# Service description & additional terms and conditions
## VERSIEGELTE CLOUD

**Last revised:** March 19, 2018

# PUBLICATION DETAILS

**Published by**

**Telekom Deutschland GmbH**

**Landgrabenweg 151**

**53227 Bonn**

**WEEE-Reg.-Nr. DE60800328**

**hereinafter referred to as "Telekom"**

https://www.telekom.de/compulsory-statement

# Contents



# 1 Introduction

„Versiegelte Cloud“ consists of Telekom providing the customer with an SaaS solution in the form of virtual project spaces (privacy boxes and data rooms) along with sealed communication options.

The solution makes it possible for a number of users authorized to use the project rooms to meet in these spaces to exchange documents and information, and to work together on projects. „Versiegelte Cloud“ technology includes automated key management, thereby preventing access by unauthorized persons. While its security standard is very high, the system is nevertheless very easy to use.

# 2 Services provided by Telekom

## 2.1 Provision of the service

The customer can choose from a range of service packages. A given package consists of a number of full licenses, guest licenses, and memory blocks. The type of license defines the range of functions allocated to a given user. Please see the glossary for details.

When the customer places its order, it receives an activation link by e-mail. The service is available from the moment when the administrator named by the customer receives the e-mail with the activation link (date of provision).

The customer then uses this link to complete the registration process independently. As part of the process, the administrator named by the customer selects a user name (administrator ID) and password that only he/she knows. Telekom does not save this user name and password.
For security reasons, Telekom does not receive these details and is unable to reconstruct them. In other words, Telekom has no means of resetting the administrator's user name and password. The customer cannot access its account without these details, so the administrator should store his/her ID, password, and PUK (password unlocking key) in a secret and very secure location.

The customer or its administrator can create other users who complete their own registration in turn. Details about the given roles and rights are available in the glossary.

## 2.2 Operation, service, service quality

## 2.3 Operation

Telekom provides the customer with access to the „Versiegelte Cloud“ as an SAAS. The solution is operated from a data center located in Germany.

## 2.4 Service

The customer can address their support requests concerning „Versiegelte Cloud“ functions and disruptions directly to the Telekom support team (service desk). This service is available Monday to Friday, from 8:00 a.m. to 8:00 p.m. (excl. public holidays for all of Germany). The support team can help clarify issues relating to how to use the service. However, they cannot function as administrators and access customer data, as they have no access to data in the „Versiegelte Cloud“ for security reasons.

## 2.5 Service quality

The following service parameters apply to the „Versiegelte Cloud“:

| Objective | Values/timeframe |
|---|---|
| **Availability** | There is no minimum availability. Telekom will work to ensure that restrictions on availability are kept to a minimum. |
| **Operating hours** | Monday – Sunday, 24/7, excl. maintenance windows |

| | |
|---|---|
| **Disruption notification by e-mail** | Monday – Sunday, 24/7 |
| **Disruption notification via service desk** | Monday - Friday (excl. public holidays for all of Germany)<br>8:00 a.m. to 8:00 p.m. |

## 2.6 Functions

## 2.7 General functions of „Versiegelte Cloud“

„Versiegelte Cloud“ is a web service that protects and simplifies digital communication and collaboration between the customer and its partners.
The customer and authorized users can do the following:

- Create virtual project rooms
- Exchange documents in the virtual project rooms
- Work on documents together
- Exchange information
- Chat

A multi-level rights management system is part of the service. This system can be used to define what users are authorized to perform what actions.
Details are available in the user manual that customers can access as part of „Versiegelte Cloud“ help function.

## 2.8 Access to project rooms

Access to the project rooms via the internet (app or browser) is encrypted. Smartphones operating either Android or iOS can be used for access via mobile end devices. The customer's users download the app themselves from the Google® Play Store or the Apple® App Store, depending on their operating system. The customer can negotiate with Telekom to agree other, customized access options.

## 2.9 Security

Patented sealed cloud technology is used in Europe, the USA and China. It takes into account the technical and operational conditions and ensures that the data added by the customer remains inaccessible (known as the computer center's "technical seal").
The technological solution is designed in such a manner that the computer center operator cannot access any customer data. This technology protects the data during processing. Telekom has no access to the keys. Telekom employees can only access the application server again when it no longer contains any information. The data is encrypted right from the moment that the customer transfers it to the computer center that hosts the data.

