Service Description

Enterprise Service Cloud - Managed MS SQL DBMS Services

Table of contents

1 **Service Overview** 3

2 **Definitions** 4

2.1 The Service Access Interface Point (SAIP) 4

2.2 Service-specific definitions 4

3 **Variants and options** 5

3.1 Definition of the service variants 5

3.2 Definition of the service specifications and options 5

4 **Service provision and responsibilities** 7

5 **Service Level and Service Level Reporting** 9

5.1 Service Level 9

5.2 Service Level Reporting 10

6 **Billing and quantity report** 10

6.1 Billing 10

6.2 Quantity report 10

7 **Special provisions** 11

7.1 Lifecycle management 11

7.2 Miscellaneous 11

7.3 Data protection provisions 12

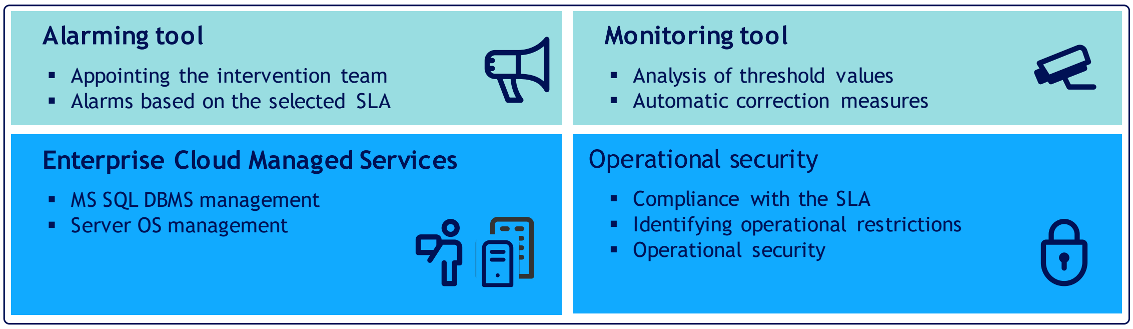
7.3.1 Data processing by third parties in Switzerland or abroad 12

1 Service Overview

The managed MS SQL DBMS service enables customers to transfer operational tasks associated with the Enterprise Service Cloud and up to the Database Management System (DBMS) level to Swisscom. This comprises the operation of the DBMS instances, backup/restore functionalities, antivirus and malware protection, patching, hardening accordint to “good practices” and monitoring of system-relevant parameters (monitoring and alarms) as well as incident and problem management up to DBMS level. This service satisfies high quality standards and is suitable for business-critical database applications.

The managed MS SQL DBMS service comprises the components shown in the diagram below and is characterised by the following features:

- Swisscom ensures the standardised provision of MS SQL DBMS instances that can be ordered via self-service (UI and API) by the Customer.
- When ordering MS SQL DBMS, the customer can specify whether a single instance (MS SQL DBMS Single Instance) or a MS SQL DBMS cluster (MS SQL Always-on) is to be provided.
- Swisscom ensures the secure and reliable operation of the MS SQL DBMS instance as well as the underlying operating system and thus enables the Customer to make targeted use of IT resources at the database and application level.
- High service levels and reporting form a stable basis for database operation.
- All the operational services are provided by Swisscom employees in Switzerland.



Alarming tool

- Appointing the intervention team
- Alarms based on the selected SLA

Monitoring tool

- Analysis of threshold values
- Automatic correction measures

Enterprise Cloud Managed Services

- MS SQL DBMS management
- Server OS management

Operational security

- Compliance with the SLA
- Identifying operational restrictions
- Operational security

The managed MS SQL DBMS service is based on the “Enterprise Service Cloud”. As a consequence, the purchase of Enterprise Service Cloud is a precondition for the purchase of the managed MS SQL DBMS service.

