# Microsoft Cloud Germany

*Compliance in the cloud for organizations in EU/EFTA*

# Disclaimer

Published September 2016



# Acknowledgements

Authors:
Frank Simorjay

Reviewers:
Pradeep Ayyappan Nair
Yen-Ming Chen
Markus Feichtner
Rainer Strassner
Ralf Wigand
Paul Henry (Wadeware)

# Executive summary

Microsoft is committed to protecting the security, privacy, and integrity of sensitive customer data for all its cloud-based services, including Azure. As Brad Smith - President and Chief Legal Officer stated, "As a global company we've long recognized that if people around the world are to trust the technology they use, they need to have confidence that their personal information will be protected by the laws of their own country."

Thus, Microsoft created the Microsoft Cloud Germany for commercial customers in the European Union (EU) and European Free Trade Association (EFTA). Customer now can store and manage customer data in compliance with applicable German laws and regulations as well as key international standards, using the Microsoft developed data trustee model that provides, and enables European customers to move to the cloud.

## Table of Contents

# Establishing trust for Microsoft cloud customers in Germany

Microsoft understands that for its enterprise customers to realize the benefits of cloud computing, they must be willing to entrust their cloud services provider with one of their most valuable assets—their data. Although Microsoft cloud services are global in scope, they recognize that a one-size-fits-all solution can't work for everyone.

To help meet the needs of customers and prospective customers in the European Union (EU) and European Free Trade Association (EFTA), who have expressed concern about the security and privacy of their online data in a digital world, Microsoft has developed Microsoft Cloud Germany: a separate instance of Microsoft industry-leading enterprise cloud services hosted and operated entirely within Germany, with special protections built in to help assure customers that their data will remain there with access controlled by a local company. This paper explains what Microsoft Cloud Germany is, how it is different from and similar to Microsoft cloud services worldwide, and how the data trustee model provides both technical and legal protection for customer data.

## Microsoft cloud principles of trust

Protecting the security, privacy, and integrity of sensitive customer data—not only from malicious attackers but also from demands made by governments and other parties—is one of Microsoft's highest priorities. The Microsoft Trust Center (www.microsoft.com/TrustCenter) lists a number of underlying principles that guide the way Microsoft cloud services are built and operated, including:

- Security: Customers must be able to count on their data remaining secure from threats. Security is built into Microsoft cloud services from the ground up, starting with the Security Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process. Microsoft engineers help ensure that Microsoft cloud services are protected at the physical, network, host, application, and data layers so that all services are resilient to attack. Continuous proactive monitoring, penetration testing, and the application of rigorous security guidelines and operational processes further increase the level of detection and protection throughout Microsoft cloud services.
- Privacy: Customers must be able to trust that the privacy of their data will be protected and that it will be used only in ways that are consistent with their expectations. The Microsoft Online Services Privacy Statement describes the specific privacy policy and practices that pertain to customer data in Microsoft enterprise cloud services. Microsoft was also the first major cloud provider to adopt the first international code of practice for cloud privacy, ISO/IEC 27018.
- Transparency: Customers should know as much as possible about how their data is handled and to whom it is disclosed. Microsoft provides a wide range of evidence, including third-party audit reports and certifications for most services, to verify that Microsoft meets the standards it sets for itself. The Microsoft Transparency Hub (https://www.microsoft.com/about/csr/transparencyhub/) provides extensive information and statistics about how Microsoft has responded to law enforcement requests, US national security orders, and content removal requests.

- Compliance: Microsoft is committed to respecting and accommodating regional regulatory standards. To help organizations comply with national, regional, and industry-specific requirements that govern the collection and use of individuals' data, Microsoft offers the most comprehensive set of certifications and attestations of any cloud service provider.

