



# Service Description & Additional Terms and Conditions OPEN TELEKOM CLOUD – MANAGED SERVICES

Open Telekom Cloud

Version: 12.07.2021

# Impressum

---

## **Published by**

---

T-Systems International GmbH

Hahnstraße 43d

60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

<https://www.t-systems.com/de/en/compulsory-statement>

hereinafter referred to as "Telekom"

Copyright

© 2021 All rights reserved, including those of reproduction, electronic or photomechanical copies, and evaluation by electronic data processing methods.

# CONTENTS

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
<b>2</b>	<b>Services.....</b>	<b>5</b>
2.1	Tenant-Management.....	5
2.2	Storage Management .....	5
2.3	Security Management.....	5
2.4	Managed Subnet .....	5
2.5	Activity logging within a tenant .....	6
2.6	Managed Operating Systems.....	6
2.7	Managed Database Services .....	6
2.8	Managed Application Services .....	6
2.9	User management.....	6
2.10	Optional services .....	7
2.10.1	Reporting .....	7
2.10.2	Extended Monitoring .....	7
2.10.3	Backup & Restore.....	8
2.10.4	Support of customer projects .....	8
2.10.5	Upgrade and Migration .....	8
2.10.6	Custom maintenance periods.....	8
2.10.7	Private Image Management .....	8
<b>3</b>	<b>Services provided by Telekom .....</b>	<b>9</b>
3.1	Provisioning.....	9
3.2	Operation .....	9
3.2.1	Customer Support.....	9
3.2.2	Location of service provision.....	10
3.2.3	Unilateral changes to the service .....	10
3.2.4	Service Level .....	11
3.2.5	Excused Events.....	13
3.3	Monitoring and Troubleshooting.....	14
3.4	Release and Deployment Management .....	14
<b>4</b>	<b>Customer Obligations.....</b>	<b>14</b>
4.1	General cooperation .....	14
4.2	Cooperation within the scope of the provision .....	15
4.3	Cooperation for optional services .....	15
<b>5</b>	<b>Termination/ minimum lease periods .....</b>	<b>16</b>

6	Payment .....	16
6.1	Method for calculation charges .....	16
7	Glossary / Abbreviations .....	17

# 1 INTRODUCTION

With Open Telekom Cloud Managed Services, Telekom provides support services for the management of the customer's Open Telekom Cloud resources.

## 2 SERVICES

Telekom will perform the following services:

### 2.1 Tenant-Management

Telekom implements and maintains the system environment documented in the onboarding process based on the functional components of the Open Telekom Cloud. This is a basic service that must always be ordered. Telekom provides the following services:

- a. Assignment and management of IP addresses on instances of the Open Telekom Cloud
- b. Configuration of the necessary Open Telekom Cloud infrastructure components, such as load balancers
- c. Configuration of identity and access management (IAM groups, policies and roles)
- d. Set-up and maintenance of a technical connection of the customer's tenant to the central management environment of the Managed Services
- e. Configuration and monitoring of quotas
- f. Configuration and maintenance of subnets
- g. Configuration of accesses

In addition, Basic Tenant Management includes the following activities:

- i. Coordination of changes, updates, support and maintenance activities
- ii. Coordination of incident and problem management processes
- iii. Handling prioritizations and escalations
- iv. Review and adjustments to documentation
- v. Identifying and implementing updates or configuration changes

### 2.2 Storage Management

Telekom monitors the tenant's allocated storage. Growth trends and maximum capacity are analyzed. The memory utilization of volumes per virtual machine are checked. In the event of disruptions or negative growth trends, Telekom will inform the customer and initiate troubleshooting measures.

### 2.3 Security Management

Telekom configures one-time necessary security components (firewall rules and port forwarding) according to customer specifications.

### 2.4 Managed Subnet

Telekom sets up one-time subnets within a virtual private cloud according to customer specifications and manages the configuration and access rights.

## 2.5 Activity logging within a tenant

Telekom activates the logging (CTS, Cloud Trace Service) of all activities of a user within a tenant.

## 2.6 Managed Operating Systems

Telekom provides the following services for operating systems of the Image Management Service (IMS) of the Open Telekom Cloud:

- a. Telekom installs and configures the operating system as a hardened shared image. This version includes pre-configured programs that enable integration into the existing Managed Services monitoring and reporting infrastructure.
- b. Telekom starts and stops the systems according to customer specifications. Telekom sets up environment variables as specified by the customer.
- c. The operating systems are patched and updated in consultation with the customer (this does not include updates to new major versions).