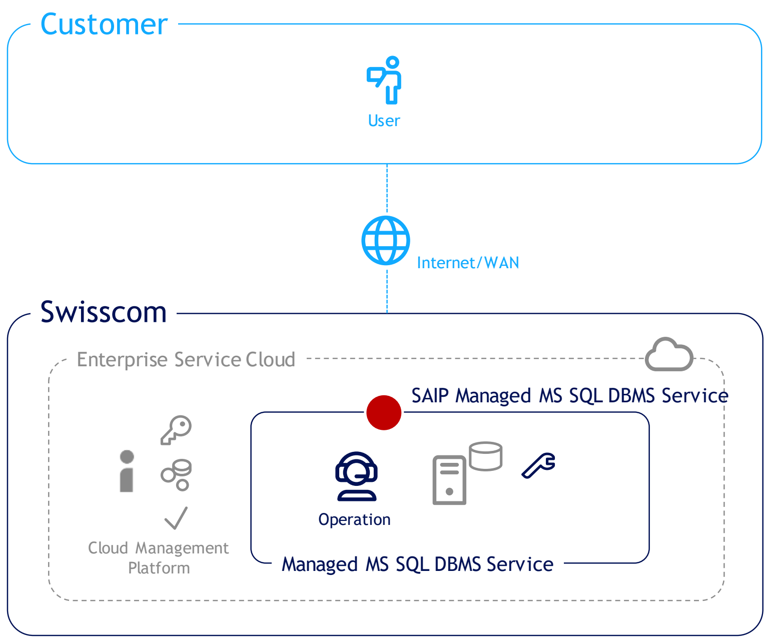
The managed MS SQL DBMS service can be purchased on the basis of standard Swisscom templates (blueprints) that are made available in the Enterprise Service Cloud service catalogue. Blueprints for MS SQL Single-Instance and MS SQL Always-on are available. The service is offered for Microsoft MS SQL with an underlying Windows Server operating system.

2 Definitions

2.1 The Service Access Interface Point (SAIP)

The Service Access Interface Point (SAIP) is the contractually agreed, geographical and/or logical point at which a service is delivered to the user. It is also the point at which a service is monitored and the service level provided are reported. Within the scope of the present service description, the SAIP is located on the network adaptor of the virtual server on which the service is operated. In the case of MS SQL Always-on, this definition refers to both virtual servers required to operate the cluster.

The following schematic diagram serves to show the services and service components of MS SQL DBMS services:


Customer
User
Internet/WAN
Swisscom
Enterprise Service Cloud
SAIP Managed MS SQL DBMS Service
Cloud Management Platform
Operation
Managed MS SQL DBMS Service

🟦 = Customer ⬛ = Swisscom service ▨ = Scope of Enterprise Service Cloud

The availability of the cloud management platform and the cloud infrastructure is defined in the Enterprise Service Cloud service description.

2.2 Service-specific definitions

Term	Description
Agent	An agent (technical agent) is a software component installed on the target system (VM). The agent’s task is to carry out defined tasks such as the surveillance of monitoring metrics.
DBMS	A database management system (DBMS) is the administration software that forms the basis for the operation of databases. Between 1 and n databases can be set up and installed on each DBMS instance.
VM	A virtual machine (VM) describes the software encapsulation of a computer system within another. The virtual machine replicates the computing architecture of a server that actually exists as hardware.

3 Variants and options

The following specifications apply to the use of MS SQL Single Instances and MS SQL Always-On. With MS SQL Always-on, the performance characteristics refer to both MS SQL instances, which form the basis of the cluster.

	Enterprise Service Cloud Managed MS SQL DBMS Service		
Standard variant	Single Instance DBA Mode	Single Instance	Always-on
Operation of Microsoft OS	●	●	●
Operation of MS SQL DBMS instance	–	●	●
Redundant VM Architecture	–	–	●
File Share Witness	–	–	●
Antivirus and malware protection	●	●	●
Patching and security updates	●	●	●
Backup	●	●	●
Monitoring and alarms	●	●	●
Incident resolution	●	●	●
Security reporting	○	○	○

● = Standard (included in the price) ○ = For an additional fee – = Not available

3.1 Definition of the service variants

The Service is available in the following service variants:

Service variant	Definition
Single Instance DBA Mode	A MS SQL DBMS single instance is set up on a VM. There is no redundancy at the DBMS level in the event of an outage. Under this option, the Customer has administrator rights (Sys Admin) at the DBMS level but not at the operating system level. A service level can only be ensured up to and including the operating system level.
Single Instance	An MS SQL DBMS Single Instance is based on a VM. At DBMS level, there is no redundancy in the event of a failure. Under this option, the Customer has no administrator rights, either at the DBMS level or the operating system level. The Customer is, however, granted restricted rights at the DBMS level. Authorisations are described in the currently valid technical online Enterprise Service Cloud documentation, which can be accessed via the Cloud Portal.
Always-on (Cluster)	An MS SQL Always-on cluster provides a redundant architecture with two nodes (DBMS instances) that are installed on two different VMs. This ensures that the two nodes are provided in different data centers. The function "File Share Witness" is activated on a third server. Under this option, the Customer has no administrator rights, either at the DBMS level or the operating system level. The Customer is, however, granted restricted rights at the DBMS level. Authorisations are described in the currently valid technical online Enterprise Service Cloud documentation, which can be accessed via the Cloud Portal.

