COSMO CONSULT
Business-Software für Menschen

DATA PROTECTION AND DATA SECURITY AT COSMO CONSULT

Version: 3.2 | 13.09.2019

Table of content

1. General data protection measures at COSMO CONSULT

1.1 COSMO CONSULT has taken measures to ensure the security of objects and data as well as the uninterrupted operation of the facility in terms of construction, personnel, organisation and technology.

1.2 COSMO CONSULT is committed to secrecy towards its customers. All employees of COSMO CONSULT are committed to data privacy when hiring them.

1.3 At COSMO CONSULT, the scope of protection includes any handling of data of natural or legal persons and other confidential or sensitive data (e. g. company or financial data).

1.4 Fire protection and loss prevention measures have been taken at all COSMO CONSULT locations and offices.

1.5 Requirements for access and exit control are ensured at all locations by structural security of the offices and, as a rule, electronically monitored security areas. The disposal of confidential documents is carried out exclusively via a shredder system or document shredders.

1.6 COSMO CONSULT relies on the latest Microsoft technology, which meets all data protection requirements. This is evidenced by various data protection seals for Microsoft products.

1.7 COSMO CONSULT employs several IT specialists (certified, usually Microsoft Certified) to check security precautions, to supplement them according to the requirements and to further develop them in consideration of the latest technical measures.

1.8 COSMO CONSULT processes the data during software implementation, for data migration and testing purposes. Furthermore, COSMO CONSULT sets up test systems in coordination with the customer. Test systems will be retained as long as support is provided by COSMO CONSULT or as contractually agreed. After consultation with the customer, the dataset of the test systems can be a dataset that has been adjusted for sensitive data and simulated for testing purposes.

1.9 In the case of remote maintenance/access to customer systems, there is always a security system (encryption measures, etc.) that protects against unauthorized access.

1.10 To protect against computer viruses, all incoming media, emails and attachments are scanned for viruses. In addition, all PCs and servers are protected by centrally managed EndPoint Protection.

1.11 COSMO CONSULT has almost completely migrated central services and data protection requirements to a central data center.

1.12 Data processing is carried out exclusively within the scope of the EU-GDPR

1.13 If an order processing agreement has been concluded with our client, the following additional data protection measures apply:

1.13.1 The principle of separation of functions exists in all important areas. Areas affected by data processing are functionally and organisationally separated. All customer systems are only accessible to authorized employees, the respective project or customer support team. The access rights are assigned by the responsible project manager and checked regularly.

1.13.2 The required dial-in data for remote maintenance are either personalized or only accessible to authorized employees of the respective project or customer support team, depending on customer requirements.

1.13.3 Data protection and data security are of great importance for COSMO CONSULT. Therefore, COSMO CONSULT has its internal processes audited regularly.

2. Technical and organizational measures

2.1 The technical and organisational measures (TOM) are measures relating to:

2.1.1 order control, physical access control, logical access control, data access control, data transmission control, input control, availiability control,separation control and effectiveness controll

2.1.2 Type of data exchange, provision of data, type and conditions of processing, data retention as well as type and conditions of data transmission

2.1.2 Measures to ensure the confidentiality, integrity, availability and robustness of systems and services on a permanent basis, as well as the possibility of rapidly restoring the accessibility and availability of personal data in the event of a physical or technical incident.

2.1.3 A procedure for the regular review, evaluation and validation of the effectiveness of these measures.

2.2 As far as individual services are hosted by contractors, COSMO CONSULT will select them exclusively according to the legal requirements, order them in writing and inform the customers in the contract to be concluded about the order data processing.

2.3 The COSMO CONSULT Group regularly ensures and supervises compliance with the technical and organisational measures taken by all companies that have joined the Joint Controllership Agreement in accordance with Art. 26 of the GDPR.

2.4 In general, the technical and organisational measures of COSMO CONSULT are based on technical progress and further development. COSMO CONSULT will take all the necessary measures to increase security.
The recent documentation of the technical and organizational measures "Data Protection and Data security at COSMO CONSULT" is available for download on the website https://www.cosmoconsult.com/data-protection

2.5 Data processing locations

2.5.1 Centralized data center of COSMO CONSULT

COSMO CONSULT hosts all central services and servers in Microsoft Azure

See: https://azure.microsoft.com

2.5.2 COSMO CONSULT locations

COSMO CONSULT is an international group of companies with several locations and realizes IT projects worldwide. The regulations and measures documented here apply to all locations of the joint controller ship COSMO CONSULT Group.

See: https://www.cosmoconsult.com/data-protection

2.5.3 data processing in Microsoft Azure

As far as in the context of customer orders the data are hosted on the Azure platform and a transmission of personal data outside Europe cannot be excluded, a contract has been concluded with Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland according to the legal requirements. The adequacy of the data protection level is additionally guaranteed by a currently valid certification according to the so-called Privacy Shield.

Further information:

https://www.privacyshield.gov/pmodalityicipant?id=a2zt0000000KzNaAAK&contact=true#dispute-resolution-1

2.6 Physical access control

The following describes the measures that prevent forced or unauthorized intrusion into the offices of COSMO CONSULT.