## 2.7 Managed Database Services

Telekom provides managed database management systems (DBMS).

Telekom installs and configures a managed DBMS on an ECS instance of the customer. The DBMS is started and stopped according to customer specifications. Environment parameters of the database management system can be specified based on Group policies. The DBMS is patched and updated in consultation with the customer (this does not include updates to new major versions).

Telekom will troubleshoot the DBMS in the event of a malfunction. This includes failures that can be directly assigned to the DBMS. Errors at application level, such as faulty referential integrity or faulty SQL scripts, are not part of the general trouble-shooting service.

## 2.8 Managed Application Services

Telekom offers additional managed middleware components as an extension to the PaaS services of the Open Telekom Cloud.

Telekom installs and configures a managed middleware component on a customer ECS instance and connects to the managed services monitoring infrastructure. The middleware components are started and stopped according to customer specifications. Environmental parameters can be customized as long as they are compatible with Group policies. The middleware components are patched and updated in consultation with the customer (this does not include updates to new major versions).

Telekom will troubleshoot the middleware components in the event of a malfunction. This includes failures that can be directly assigned to the middleware component. Errors that are located at application level (e.g., error 500) or originate from it (e.g., memory errors) are not part of the general trouble-shooting service.

## 2.9 User management

Telekom will perform up to 5 user management changes for the managed services. These include:

- i. Create or delete a user
- ii. Create or delete a user group
- iii. Setting up or revoking permissions for users or user groups
- iv. Assigning users to user groups
- v. Resetting passwords
- vi. Disable or Enable user access

- vii. Modification of general profile information

## 2.10 Optional services

The following optional services shall be provided against additional payment if ordered separately. Upon request, Telekom shall submit an offer to the customer and provide more detailed descriptions of the following services.

### 2.10.1 Reporting

Telekom creates a weekly report. The report may contain the following information and is sent to the customer by e-mail:

- i. List of ECS instances deployed
  - a. Name
  - b. ID
  - c. IP-Address
  - d. Flavor-Type
  - e. Start time
- ii. Deployed resources and current quota limits for the following functions:
  - a. Number of CPU cores
  - b. Main memory
  - c. Number of ECS instances allowed
  - d. Number of hard disks
  - e. Maximum capacity of hard disks
  - f. Number of available backup copies (snapshots)
- iii. List of backup copies created via Backup&Restore incl.
  - a. Backup name
  - b. Backup ID
  - c. Backup Status
  - d. Creation date
  - e. Size of the backup
  - f. Expiration date of the backup (if available)
- iv. Configured Cloud Server Backup Strategy (Backup policy)
  - a. Name of the policy
  - b. Status
- v. Cloud Traces: Maintenance work that is carried out within the tenant
  - a. Activity type
  - b. Time stamp (UTC)
  - c. Type and name of changed resource
  - d. Trace type
  - e. ID of the executing user

### 2.10.2 Extended Monitoring

Based on individual customer requirements, Telekom sets up extended monitoring that monitors the following application areas:

- a. Web-based monitoring (evaluation of the http response code)
- b. Monitoring of additional log files
- c. API monitoring
- d. Monitoring of certificate expiration

### 2.10.3 Backup & Restore

Telekom creates backups of Managed Operating Systems using the Cloud Server Backup Service of the Open Telekom Cloud. This is an integrated service that creates a complete copy of computer and customer data including all connected storage on the customer's tenant.

The default backup policy provides the following time windows:

- a. Every Friday, starting at 21:00 (CET), a full backup of the operating system instances is performed. The last 10 backup copies are kept each time.
- b. Monthly backups are retained for long-term archiving for 36 months. The first backup copy of each month is archived.

### 2.10.4 Support of customer projects

Telekom provides the following services:

Service	Description
Audits and reviews	Support the customer in conducting audits and reviews by providing required data from the managed environment.
Disaster recovery tests and concepts	Support the customer in the creation and testing of disaster recovery concepts.
Backup and recovery tests	Support the customer in checking the quality of his backup and restore concept and the resulting backup files
Performance optimization for customer applications	Implementation of optimization measures according to the customer's specifications.
Other customer projects	Other customer projects can be supported upon request.

### 2.10.5 Upgrade and Migration

Telekom advises the customer on decisions regarding upgrades and migrations of flavors, operating systems and applications. In the event of a desired change, Telekom supports the customer in the implementation of upgrades and migrations.