## Goals

A trustworthy cloud solution for German, European Union (EU) and European Free Trade Association (EFTA) region customers is one that meets the following goals:

- It should host customer data entirely within the German, European Union (EU) and European Free Trade Association (EFTA) region. This goal requires establishing an entirely separate instance of Microsoft cloud services for Germany with its own locally hosted infrastructure for support, backup, high availability, and disaster recovery.
- It should provide a secure and trustworthy solution for cross-border maintenance and service, which enables Microsoft employees and contractors located outside of Germany, or European Union (EU) and European Free Trade Association (EFTA) regions, to perform necessary tasks without putting customer data at risk.
- It should enable Microsoft to provide its German, European Union (EU) and European Free Trade Association (EFTA) region customers with high quality services that leverage the advantages of Microsoft cloud services without adding onerous restrictions.
- It should comply with all relevant German, European, and international standards for privacy, security, and transparency.

# The data trustee model

To meet these goals, Microsoft created a data trustee model that delivers the power and flexibility of Microsoft cloud services in an environment that provides both technical and legal protections for German customer data. With the data trustee model, all data that belongs to German, European Union (EU) and European Free Trade Association (EFTA) region customers is stored exclusively in datacenters on German soil, and a third party—the data trustee—controls all access to customer data and any associated infrastructure. Microsoft Cloud Germany has contracted with T-Systems, a subsidiary of Deutsche Telekom, to serve as the data trustee.

## What is it?

The data trustee model fulfills the goal of providing country-specific datacenter locations over which non-domestic entities are proven to exercise no control. To create the physical and logical infrastructure separation required to enable the data trustee model, Microsoft has implemented a separate and isolated instance of Microsoft Azure, Microsoft Office 365, and Microsoft Dynamics 365 Online services located entirely within Germany. All customer data is stored in two datacenters in two German cities, Frankfurt and Magdeburg, ensuring that customer data remains within the country. The datacenters are connected by a dedicated network that prevents data from traveling over the public Internet when it is transferred from one datacenter to the other for backup or other purposes. Likewise, the technical staff that manages the service works within

operations centers located within two German cities, Magdeburg and Berlin. Any operational activities performed by Microsoft that could potentially enable access to customer data—such as incident management and software updates—are subject to technical controls that require the German data trustee's explicit approval and supervision.

# How does the trustee model work?

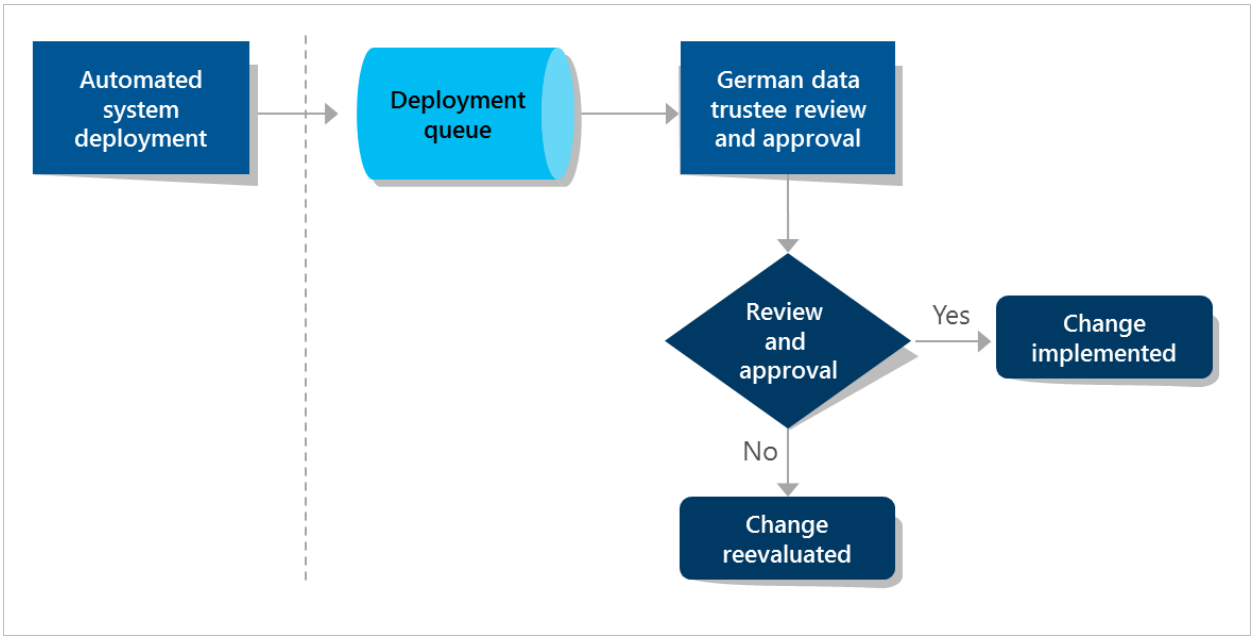
The data trustee controls access to customer data by implementing role-based access control (RBAC) tools that allow it to identify and control access privileges for each service team's personnel. The combination of these tools and the physical and logical segregation of systems and data inside Germany give the data trustee the technical capability to control all access to customer data, other than that initiated by the customer or its end users themselves. Under normal operating conditions, therefore, Microsoft has no access to German customer data.