Local server rooms (if applicable) are additionally secured at all locations within the office buildings.

2.6.1 Technical

Modality	Target
Physical access controll	Yes
Locking system	Yes

2.6.2 organizational

Modality	Target
Visitor registration at reception	Yes
Personal/supervised visitor guidance	Yes
Key rules and key book (use of security keys)	Yes

2.7 logical access controll

COSMO CONSULT secures the use of the data processing systems through various access controls, so that only authorized persons can access them. Each access requires identification and authentication of the user. Access from outside is secured by a firewall at all locations.

2.7.1 Technical

Modality	Target
Authentication with user name and password	Yes
Usage of Endp-PointProtection software	Yes
Usage of firewalls	Yes
UsageVPN-technology	Yes
Encryption of internal data disk (int. HD)	Yes
Encryption of external (mobile) devices (USB sticks, ext. HD, DVD etc.)	Yes

2.7.2 Organizational

Modality	Target
Managed Users and user permissions	Yes
Password assignment / password rules	Yes
User profiles	Yes
Key rules and key book (use of security keys)	Yes

2.8 Data access controll

In the following, COSMO CONSULT's measures are listed, which guarantee that those authorised to use a data processing system can only access the data provided to them and that personal data cannot be read, copied, changed or removed without authorisation during processing, use and after storage.

2.8.1 Technical

Modality	Target
Use of document shredders or collection containers (file disposal system)	Yes
authorization concept	Yes

2.8.2 Organizational

Modality	Target
authorization concept (AD-Groups, Role definition)	Yes
Password policy incl. length and change	Yes
Administration of user rights by system administrators	Yes

2.9 Data transmission control

COSMO CONSULT's measures are set out below to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during transport or storage on data carriers, and that it can be verified and determined at where personal data will be transmitted.

2.9.1 Technical

Modality	Target
Logging of data transfers	Client
VPN tunnel (secure line) into the COSMO CONSULT network	Yes
VPN tunnel (secure line) into the client's network	Client

2.9.2 Organizational

Modality	Target
Careful selection of employees	Yes
Usage rules for external (mobile) devices	Yes

2.10 Input control

The following is a list of COSMO CONSULT's measures to ensure that it can be verified and determined at a later date whether and by whom personal data have been entered, modified or removed in data processing systems.

2.10.1 Special feature / notes

The TOM with regard to input control must be made on the side of the customer (customer).
For example, it is the responsibility of the client to assign individual user names instead of collective logins for entire employee groups or teams (the COSMO CONSULT; to support the client) and to log data entries/changes, etc., so that it is possible to trace entries, changes and deletions of data in the production system.

2.10.2 Technical

Modality	Target
Logging of the input, modification and deletion of data (change protocol or similar)	Client

2.10.3 Organizational

Modality	Target
Assignment of rights to enter, change and delete data on the basis of an authorization concept	Client
Traceability of input, modification and deletion of data through individual user names (not user groups)	Client

2.11 Order control

In the following, COSMO CONSULT's measures are listed, which ensure that personal data processed on behalf of COSMO CONSULT by other suppliers can only be processed in accordance with the instructions of the client.

A list of approved subcontractors is regularly updated at https//www.cosmoconsult.com/data-protection. In the event of a change, customers will be informed in advance by email.

2.11.1 Organizational

Modality	Target
Only on written order data processing agreements	Yes
Only on written order processing agreements	Yes
Selection of the contractor from a diligence point of view (especially with regard to data security)	Yes
Obligation of the contractor's employees to maintain data secrecy	Yes

2.12 Availablility control

COSMO CONSULT's measures to ensure that personal data are protected against accidental damage or loss or that they can be recovered quickly in the event of an incident are listed below.

2.12.1 Special feature / notes

TOMs with reference to availability control must be made on the part of the sold-to party (customer). The TOMs are used exclusively for internal/own purposes of COSMO CONSULT and guarantee the ability to work and accessibility.

2.12.2 Technical

Modality	Target
Fire extinguishers in local server rooms (or nearby)	Yes

2.12.3 Organizational

Modality	Target
Store data backup in a safe place	Yes
Backup & Recovery Precautions	Yes

2.13 Seperation control

The following are measures to ensure that data collected for different purposes can be processed separately.

2.13.1 Technical

Modality	Target
Separation of productive and test system	Yes
Database and multi-tenant separation	Yes

2.13.2 Organizational

Modality	Target
Define access rights for different clients/customers	Yes

2.14 Effictiveness control

In the following, measures are listed to ensure that the internal organization of the company meets the special requirements of data protection.

2.14.1 Organizational

Modality	Target
Standards and regulations for IT security	Yes
Standards and regulations for securing the data stock	Yes
Organization manual at the location	Yes
Regular audits to ensure compliance with TOMs	Yes
Regular training sessions	Yes

3. Data Protection Officer

2b Advice GmbH
Joseph-Schumpeter-Allee 25
53227 Bonn

Tel: +49 (228) 92 61 65 123
Fax: +49 (228) 92 61 65 109

E-Mail: cosmoconsult@2b-advice.com
Web: http://www.2b-advice.com