### 2.10.6 Custom maintenance periods

If Telekom's maintenance periods do not meet the customer's requirements, the customer may request maintenance periods upon request, taking Telekom's lead times and internal processes into account. In this case, maintenance is performed at the customer's request.

In addition, maintenance periods shorter than quarterly can be requested. In this case, the requested schedule must be provided by the customer.

### 2.10.7 Private Image Management

As part of Private Image Management, Telekom provides the following services for all Public Image operating systems that can be ordered via the Open Telekom Cloud Platform:

- a. Creation of private OS images based on public images or customer-owned images for exclusive use on the Open Telekom Cloud.
- b. Telekom shall perform update and modification requests of the Customer on the Private Image once a month.
- c. If necessary, Telekom shall perform emergency maintenance work.



- d. Provision of a Managed Operating System based on the Private Image created.
- e. Transfer of Private Images between different tenants of the Customer.
- f. Decommission of existing images

Telekom shall be entitled to decommission Private Images twelve months after notice. Telekom shall delete the Private Image from the image database and delete all instances and the customer's data stored on them. Telekom shall not back up the data. The customer shall consult with Customer Support about backing up the data at least one month before decommissioning the Private Image.

## 3 SERVICES PROVIDED BY TELEKOM

### 3.1 Provisioning

Telekom conducts an onboarding workshop with the customer on the basis of a questionnaire to obtain relevant information for the implementation of the managed services and to define the necessary guidelines for operation. The workshop takes place either on-site at the customer's premises or online via video conference.

After conducting the onboarding workshop and implementing all measures, Telekom sets up the Managed Services on the tenant environment assigned to it with a dedicated subnet or VPC and configures the customer's tenant according to the results worked out in the workshop. The setup of the environment is priced separately according to time and effort. Subsequently, a monthly costs will apply, which can be derived from the price list.

Telekom shall appoint a technical contact for the provision of the Managed Services to the customer and shall inform the customer by e-mail as soon as the deployment has been completed. The service is provided when the e-mail is sent, but at the latest when the services are used.

If services were ordered without an onboarding workshop, the standard services described in this document apply without individualized service agreements.

### 3.2 Operation

The services of the Managed Service of the Open Telekom Cloud are based on the Open Telekom platform. The service description of the Open Telekom Cloud shall therefore apply insofar as no deviating provisions are made.

#### 3.2.1 Customer Support

Customer Support is the central point of contact for questions and problems regarding the Managed Services, as well as inquiries regarding optional services and service adjustments. The customer support is available to the customer under the contact options specified in the service description of the Open Telekom Cloud at the following service times:

Language	English
Availability of the hotline	24x7
Provision of the service	EU
Operating hours	09:00 – 17:00

The communication is conducted in English.

### 3.2.2 Location of service provision

Telekom provides the services within the European Union.

### 3.2.3 Unilateral changes to the service

#### 3.2.3.1 Service changes made by Telekom

If Telekom intends to make changes to the services or increase prices, the customer shall be notified of the changes in text form (e.g., by letter or e-mail) at least six weeks before they take effect. The changes shall become part of the contract at the time they take effect subject to the following conditions of the clauses:

- a. Telekom shall be entitled to make unilateral changes to the legal conditions, service descriptions and prices in favor of the customer.
- b. In the event of price increases and significant changes to the service descriptions to the customer's disadvantage, the customer shall be entitled to terminate the service in text form without notice as of the date on which the changes take effect. The customer shall be expressly informed of the right of termination in the notification of change.

#### 3.2.3.2 Configuration changes at the request of the customer

The standard prices for managed instances and services include a maximum allowed limit of 10 changes each, unless otherwise stated. This quota can be extended upon request.

A Change is defined as a modification or extension of an existing specification, product or service. Examples of a Change are the modification of a configuration parameter or the addition of a new user account. Adding a new service or changing the architecture of a system landscape is not a Change, but requires a separate order.

#### 3.2.3.3 Open Telekom Cloud dependent changes

All services of the Open Telekom Cloud Managed Services are based on the performance features of the Open Telekom Cloud Platform. Insofar as modifications are made to the Open Telekom Cloud platform and/or individual performance features are no longer available, these changes must also be implemented for the Open Telekom Cloud Managed Services.

Telekom shall inform the customer of any upcoming changes. Telekom shall be entitled to update or discontinue the affected service three months after notification. In the event of discontinuation of the service, Telekom shall delete the customer's affected data. Telekom shall not back up the data.