Only the customer and its users are responsible for protecting the usage rights, access rights and passwords allocated to the administrator and users. Only the customer and its users are responsible for ensuring that these details are not forwarded to unauthorized users. Responsibility for accessing, changing, or downloading data stored by the customer in the project room, and responsibility for issuing authorization lie with the customer's users, i.e. with the customer's administrator at first and then with anyone receiving authorization from him/her.

## 2.10 Privacy boxes

The customer can create its own storage sites for files of all kinds and notifications in privacy boxes. Only the user and other users that he/she invites thanks to his/her authorizations can access these storage spaces.

## 2.11 Productivity tool

The productivity tool is a means of automatically synchronizing the privacy boxes in „Versiegelte Cloud" and the file system on a given user's local hard drive. The function is part of the user's Windows Explorer.
The user can use this tool to lock documents with a single click and so prevent other users from modifying them. Users can also exclude certain privacy boxes from the synchronization process.

## 2.12 Optional services

In the case of a separate order, the following optional services are provided for an additional charge.

## 2.13 Audit-proof data rooms

Audit-proof data rooms are privacy boxes with special functions. The contain a logbook that can be used for documenting the user's actions (uploads, downloads, document views, deleting, etc.) and for undertaking steps to prevent documents from being dissemination (watermark, etc.).
The following functions for strengthening protection against document dissemination are in place for the data rooms.

- When a user downloads a file, the system adds a watermark that provides information about the user's name and when (date and time) the download occurred (only for PDFs).
- Document usage can be restricted to on-screen viewing only (only for PDFs).
- An alarm is triggered if a user exceeds his/her number of permitted downloads during a specified period, i.e. the system registers irregular user activity and displays this in the logbook.

The above-mentioned functions help to make it more difficult to disseminate documents, but they cannot completely prevent it.
For operational reasons, there is a delay of a few minutes between an action and its registration in the logbook. The logbook normally lists every action, but in very specific technical conditions, information about a given action can be mislaid.
Every privacy box can be transformed into a data room.

## 2.14 Additional users and storage

The customer can add additional full licenses, guest licenses, and more storage to every service package.

## 2.15 Two-factor authentication

To enhance log-in security, it is possible to activate a two-factor authentication process. In this case, logging in requires not just the customer's specific password, but it also needs a PIN which the user receives by text message (for a fee).

## 2.16 Changes in favor of the customer

Telekom reserves the right to make unilateral changes to the service and to reduce charges in favor of the customer. The customer agrees to these adjustments in advance when signing the agreement. In an exception from the requirement to communicate in writing, Telekom informs the customer by e-mail. The new documents issued this way replace existing documents.

# 3 Services to be provided by the customer

The customer undertakes to perform all duties to cooperate required for the proper provision of services and, in particular, the following ones at no charge, in good time, and to the extent required.

a. The customer assures that it will not store any content on the contractual storage space and make available online, if the provision, publication, or use of such content violates applicable laws or third-party rights – this applies in particular to defamatory, hatred-inciting, or extreme right-wing content. The customer ensures that it has the rights to save and edit its data in the project room.

b. The customer refrains from actions that could endanger or disrupt the services of third parties or to Telekom's infrastructure (e.g. due to a DDoS attack). In such a situation, Telekom is entitled to deactivate the service concerned, without prior notification of the customer, until the risk or impairment has been remedied. This also applies if the customer uses, saves on the contractual storage space, or in any other way makes accessible any content that contains malicious codes or other malware. Further claims by Telekom shall not be affected by such a situation. Telekom provides the customer with information about relevant incidents and measures to the greatest extent possible.

c. The customer is responsible for checking and ensuring compliance with any and all legal provisions, laws, regulations, and industry-specific provisions that are relevant and applicable in connection with the use of the service. This particularly also includes compliance with confidentiality obligations, for example those resulting from a professional activity. The customer confirms that data of relevance to confidentiality or persons will only be stored where there is an effective approval.

d. The customer's users are obligated to exchange data solely in a manner compliant with the usage and acknowledgement of standards in line with the internet http/https protocol. The customer may only use interfaces recognized as standard or defined by Telekom. Exceptions require written consent.

e. The customer declares that it agrees to exchange information by e-mail and will always provide a current e-mail address. The customer is aware and authorizes that essential information for service provision, such as access data, information on modifications to the services and the legal conditions, etc., shall only be sent by e-mail.

f. The customer is obligated to back up its data at adequate intervals and in a suitable form on other systems of its own so that such data can be recovered at a reasonable cost. Telekom does not back up data. For this reason, the customer should, in its own interests, transfer its data to other systems in a suitable form by the contract's expiry date at the latest.

