Cloud Privacy and compliance as a Managed Service

T-Systems Cloud Privacy Service Ensure GDPR compliance for usage of public cloud and Office365

Ensure compliance and retain your investment in public cloud without worrying about Privacy Shield cancellation

The latest GDPR compliance rules in the EU have put many companies' investment in public clouds, including Office 365 in doubt. Transfer of personal user specific data to US based clouds is now in breach of the strict data privacy rules. T Systems' 'Cloud Privacy Service' allows organizations to encrypt their data while using Microsoft 365 services, and other public cloud SaaS environments.

T-Systems offers the encryption gateway as a managed service including the key management and backup, which is crucial aspect. This allows you to take advantage of the full solution without the need for lengthy internal set up or upskilling your team.

Stepping into the future with a Secure Cloud Gateway

With Cloud Privacy Service for Collaboration 365, T- Systems' and technology partner eperi, offer a service which enables companies to store encrypted data in 1 Microsoft 365 Services in a way that only they should be able to access, the plain text data, or prevent third party access as far as possible.

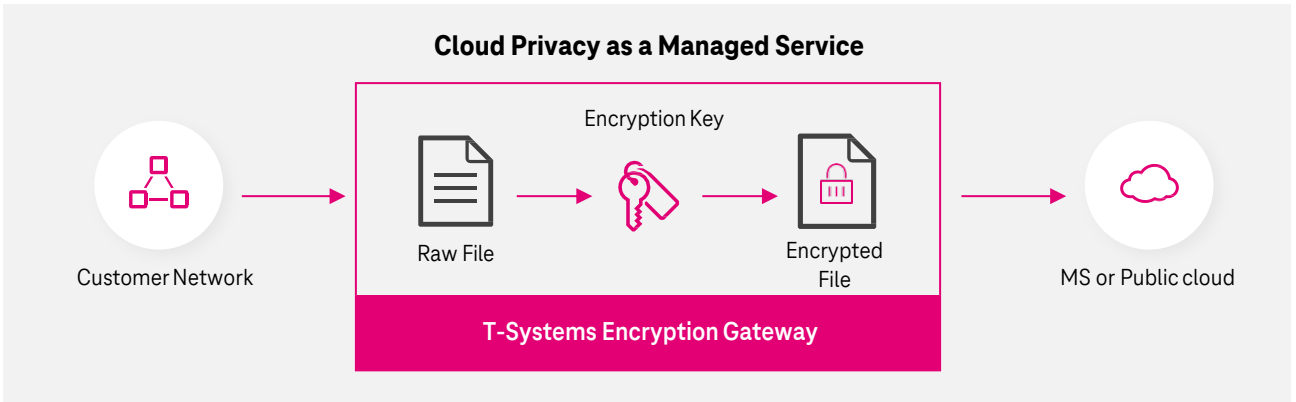
The solution is offered as a managed service and supports Microsoft 365 services including:

- Microsoft Teams
- SharePoint Online
- Exchange Online

The service also supports the 'search functionality' for the plain text to make data management easier.

Encryption Gateway and its functionality

The Cloud Privacy Service is logically located between the customers network and the Microsoft 365 cloud. The incoming traffic will be encrypted according the configuration of the gateway so that only encrypted data is stored in MS365. When data is read from MS365 the gateway decrypts this data so that it is readable and searchable in plaintext for users. For this purpose, the Cloud Privacy Service generates 10,000 AES encryption keys with an encryption depth of 256 bits, which are used randomly to encrypt the data. The keys are stored encrypted in the Telekom data center.



T Systems Let's power higher performance

Encryption of Microsoft Teams Data

The encryption gateway encrypts the following content when accessing Microsoft teams through the gateway:

- Messages sent by users within the Teams environment to other users or teams (chats)
- Files that are attached to messages by users
- Content metadata such as file properties
- Connection metadata such as call lists

Encryption of SharePoint Online Data

The encryption gateway encrypts the following content when SharePoint Online is accessed through the gateway:

- Files that are uploaded to Mysites via the web front-end or synchronized to SharePoint Online from the user's end device via the OneDrive for Business Client
- Files that are stored in SharePoint lists.
- Content metadata such as file properties or change history
- SharePoint lists and list entries

Encryption of Exchange Online Data

The encryption gateway encrypts the following content when Exchange Online is accessed through the gateway:

- Message body, subject and attachments of e-mails delivered to Exchange Online via SMTP using the encryption gateway
- Message body, subject and attachments of items in draft and sent items
- Calendar entries
- Contacts

Search Index feature

The encryption gateway creates a search index of the encrypted data and makes it available to the user via the corresponding search functionalities.

Office Online Server

Telekom installs and configures an Office Online Server to enable the preview of encrypted Office documents when using SharePoint Online via the web interface. This includes all necessary infrastructure components.

Customer Value

- Smoothly, securely and affordably into the public cloud
- Use Microsoft or Googles Cloud Services respective to European privacy requirements
- Encryption as a dedicated Service hosted in T-Systems Data Center
- 99.9 % approx. – technical service level.
- Central Key Management
- BSI, GDPR compliance

Additional benefits

01 Use American or other hyperscalers outside the EU with confidence

02 Data will be encrypted before it is stored in US based clouds

03 Solid secure cloud management with deep knowledge of European regulations, privacy and security requirement

04 Other additional benefits like backup and transfer of encryption key available on demand

Optional Services

01 Hardware Security Module – The keys for Encryption are stored in a dedicated hardware security module

02 Customer provided Encryption keys – We can import customer-supplied encryption keys for use by the Encryption Gateway for encryption and decryption*

03 Encryption and Decryption of large amounts of data

04 Key handover to Customer – We support in creation of the encryption keys and later submit these to the customer

In this case, Telekom does not generate keys, or deletes the keys generated during initial deployment

Contact
www.t-systems.com/contact
00800 33 090300
E-Mail: info@t-systems.com

Published by
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany

T Systems Let's power higher performance