The customer is obligated to carefully examine the effects of the changes and, if necessary, coordinate with Telekom's customer support in a timely manner to work out alternative solutions or back up its data.

### 3.2.4 Service Level

Service Type	SLA Name	Description	Availability	Service Window
Standard operation of a managed operating system or a managed application	Availability	Monthly availability of a managed application or operating system (without high availability option).	99,50%	24x7
	Maximum Downtime	Monthly cumulative downtime of a single instance, application, or operating system.	4 hours per month	24x7
	Maximum downtime per event	Maximum downtime of a single instance of an application or operating system for an event	4 hours	24x7
Application operation in high availability mode	Availability	Monthly availability of a managed application in high availability mode.	99,95%	24x7
	Maximum Downtime	Maximum downtime of a single high-availability application	30 minutes per month	24x7
	Maximum downtime per event	Maximum downtime of a single, highly available application for one event	30 minutes	24x7
Incident	Response time for P1	Complete failure of an application and/or complete failure of a defined critical application where the application is unavailable to more than 50% of end users or has a significant degradation in performance. A P1 failure must be reported or confirmed by the customer both by telephone and in writing.	30 minutes	24x7
	Response time for P2	Application is unavailable for 5% to 50% of customers or has performance issues that severely impact business continuity	1 hour	24x7
	Response time for P3	The application is unavailable or has performance issues for up to 5% of customers, resulting in a loss of technical (non-business) functionality	2 hours	09:00 – 17:00
	Response time for P4	All main areas of the application are operational only one minor error has occurred, usually with a single user; technical queries	24 hours	09:00 – 17:00

Incident	Resolution or escalation time for P1	100% failure of an application and/or 100% failure of a defined critical application where the application is unavailable to more than 50% of the end users/exhibits performance degradation.	2 hours	24x7
	Resolution or escalation time for P2	P1 problem must be reported or confirmed by the customer both by phone and in writing.	3 hours	24x7
	Resolution or escalation time for P3	The application is unavailable or has performance issues for up to 5% of customers, resulting in a loss of technical (non-business) functionality	2 Workdays	09:00 – 17:00
	Resolution or escalation time for P4	All main areas of the application are operational only one minor error has occurred, usually with a single user; technical queries	5 working days or during the next maintenance cycle	09:00 – 17:00
Problem	“Root cause Analysis” (RCA) for P1	Telekom provides RCA based on a defined template upon customer request.	5 working days from the written request	09:00 – 17:00
	RCA submission for P2		7 working days from the written request	09:00 – 17:00

### Compensation in the event of a breach of the service level agreements

The customer is entitled to claim 10% discount on the actual monthly operating fee	If the monthly <b>availability</b> of the operating system or a single instance application falls below 99.50%.
The customer is entitled to claim 10% discount on the actual monthly operating fee	If the monthly <b>availability</b> of the high availability application falls below 99.95%.

### Attachments for service levels

Availability	Service availability is calculated as follows: $\frac{(\text{Total Service minutes}) - (\text{Total Downtime minutes})}{\text{Total service minutes}}$
	Availability excludes incidents, downtime and problems attributable to Customer, its users or representatives.
	Availability excludes downtime for: Hardware, data network, WAN, data center, OTC portal
Downtime	Complete unavailability of the service. Availability is charged for the application service. All platform-related failures are not part of the agreement, as these are covered in the platform form contract.
	Downtimes that are due to external influence (e.g. DDoS attack) are not part of the agreement.
Response time	Maximum time between the receipt of the issue and the start of work on solving the problem.
Resolution time	Time difference between the start of the problem and the end of the problem. Resolution time is defined as the time between when the customer first reports an incident and when the problem is actually resolved. A workaround counts as a resolution. "Long time resolution" is not part of resolution time. The resolution time only applies to the agreed technical level described in the service description. If the problem cannot be solved by these measures, Telekom informs the customer hotline within the resolution time (escalation). After that, Telekom is no longer responsible for solving the problem, but continues to actively support the customer in the solution steps. In this case, the customer must specify the solution steps
Start of the issue	Start time of the event in the ticketing tool created via the self-service portal or by the IT service desk or other support group manually creating a record.
End of the issue	End time of the event (event deleted) in the ticketing tool or agreed time based on customer feedback.