# 4 Commercial conditions, contract termination

The customer books a basic package that contains a certain number of full and guest licenses in addition to memory blocks. At a later date, the customer can book additional full and guest licenses or options mentioned above for a separate fee.

For an additional fee, the customer can book additional storage for its package (optional service). The storage volume (plus storage volume booked as an optional addition) is available for use by all of the customer's privacy boxes or data rooms.
The contract is concluded for a term of one month, authoritatively for the beginning of the month term is the date of registration. The fixed term is automatically extended by one month if neither party terminates the contract at least one month before the authoritative fixed term is due to expire (by the customer via cloud-portal per button in the area of contract management or by Telekom by sending an e-mail to the given e-mail address of the customer). The customer can change in each case to the end of the fixed term between the offered packages.

The general terms and conditions of Telekom Deutschland GmbH are valid for IT achievements, available under https://cloud.telekom.de/agb as well as on the website https://cloud.telekom.de/magenta-security/versiegelte-cloud available price sheet.

# 5 Data collection on the contract's expiry date

The customer is responsible for remotely transferring its data from the project room to another means of storage at its disposal when the contract expires. In its own interests, the customer should therefore select the termination date in such a manner that it still has time to collect data while the contract is still in force. All data within the „Versiegelte Cloud“ is deleted when the contract expires.

# 6 Glossary

| | |
|---|---|
| **SaaS** | Software as a Service |
| **DDoS** | Distributed Denial of Service |
| **Privacy box** | • Confidential project workspace with file storage, notes, and chat functions.<br>• Privacy boxes behave like network drives. Access does not require software to be installed. Instead, it uses all modern browsers or WebDAV, Windows client, or mobile apps (iOS, Android).<br>• Only users invited by the box's creator have access to a box. |
| **Data room** | • A data room has the same features as a privacy box but has additional functions as well, e.g. logbook and anti-dissemination protection. |
| **Project room** | • Superordinate term for the data room/s and privacy box/es used by the customer. |
| **Full license** | • A licenses allocated to a member of the customer's workforce.<br>• User rights:<br>o Creating privacy boxes (currently up to 2,000 boxes per package)<br>o Uploading and downloading documents<br>o Writing notes, chatting<br>o Issuing guest licenses |
| **Full license with administrator role** | • The first user automatically has the role of administrator for the entire term.<br>• Every full license can contain the administrator role. We recommend naming two additional administrators along with the registering (i.e. initial) administrator.<br>• The administrator assumes additional administrative functions.<br>• User rights:<br>o Issuing additional administrator roles<br>o Issuing full and guest licenses (i.e. allocating booked full and guest licenses to employees or people outside the company) |

| | |
|---|---|
| **Guest license** | • Guest licenses are intended for external users.<br>• They can be assigned on a permanent or temporary basis. After 30 days of inactivity, temporary licenses lapse and are sent back to the pool of guest licenses.<br>• Guest license users can made into members of privacy boxes or be invited to become members.<br>• User rights:<br>  o Uploading and downloading documents<br>  o Writing notes, chatting<br>• Guest license users cannot create privacy boxes or invite other guests |
| **One-off read-only access (free)** | • One-off read-only access can only be issued by the owner of the project room in question.<br>• Authorization is issued via a link that can be protected with a passcode.<br>• This option makes it possible to download documents without a guest license, i.e. free of charge.<br>• By sending someone the link and passcode, the sender provides access to the project room in question. For this reason, Telekom bears no responsibility if the person receiving access data for read-only access forwards this information to unauthorized persons. |
| **User** | This term covers all users in general:<br>• Users with administrative role<br>• Users with full licenses<br>• Users with guest licenses<br>• Users with one-off read-only access |