## Process

Any requests by Microsoft to access systems that hold customer data must go through the following approval process:

1. Microsoft makes a request for access based on a specific need (for example, troubleshooting that cannot be resolved by the data trustee).
2. The data trustee verifies that the request is for a permitted purpose.
3. The data trustee grants access, scoped to a specific service and only for the time necessary to accomplish the permitted purpose. During access, Microsoft personnel have their activities logged and monitored by the data trustee.
4. Upon completion of the task, access terminates. If more time is needed, Microsoft personnel must obtain new approval.

This process helps ensure that customer data is protected even during routine tasks such as rebooting a server or installing software updates. To facilitate maintenance of the Microsoft Cloud Germany infrastructure, Microsoft has developed processes for automating routine tasks that do not require access to customer data. In such cases, Microsoft engineers generate an automated system deployment request and load it into a deployment queue for review by the data trustee. If the data trustee approves the request, Microsoft engineers use automated tools to implement the change.




*Approval process for Microsoft to access Microsoft Cloud Germany systems that hold customer data*

For the rare requests that require that Microsoft be granted access to systems processing customer data, the data trustee contractually commits to customers that it will provide access under the following conditions:

- The data trustee grants Microsoft temporary access to resolve a customer support problem or perform maintenance or improvements. In such circumstances the data trustee monitors the session until the issue is resolved.
- The customer requests assistance, and the customer chooses to share customer data with Microsoft for assistance with resolving a customer support incident. In such circumstances, the customer—not the data trustee—controls what customer data is shared[1].

## Methods

When a properly logged incident or system update is required by a Microsoft engineers they can start one of two types of access processes.

### Least privilege access

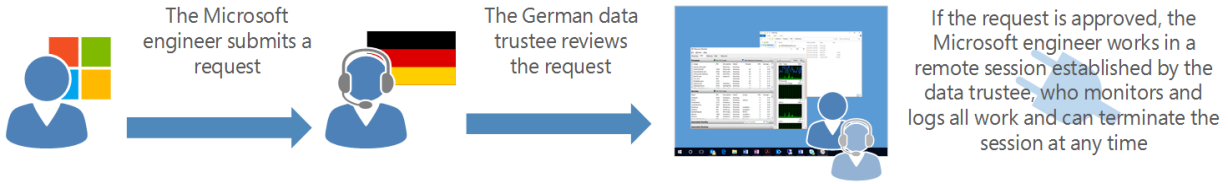
In the least privilege access model, a Microsoft engineers receives least-privilege access to perform a specific operations task for a limited amount of time. The trustee receives logs for all access approvals as well as task operations. Upon expiration of the time period allotted for the task, access expires. If more time is required for the task, Microsoft must submit a separate request to have the time period extended. The trustee is always in control of access and can choose to modify the time period or privileges granted at its discretion.

