection information sheet for the use of TeamDrive

1. Introduction

Data security and data protection are areas with high relevance for every company, but equally important for every user or private person who works with data on the Internet. With this info sheet, we would like to provide you with necessary information and measures for handling data in connection with our TeamDrive product.

Data security, as part of IT security, is primarily about protecting data from unauthorised access and loss. Here TeamDrive offers the technical prerequisites to meet these requirements. However, the user himself must ensure that the correct settings and configurations are set according to his personal requirements.

Data protection is primarily concerned with the protection of personal data, which has been regulated in the Basic Data Protection Ordinance (GDPR) since May 2018. Any violation of the rules of the GDPR can be punished by the responsible authorities with heavy fines. In this information sheet we provide you with an overview of important questions, decisions and configurations that you should make yourself according to your requirements.

2. General principles

This document refers to data protection requirements which should be observed when using the "TeamDrive" product. This document is intended to serve as basic information for the application planning of a product such as "TeamDrive". The data protection laws and guidelines of the federal government and the respective federal states must also be observed.

TeamDrive supports data protection requirements with technical measures to adequately support both sides (security requirements of the operator and protection of personal rights). Privacy by Default and Privacy by Design in the sense of Art. 25 GDPR are the basis of the development.

The TeamDrive software and cloud services are based on a zero-knowledge architecture. This means that the service provider (e.g. our company TeamDrive) and the operator of the cloud data center never have access to the documents, folders, names and other metadata stored in TeamDrive. All data is encrypted before it is uploaded to the user's cloud and the user keeps the keys. These keys are never made readable to the service provider. This solution is called end-to-end encryption. Furthermore, no information is stored as to which persons have access to the encrypted data. For billing and administration purposes, only the person who created the space (data room) and who pays for it is known.

All TeamDrive services are designed for minimal data storage of user data. Data economy means that server log data is deleted after a short time, no restore is possible after the data has been deleted.

The product is delivered with a data protection-friendly default setting.

When creating new users, BSI-compliant passwords (see point 7.) are enforced.
Password policies and encryption mode cannot be changed by the user or the system administrator in live mode.

TeamDrive stores all data in Germany in ISO 27001 certified data centers. All requirements of the GDPR and of professional secrets according to § 203 of the German Criminal Code (StGB) are fulfilled. For each paying customer of TeamDrive we hold a data processing agreement.

If and to the extent to which TeamDrive is used by professionals bound to secrecy, its regular use is permissible in accordance with the provisions of the GDPR, particularly as we as the provider do not obtain any knowledge of the data processed by said professionals. In particular, no unauthorized disclosures as per the definition of § 203 StGB (German Criminal Code) take place.

Important note: In addition to the configurations and security settings in accordance with the requirements of the GDPR, personal responsibility lies in the careful handling of personal passwords, security keys and space keys.

3. Configuration settings (defaults)

All presettings described in the following can be adapted to individual requirements and wishes. Some adjustments require optional license extensions.

Every TeamDrive user requires a TeamDrive user account. Each user needs an email address for this. This is used for authentication and notifications. Each user can change their email address themselves and delete their user account themselves. With the deletion of the user account all data of the user are deleted.
Excluded from this are only legally required data, such as offers or invoices, which are deleted in accordance with the retention periods after their expiration.

TeamDrive users who are connected by means of a self-hosted Enterprise Installation are not known by name to the TeamDrive system. (not even the email address). These users are managed via an anonymous hash.

Each user requires a password with a minimum length of 8 characters. Changing the password is only possible via email confirmation or authentication. Newly installed endpoints (client/software installations) must be activated by an email confirmation.

Each user can create a space. A space is usually a monitored folder whose contents (folders and files) are encrypted before synced and synchronized via cloud services. The person who creates a space is the administrator and owner of the space. Only this administrator has the keys of the space. These are stored locally on his computer and encrypted with his credentials (user name and password) in a central key repository. If the user forgets his password, he can no longer decrypt his keys from the key management and risks data loss. In case the user changes the password while his client is running, his keys will be uploaded to the key management with the new password and credentials.

The local data storage is preset differently for the different TeamDrive clients.

Desktop Clients (WIN/MAC/LINUX) : Complete synchronization of all data in the local file system.

Mobile Clients (IOS/ANDROID) : Only the metadata, directory names and file names are downloaded (file system) and displayed.

WebClient (HTML BROWSER) : Only the metadata, directory names and file names are downloaded (database) and displayed. No readable data is ever stored in the Docker Container.

These settings can be changed by the user individually for each space. If necessary, the local storage of data in the desktop clients can be switched off. Or be switched on in the Mobile Clients. This influences the offline availability and usability of the data without an Internet connection.

In the Desktop Clients (WINDOWS/MAC) there is also the possibility to configure a virtual drive. This allows the user to work comfortably with his data as in the local file system, without the data remaining permanently stored on his computer. This setting makes sense if the data in the spaces is personal data that may not be stored distributed on different computers and therefore always remain in the encrypted cloud.

The desired behavior and storage locations can be preset so that the data storage always automatically meets the requirements and compliance guidelines.

Each local TeamDrive installation is deeply connected to the logged-in Windows/Mac/Linux user account. This is done because TeamDrive connects to this account for monitoring local data. Therefore it is not possible to change TeamDrive user by logout. However, the local TeamDrive application can be additionally secured via the application protection, using the user password or a 6-digit PIN code, at start of the application or a defined idle time.