3.2 Definition of the service specifications and options

The managed MS SQL DBMS service comprises the operational service on the VM up to the level of the MS SQL DBMS instance (without database operation), including outage and fault rectification for the selected virtual server.

The service is provided only for VMs based on Swisscom standard templates (blueprints). The service can be purchased via self-service from the cloud service catalogue by selecting a Managed MS SQL Server <Version>" blueprint.

Specification/Option	Definition
Operation of Microsoft OS	Swisscom ensures the secure operation of the Microsoft OS, which is automated and made available on a VM and installed in a standardised manner.
Operation of MS SQL DBMS instance	Swisscom ensures the secure operation of the MS SQL DBMS instance that is automated and made available on a VM and installed in a standardised manner.
Redundant VM Architecture	Redundant architecture with two nodes (DBMS instances) installed on two different VMs.
File Share Witness	The File Share Witness Server monitors which databases are running on which MS SQL DBMS Cluster Node and ensures that in the event of a cluster node failure, affected databases can automatically be restarted on the second cluster node.
Antivirus and malware protection	Swisscom protects the server against viruses and malware. The antivirus/ malware protection is implemented and operated using an agent in the relevant OS. The targeted use of antivirus/malware software provides the servers with effective protection against viruses and malware.
Patching and security updates	Operating system patches (minor releases only) are made available to the Customer by Swisscom in accordance with the instructions. When ordering, the Customer selects a defined time window for each VM running the MS SQL DBMS service in which Swisscom is authorised to run system updates and restart the VM if necessary. The time windows available for selection are spread out over a period of several weeks each month. New deployment packages are distributed in the first week of the month. Because time windows are available across several weeks in each month, the Customer can ensure that the distribution of new patches is spread (e.g. distribution on test systems in week 1, distribution on integration systems in week 2 and distribution on production systems in week 3).
Backup	Image based backup to back up the VM (snapshot of the VM and save the data as backup in a remote location). Ability to restore the VM on demand. Standard Backup Policy daily snapshot with 30 days retention time. Supplementary use of agent-based backup to back up MS SQL databases and transaction logs to consistently restore databases. There are various standard backup policies defined by Swisscom for database backup available to the customer.
Monitoring and alarms	The service includes monitoring for all service options at the operating system level, in order to detect when threshold values are exceeded and to trigger an alert to the persons responsible for operations at Swisscom. For "Single Instance DBA Mode", "Single Instance" and "Always-on" options, the DBMS is monitored in addition to the operating system. The metrics monitored are described in the currently valid technical online Enterprise Service Cloud documentation, which can be accessed via the Cloud Portal.
Incident resolution	The service includes the rectification of faults for all options up to the operating system level. Faults at the MS SQL DBMS instance level are also rectified under the "Single Instance" and "Always-on" options. Availability is ensured in accordance with the agreed service level. If the resolution of the incident requires the involvement of the customer, Swisscom will contact the customer. The Customer is responsible for rectifying faults at the database level.
Security reporting	The security reports show status information relating to patch management, malware protection and hardening. The report can be requested by the customer and is provided in pdf format on a monthly basis.

4 Service provision and responsibilities

Non-recurring services

Activities (S = Swisscom/C = Customer)	S	C
Provision of the service		
1. The service is made available in the desired version by selecting the “Managed MS SQL Server <Version>” blueprint on the self-service portal or via the API.		✓
2. Provision and switch of the virtual server to “Managed MS SQL DBMS” mode.	✓	
3. Installation of the required agents on the VM for the provision of the managed MS SQL DBMS service.	✓	
4. Creation of the required provider firewall rules to guarantee communication with the peripheral systems (monitoring server, logging server, patching server backup server and malware protection management server).	✓	
5. Connection of the virtual server to the required peripheral systems (monitoring server, logging server, patching server backuo server and malware protection management server).	✓	
6. Takeover of operation by Swisscom.	✓	
7. Naming of a technical contact [1] who can be contacted by Swisscom where necessary.		✓
Termination of the service		
1. Deletion of the VM on which the managed MS SQL DBMS is operated.		✓
2. Responsibility for timely exporting of installed databases and securing the relevant data (Microsoft’s licencing terms must be taken into account if the database is to continue to be operated externally).		✓
3. The customer can order the immediate deletion of backup data by means of a service request from Swisscom. Without an order, backup data will be stored until the end of the retention period agreed in accordance with the backup policy.		✓
4. Release of Swisscom from all contractual obligations relating to data storage.		✓