### 3.2.5 Excused Events

Interruptions in service based on any of the following events shall not be considered downtime and shall not be included in the calculation of availability:

- i. The Open Telekom Cloud is not available.
- ii. Incidents, failures and problems attributable to the customer, its users or otherwise.
- iii. Outages attributable to third-party interference (e.g. DDoS attack).
- iv. Maintenance activities

If there is a threat of significant damage to the customer's systems, the existing security vulnerabilities will be eliminated as part of emergency maintenance work. This applies primarily to all other specifications for maintenance work and service levels for the affected service.

All other patches and updates will be installed within 12 months, after their release by the manufacturer, according to the time frames defined in the onboarding workshop.

If this maintenance work leads to interruptions in service, Telekom will inform the customer in advance. Telekom shall endeavor to keep any disruptions caused by maintenance work to a minimum. Maintenance-related downtimes are not taken into account when calculating availability.

The maintenance regulations of the Open Telekom Cloud Platform remain unaffected.

### 3.3 Monitoring and Troubleshooting

Telekom monitors the customer's environment according to predefined values. When errors are detected, a troubleshooting process is initiated. The customer is notified by e-mail of the initiation of the troubleshooting process and is kept informed of the current status until the incident is cleared. Errors caused by the customer are excluded from the fault clearance service.

### 3.4 Release and Deployment Management

Telekom installs fixes, bug fixes, feature releases, feature retirements and general configuration adjustments to managed instances according to established patching guidelines during service hours. Telekom provides the following services:

- i. Assist customer with test and implementation planning of release changes.
- ii. Implementation of release changes.

The results of release changes are communicated to the customer by e-mail.

## 4 CUSTOMER OBLIGATIONS

The customer is obliged to provide cooperation that is necessary for the proper provision of services, in particular, however, the following, free of charge, in a timely manner and to the necessary extent:

### 4.1 General cooperation

- i. The customer agrees to unencrypted correspondence by e-mail and will always provide an up-to-date e-mail address. The customer is aware that information essential for the provision of services, such as access data, information on changes to the services and the legal conditions, as well as invoices are sent exclusively by e-mail.
- ii. The customer shall provide Telekom with all necessary information, in particular the following:
  - a. Installation materials and instructions
  - b. Software dependencies
  - c. Qualified and decision-making contact person, contact information, and representative
  - d. Fully completed onboarding questionnaire.
  - e. Capacity changes
  - f. Criticality list of managed systems, data and applications for the support case.
  - g. Email address and/or cell phone numbers for SMN service.
  - h. any information that may have an impact on Telekom's service delivery.

The customer assures that all the information is complete and accurate and that he is authorized to submit the corresponding information. The customer shall keep his information up to date at all times.

- iii. The customer shall independently check all relevant and applicable legal provisions, laws, regulations and industry-specific provisions in connection with the use of the service and shall ensure compliance therewith. This includes, in particular, compliance with confidentiality obligations arising, for example, from a professional activity.
- iv. The customer must provide a tenant environment with dedicated subnet or VPC exclusively for hosting Managed Services for the term of the agreed services and grant Telekom unrestricted administrator rights to it to ensure the separation of areas of responsibility.

- v. The Customer shall provide the required resources on the Open Telekom Cloud platform - in particular Storage, Compute, Network and Application - for the term of the agreed services. The Customer shall be responsible for providing sufficient resources for its Managed Virtual Machines and shall book any necessary capacity extensions in a timely manner.
- vi. The Customer is obliged to use and follow the Open Telekom Cloud Customer Support Process. He must support it and provide all necessary data and information in a clear and understandable manner so that Telekom is able to identify and solve problems that may fall within its area of responsibility.
- vii. The customer is obligated to keep passwords and access data secret, to disclose them only to authorized third parties, or to protect them from access and to change them if necessary. The customer shall inform Telekom immediately if there are any indications that unauthorized third parties have gained knowledge of the data.
- viii. Customer is responsible for providing and authorizing the domain, as well as issuing a server certificate for Custom Services and any associated domains.
- ix. The Customer is obliged to cooperate in the creation/adjustment of the operating concept (including backup/restore/monitoring/security/patching).
- x. The customer agrees that Telekom may create a trace for logging user activities within the managed tenant, which is stored in a private object storage bucket in the Telekom tenant and to which only Telekom has access.
- xi. The customer shall provide all rights of use and software licenses (including updates or upgrades) required for the provision of the service, unless these are to be provided by Telekom on the basis of a written agreement. This shall apply in particular to the use of the customer's own images.
- xii. For software provided by Customer, Customer shall provide manufacturer support (e.g., by maintaining maintenance agreements) and designate a contact person for Customer support.
- xiii. The customer is prohibited from changing the network and security rules, defined managed services and created traces set by Telekom.
- xiv. Customer is prohibited from modifying, deactivating or deleting the IAM resources with the prefix "Telekom\_" and/or creating its own IAM policies, roles or groups with the prefix "Telekom\_".
- xv. The customer shall inform Telekom immediately in writing if it is unable to provide a cooperation service as agreed.
- xvi. The customer will be required to review and approve maintenance work that impacts service availability or costs. Telekom will inform the customer of planned changes by e-mail.