Spaces can be individually configured at time of space creation. There are configurations that cannot be changed afterwards. These include functions such as the monitoring of retention periods. Retention periods can only be extended by the space administrator and a deletion block for a space cannot be removed. In required cases, a documented new creation of a space is necessary. In this way, the archiving of data in the appropriately configured TeamDrive Space is GoBD compliant. This means that offers, invoices and other financially relevant documents can be stored and archived in TeamDrive in accordance with the requirements of the financial authorities and the GoBD guidelines.

Configured accordingly, working with TeamDrive is largely automated. The user then has little to do with processes such as data backup, backups, encryption, etc. If required, he can securely access his data and work on his documents at any time and from any location via any of his computers or mobile end devices.

4. Privacy Policy

As a user, you must observe the following data protection guidelines when storing your data in TeamDrive. If you work with personal data, you must answer the following questions for yourself.

a) Legal basis

The processing of personal data is permitted pursuant to Art. 6 para. 1 GDPR:

- if the consent of the data subject has been obtained,
- for the fulfilment of a contract or for the implementation of pre-contractual measures,
- to fulfil a legal obligation
- to protect vital interests,

- to perform a task carried out in the public interest or in the exercise of official authority, or
- is necessary due to a balancing of interests.

Data processing is already lawful if one of the aforementioned facts is present.

b) Principles of data processing

According to Art. 5 GDPR, the following principles must be observed when processing personal data:

-Legality, good faith, transparency
-earmarking
-data minimization
-correctness
-memory limit
-Integrity and confidentiality

You can find more details in Art. 5 GDPR.

c) Data deletion

The GDPR requires secure data deletion.

This is mapped very transparently by TeamDrive and fulfilled in an exemplary manner. Deletion processes can be configured and automated. This prevents deletion requests from being forgotten.

Please also note that every person concerned has the right to demand that the person responsible delete personal data relating to them immediately.

d) User rights

The rights of users have been strengthened by the GDPR and, in addition to the right to delete personal data, also include extended information obligations.

e) Testing and release

When using data processing software, please always remember that this software must be suitable to comply with all requirements of the GDPR. Talk to your data protection officer or responsible person and obtain permission to use the software.

5. Data protection impact assessment

The GDPR introduces the instrument of data protection impact assessment (Art. 35 EU-GDPR). This is the obligation for the person responsible to carry out and document an assessment of the consequences before starting a planned data processing.
In principle, the data protection impact assessment must always be carried out if the processing is likely to entail a high risk for the rights and freedoms of natural persons.

Here TeamDrive considerably reduces the risks you have to take into account, because all data that you store in TeamDrive is and always remains highly encrypted. Encryption is "state of the art" and even if there is a data leak in the data centre where the data is stored, you are released from the reporting obligation due to the high level of encryption.

6. Encryption mechanisms

TeamDrive encrypts all data before it is transferred to the cloud AES-256 using the HTTPS/SSL method. All messages and other communications are secured by a public/private key encryption procedure.

Detailed documentation of all keys and procedures used is available as a document on request.

7. Password policies

All passwords used in TeamDrive meet the requirements of state-of-the-art technology. Passwords must be at least 8 characters long. Passwords can be reset by administrators at any time. This forces users to assign a new password. At no time will passwords be transmitted or stored anywhere in plain text. Password changes always require a second factor (e.g. an email confirmation). Optional 2-factor authentications are available and via the software module external authentication any other authentication method can be used.

8. Technical and organisational measures

TeamDrive takes appropriate measures to ensure the protection of data by us or our subcontractors.

Yourself please take technical and organizational measures for data protection in handling the product:

- Define which employees are authorized for which processes on the system.
- Check compliance with the authorization concept on a regular basis.
- Do not pass on any data to unauthorized persons.
- Please make sure that unauthorized persons do not gain access to monitors while you are working in the system.
- If you use external service providers for data processing or maintenance and care of the EDP, check these regularly and verifiably for compliance with data protection.
- End devices (PC/SmartPhone/Tablet) on which TeamDrive is installed must meet the requirements of the “IT-Gundschutz by BSI”. In particular, it is important to ensure that the end device has up-to-date virus protection and sufficient password protection.

In the event that a client device (PC/SmartPhone/Tablet) with TeamDrive installed will be defined as compromised, the account administrator can delete (delete and wipe) individual devices. This deletes the client's keys and stops the client from synchronizing. If the client can be reached online, all TeamDrive data on the client will be deleted at the first contact attempt. This ensures that lost computers or infected systems can no longer gain access to space content.

Translated with www.DeepL.com/Translator (free version)

9. Data processing contract

We have a data processing contract ready for you. You can easily conclude this contract with TeamDrive in a digital process via our website. Log in to our website with your user name. Then you will first find the GDPR item in your user account. There you can conclude the contract with us online by entering your customer or invoice number and completing the contract data. You will receive your contract copy in PDF format to the email address you provided.

10. Further information about data protection and data security

https://privacy.teamdrive.net/en/index.html (TeamDrive Privacy Policy)
https://teamdrive.com/en/privacy-policy/
https://teamdrive.com/en/certification/

**** as of January 2023 *****