Recurring services

Activities (S = Swisscom/C = Customer)	S	C
Standard services		
1. Availability management: Ensure the availability in accordance with the agreed service levels of the managed server and the service variant up to the level OS resp. the MS SQL DBMS instance.	✓	
2. Antivirus & malware management: Swisscom ensures responses to the latest threats and the appropriate updating of signature files.	✓	
3. Patching: Swisscom automatically carries out the patching of the operating system during the maintenance windows defined by the Customer. Details on patching (patching cycle, emergency patches, etc.) can be found in the technical documentation.	✓	
4. Monitoring and alarms: Monitoring the resources for the server infrastructure components in accordance with the selected service variant up to the level OS resp. of the DBMS instance.	✓	
5. Ensuring that the VM has been assigned sufficient computing resources and storage in the event of expansion (e.g. the creation of new databases by the Customer).		✓

[1] The contact details should preferably be for a team/role rather than a single person. The contact should be able to be reached by both e-mail and telephone.

Activities (S = Swisscom/C = Customer)	S	C
6. Perform recurring restore tests of database objects. (Agent based backup policy for customer databases must have been activated by the customer in advance)		✓
7. Alarms: If the monitoring threshold values are exceeded, an alert is sent to the operating organisation of Swisscom and the incident management process is triggered.	✓	
8. Incident and problem management: Fault rectification and problem resolution to restore the agreed service level (fault reports are generated by the monitoring tools and can also be reported by the Customer through the standard incident management process). If incident resolution requires customer support (e.g. due to database dependencies), Swisscom establishes contact with the technical customer contact named by the Customer. The service level will be suspended until the Customer responds. Swisscom also notifies the technical customer contact person if the assigned system resources (e.g. vCPU, memory, storage, etc.) had to be adapted as part of incident resolution.	✓	
9. Connectivity management: Operation of the necessary components for the connection between the server systems and the storage.	✓	
10. Migration to later DBMS versions: If Swisscom no longer provides support for existing DBMS versions for managed services (e.g. due to the termination of manufacturer support for a DBMS version), the installed databases must be migrated to a new DBMS version. The Customer is responsible for migrations of this kind (this can be undertaken by exporting the database from an existing DBMS instance and subsequently importing the database to a new DBMS instance with a supported software version).		✓

Licenses

Provisioning obligations (S = Swisscom/C = Customer)	S	C
Provision of software licenses		
1. Swisscom ensures the correct licensing of the operating system for each VM within the framework of the Enterprise Service Cloud. For details, see the Enterprise Service Cloud service description.	✓	
2. When ordering the DBMS instance, the Customer selects whether the required licenses should be provided by the Customer or whether this must be arranged by Swisscom. Choice of licensing variant (licensing by Swisscom or license provided by Customer).		✓
▪ Where license provided by Customer: correct licensing of the DBMS instances and reporting duties to Microsoft.		✓
▪ Where license provided by Swisscom: correct licensing of the MS SQL DBMS instance.	✓	

5 Service Level and Service Level Reporting

5.1 Service Level

The following service levels generally relate to the agreed Support Time. Definitions of terms (Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are based on the other contractual elements (e.g. “SLA Definitions”).

The following service levels are provided for the managed MS SQL DBMS service: With an MS SQL Always-on Cluster, the service levels and target values refer to the individual MS SQL DBMS instances of the cluster.