## 4.2 Cooperation within the scope of the provision

- i. The Customer shall attend the Onboarding Workshop on the date set by Telekom.
- ii. The customer supports Telekom in answering the questionnaire and ensures that the information provided is correct and complete.
- iii. If required, the customer shall provide a suitable meeting room and the necessary work equipment.
- iv. Customer shall provide integration information for the IAM and enable Identity Federation or Identity Integration for the Managed Services.
- v. Customer shall provide all necessary information and certificates to allow Telekom access via a secure connection.

## 4.3 Cooperation for optional services

Managed Services on Hybrid Open Telekom Cloud:

The customer must provide Telekom sufficiently dimensioned remote access to its on-premise services.

## 5 TERMINATION/ MINIMUM LEASE PERIODS

A minimum term of 3 (three) months applies to the agreed services. The minimum term is automatically extended by three months unless the service is terminated.

## 6 PAYMENT

### 6.1 Method for calculation charges

- i. Charges are calculated monthly per service according to the price list.
- ii. The obligation to pay fees begins on the day of the first provision of the respective Service. Services are charged for a full month, regardless of whether they are provided on a sub-monthly basis.
- iii. In the case of quantity-based billing for services, the highest value in the billing month shall be used as the basis.
- iv. The prices for the Managed Services are to be understood independently of the costs of the Open Telekom Cloud platform. The customer's tenant costs (e.g. for ECS instances and network costs) shall be invoiced separately. As a result, the customer will receive a monthly invoice from Open Telekom Cloud Managed Services for the managed services and an invoice from Open Telekom Cloud for the consumed services of the tenant.
- v. All prices are exclusive of taxes and duties applicable at the time of delivery and performance.
- vi. The costs for the initial and/or subsequent provision of services shall be charged individually on a time and material basis.
- vii. For the implementation of an additional Change, 10% of the monthly costs of the instance to which the Change relates will be charged.



## 7 GLOSSARY / ABBREVIATIONS

Term	Description
AOT	Attended Operation Time
ACL	Access Control List
API	Application Programming Interface – typically used for automatic control and/or integration into higher-level orchestration
AZ	Availability Zone
CDN	Content Delivery Network
CTS	Cloud Trace Service
CET/CEST	Central European Time/Central European Summer Time
D/R	Disaster Recovery (protection against the shutdown of a complete data center, e.g. in the event of a catastrophe.)
DB	Database
DCS	Distributed Cache Service
DDS	Document Database Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DNS record	Record of a Domain Name Service-Zone
DNS zone	Part of the domain hierarchy managed by a name server
ECS	Elastic Cloud Server (ECS)
ELB	Elastic Load Balancer
EVS	Elastic Volume Service
Flavor	Synonym for an Elastic Cloud Server type
GB	Gigabyte
Gbit/s	Gigabit per second
HA	High availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IMS	Image Management Service
IP	Internet Protocol
Managed OS	Managed Operating System
MB	Megabyte
Mbit/s	Megabit pro second
MSC	Managed Services on Cloud
MFA	Multifactor authentication
MPLS	Multiprotocol Label Switching
ms	Milliseconds
NAT	Network Address Translation

OS	Operating system
OBS	Object Storage Service
OTC	Open Telekom Cloud
PB	Petabyte
PIM	Private Image Management
PSA	Privacy and Security Assessment - <a href="https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/security/details/privacy-and-security-assessment-process-358312">https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/security/details/privacy-and-security-assessment-process-358312</a>
RAM	Random Access Memory
RDBMS	Relational database management system
RDS	Relational Database Service
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
SDRS	Storage Disaster Recovery Service
SLES	SUSE Enterprise Linux
SMN Service	Simple Message Notification Service
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TB	Terabyte
URL	Uniform Resource Locator
VM	Virtual machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network (typically via IPsec and Site2Site scenario) - enables secure communication over insecure communication paths such as the Internet