[1] This condition also applies to scenarios in which a customer has purchased service from Microsoft Cloud Germany through a cloud service provider (CSP), in which case the CSP normally has administrative access to customer data and may escalate a customer support incident to Microsoft itself. Customers should consult their CSP agreement for specific details.


### Escort model

The escort model is used for complex incidents that may involve some degree of troubleshooting or other tasks that may not be known ahead of time. In such cases, the trustee provides Microsoft engineers with supervised access to the appropriate systems and monitors all progress to ensure that no customer data is extracted without approval.

This escort scenario, a trustee engineer connects to a session and invites the Microsoft engineer to shadow the session. The trustee engineer then establishes a remote connection to the system and grants access and control to the Microsoft engineer. The trustee engineer continues to supervise the entire session remotely as the developer performs the permitted tasks.




In certain circumstances, Microsoft may need to be physically present at a Microsoft Cloud Germany datacenter to take action. If the data trustee approves such a request, the Microsoft engineer receives a physical escort to the facility from a representative of the data trustee, who monitors all of the engineer's activities in person and ensures that customer data remains safe.

## Trustee's roles and responsibilities

As detailed earlier, the data trustee controls access to customer data by anyone except the customer or the customer's end users. This control means that operational tasks that require access to customer data or the infrastructure on which customer data resides will be performed or supervised by the data trustee, or else directly by the customer.

Additional tasks the Data Trustee may perform include but are not limited to:

### Incident management

- Monitoring for incoming platform incidents, support incidents, deployment incidents, and service requests
- Triaging incoming incidents by assessing business impact
- Reporting the health of Microsoft Cloud Germany services and operational processes upon request
- Assisting in outage restoration actions

### Network management

- Maintaining the network infrastructure

- Performing system and software updates/upgrades in accordance with guidance from Microsoft teams
- Routinely validating system logging accuracy

### Datacenter management

- Providing on-site support for systems located at the datacenter
- Providing functions that require personnel to physically access the servers, associated equipment, and/or network hardware

### Risk management

- Implementing security controls
- Continuously monitoring the status and effectiveness of compliance across Microsoft Cloud Germany, providing reporting and escalation when needed
- Creating plans to scope, execute and reconcile audits

# Frequently asked questions

## How is the data trustee model enforced?

The model is technically enforced through the mechanisms described above that vest control of access to customer data with the data trustee.

The relationships between Microsoft and the data trustee, Microsoft and its customers, and the data trustee and customers are enforced by binding contracts among all three parties. Microsoft contractually commits to its customers that it will seek access to customer data from the data trustee only for permitted purposes, such as troubleshooting service problems. The data trustee separately commits to customers that it will not disclose customer data to third parties except as directed by the customer or as required by German law.

## How does Microsoft respond to government or third-party requests for data?

Because Microsoft does not have custody of or access to Microsoft Cloud Germany customer data, Microsoft is unable to comply with requests from governments or other parties for access to customer data, even if directed to do so by law enforcement or the legal system of any nation. Any parties that make requests for customer data are advised to contact the customer or the data trustee, the only entity beyond the customer that is able to provide access to such data.

Governments and other parties have the option of pursuing requests through the German court system, as would be the case with any German company hosting customer data in Germany. Even in this case, however, the requestor would have to direct the request to the customer or the data trustee, rather than to Microsoft.

# Conclusion

Upholding the Microsoft principles of security, privacy, transparency, and compliance means providing

customers in every part of the world with services designed for their concerns and needs. Microsoft Cloud Germany and the data trustee model are Microsoft's effort to provide those assurances for our customers in Germany. By hosting all customer data entirely within Germany and entrusting a German partner with control over its access, Microsoft has developed a system that it believes will satisfy the concerns of its customers, not just from a technical standpoint but from a legal standpoint as well.

For additional information, please see the following resources:

- Microsoft Cloud (in German)
- Microsoft Trust Center
- Microsoft Azure Network Security