			Managed MS SQL DBMS Service		
Service level & target values			**Basic**	**Standard**	**Advanced**
Operation Time					
Operation Time	Mo-Su	00:00-24:00	●		
Provider Maintenance Window	In accordance with the time window (at VM level) selected by the Customer in the cloud portal		●		
Support Time					
Support Time	Mo-Fr	07:00-18:00	●	—	—
	Mo-Su	00:00-24:00	—	●	●
Fault acceptance	Mo-Su	00:00-24:00	●	●	●
Availability					
Service Availability	99.9% -	Self-service portal and cloud management API	●	●	●
	99.5% -	MS OS resp. MS SQL DBMS instance[2]	●	—	—
	99.9% -	MS OS resp. MS SQL DBMS instance[2]	—	●	●
	99.9% -	MS SQL DBMS instance with Always-on	—	●	●
Security					
	Basic (ITSLB)		●	●	●
Continuity					
ICT Service Continuity (ICTSC) [3]	RTO Best Effort | RPO Best Effort		●	●	—
	RTO 4 h | RPO Near to 0		—	—	●
ICT Business Continuity (ICTBC) [4]	Is offered only on a basis of platinum data centers		—	—	○

● = Standard (included in the price) ○ = For an additional fee — = Not available

[2] Depending on the selected service variant. With the service variant "Single Instance DBA Mode", the service level can only be guaranteed up to and including the operating system level.

[3] ICT Service Continuity for instantiated objects requires that the customer has purchased the Backup option for the objects that need to be restored in the event of a disaster.

[4] Customer instances can also be secured using the ICT Business Continuity service. This involves the services for IT Business Continuity being governed in a separate contract with a separate service contract in addition to the scope of service of the Enterprise Service Cloud. If the ICTBC service is used, a customer-specific restart plan is produced for the solution and subjected to a customer-specific IT Business Continuity Test in accordance with the agreed scope of service on a regular basis. ICTBC tests for instantiated customer objects can be carried out in the cloud at a virtualisation level. (Example: For a VM to run the “Power Off” command and force a restart of the VM in the second data centre.) Switching off lower-level hardware components for the ICTBC test is not possible in the Shared Cloud Environment for individual customer tests.

N.B.:

- The service level variant (Basic, Standard or Advanced) is selected when ordering a blueprint of the managed MS SQL DBMS. The VM service level also defines the service level of the Managed MS SQL DBMS service (e.g. if the Customer selects the Standard service level for the VM, the service level of the managed MS SQL DBMS service is also Standard).
- Under the “Single Instance DBA Mode” option, service availability is ensured up to the operating system level and up to the DBMS instance level under the “Always-on” option.
- The “Advanced” service variant provides service continuity services at the VM level. Restarts at the database level are not included in this service, nor are its regular failover tests.
- The two MS SQL DBMS instances of an MS SQL Always-On must belong to the same service class. The service classes "Standard" and "Advanced" are available for the MS SQL Always-On service.
- Outages resulting from software errors attributable to the operation or DBMS software manufacturer result in the suspension of the promised service level.

5.2 Service Level Reporting

As part of the service, the Customer receives the following standard service level reports. Further reports can be provided, subject to charge, as part of the advanced reporting service after assessing the feasibility of the Customer’s requirements.

Service Level Report		Enterprise Service Cloud - Managed DBMS Service	Reporting period
Availability	Availability in % of the service at the SAIP during the measurement period	●	Month
Security	Customer notification in the event of knowingly deviating from ITSLB and not automatically correctable security breaches.	●	In the event of security breaches

● = Standard (included in price)

6 Billing and quantity report

6.1 Billing

The price of the managed MS SQL DBMS service is based on a minimum subscription period of at least one hour. Services are billed to the Customer retroactively for the previous month. The values for the effectively used managed MS SQL DBMS services are calculated pro rata per hour based on the VM status and billed in accordance with the current price list. The price for a Managed MS SQL Always-on Cluster includes the operation of the two MS SQL DBMS instances as well as the Managed Service price for the "File Share Witness" Server. Computing resources, amount of storage and backup data as well as licenses are charged according to the Enterprise Service Cloud service description.

Price position	Unit/Period	Minimum purchase/billing	Maximum purchase/billing	Included quantity
Managed MS SQL DBMS Service	Number of VMs/hour	1	Unlimited	–

6.2 Quantity report

The following data and information on the services rendered within the framework of the Swisscom managed MS SQL DBMS service is provided together with the monthly bill. Purchased resources and services are billed to the Customer post-hoc for the previous month. The values for the effectively used resources are calculated pro rata per hour in accordance with the current price list.

Quantity report Product services/options	Reporting information on billing
Managed MS SQL DBMS Service	Total for managed MS SQL DBMS services

7 Special provisions

7.1 Lifecycle management

Swisscom reserves the right to upgrade the virtualisation infrastructure hardware and software on a quarterly basis in line with the latest releases and versions. The system costs are borne by Swisscom. The cost of any modification of customer applications and upgrades of customer software, for example, is charged to the Customer.

Swisscom reserves the right to conduct standard patching for all systems of the infrastructure during any maintenance windows. If the services provided by Swisscom include third-party products, the Customer shall also respect the terms and conditions of use and licence terms and conditions associated with these. Swisscom may demand the right to enforce these terms and conditions vis-à-vis the Customer.

7.2 Miscellaneous

- Apart from databases, no further software components may be installed on a managed MS SQL DBMS instance.
- Under the “Single Instance DBA Mode” service option, the Customer can modify or delete administrative accounts, databases and jobs created on the VM. If the Customer modifies or deletes accounts, databases or maintenance jobs that Swisscom has created for the service provision, Swisscom can no longer ensure the provision of all the services defined in this service description.
- The Customer is responsible for the operation of the databases created on the managed DBMS instances.
- End-to-end availability measurement and availability guarantees for applications and appliances are not included.
- The managed MS SQL DBMS service is available only to DBMS/OS versions that still at least receive extended support from the manufacturer and are named in the technical documentation and the service catalogue. If a previously supported version is removed from the service catalogue, Swisscom terminates this with six months’ notice. Within this timeframe, the Customer is responsible for migrating databases being operated on affected DBMS instances to a DBMS instance listed in the service catalogue as being supported and for deleting the old DBMS instance (VM). Databases can be migrated using the export and import functions. After the set time period has expired, Swisscom is released from any operational responsibility for DBMS versions that are no longer supported.
- In addition to the other warranty disclaimers, Swisscom also refuses to accept liability in the following cases:
  - Restricted availability due to inadequate measurement of the computing resources by the Customer
  - Outages for which Swisscom is not directly responsible, in particular external DNS routing problems, virtual attacks on Swisscom’s network infrastructure (DDoS/viruses) and outages experienced by parts of the Internet outside Swisscom’s control which may lead to misinterpretation by the Customer
  - Outages resulting from software errors in the manufacturer’s operating system.
- The Customer is responsible for meeting all requirements relating to its storage and deletion of data:
  - The accuracy of the content saved by the Customer
  - The compatibility of the stored contents with legal requirements (e.g. the Swiss Data Protection Act)
  - Deletion of, or amendments to, data by the Customer itself
  - The accuracy of the instructions issued by the Customer to Swisscom regarding the periods for the storage of data prior to deletion.
- Swisscom will set up and operate an Active Directory Resource Domain in a business group managed by Swisscom for the operation of Managed OS services. VMs that use the managed MS SQL DBMS service must be part of this resource domain. The Customer will allow the resource domain to connect to its Active Directory using “one-way trust.”
- The Customer cannot access hardware interfaces or disk drives directly.
- The Swisscom security team regularly releases new requirements for the security settings of the operating systems. Examples may include the deactivation of outdated encryption ciphers. Such changes may be reflected in the blueprint without prior notification.

- Swisscom reserves the right to amend this service description on a unilateral basis at any time. Amendments that are necessary due to the service being extended or that do not negatively affect contractual use of the service by the Customer shall be announced as part of the release notes sent to all subscribers by e-mail. Where an amendment negatively affects contractual use of the service by the Customer (esp. if functionalities cease to be available), Swisscom shall inform the Customer about the details of the amendment and the date on which it will take effect at least six months in advance. In this case, both parties agree to seek an amicable solution to the consequences of such amendment, and to do so in good faith. If the parties fail to come to an agreement regarding the consequences of the contractual modification, the Customer shall be granted the right to terminate the relevant service contract in writing with effect from the date on which the amendment is set to take effect, subject to two weeks' notice. No further claims may be made by the Customer.

7.3 Data protection provisions

7.3.1 Data processing by third parties in Switzerland or abroad

The data transmitted to Swisscom by the Customer (customer data) within the scope of service provision is stored in Switzerland by Swisscom. Customer data is not accessed directly within the framework of the provision of the service. Swisscom employees may require access to technical system data as part of service provision. If necessary, information (such as dump files, SOS reports or system-specific log files) can be made available to third parties commissioned by Swisscom for the purpose of error analysis. It is ensured that only technical information (such as IP addresses, host names) is transmitted. Should it be necessary to transmit further information – which may contain customer data (e.g. from a memory dump) – this requires the Customer's prior written consent in each individual case. For its part, the Customer shall ensure that no customer data (e.g. from software components for which the Customer is responsible) is written to system-specific log files