data protection and data security

at the jointly controller COSMO CONSULT Group, in accordance with article 26 GDPR

Version: 3.2 | Date: 14.03.2023

Created by: Michael Makowski

COSMO CONSULT SSC GmbH
Von Steuben Straße 10 | 12
48143 Münster
Germany

dataprotection@cosmoconsult.com
www.cosmoconsult.com

Table of Contents

1 data security measures at COSMO CONSULT

This document describes the technical and organizational measures taken at COSMO CONSULT to ensure implementation in accordance with Art. 32 GDPR:

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 have been taken at all COSMO CONSULT locations and in all 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 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. COSMO CONSULT recommends running test and development systems on servers or hosted in a cloud environment of the customer.

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

1.12. the data processing is carried out exclusively within the scope of the GDPR.

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

1.13.1.1. the principle of separation of functions exists in all important areas. Areas affected by data processing are functionally and organizationally 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.

1.14. Data protection and data security are of great importance to COSMO CONSULT. Therefore, COSMO CONSULT has its internal processes audited on a regular basis.

2 data protection measures at COSMO CONSULT

2.1. The technical and organizational data protection measures (TOMs) are measures regarding;

2.1.1. Order control, physical access control, logical access control, data access control, data transmission control, input control, availability control, separation control and effectiveness control.

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

2.1.3. 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.

2.1.4. 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.

3 data processing locations

3.1 central data center of COSMO CONSULT

COSMO CONSULT runs all central services and servers in Microsoft Azure

See also: https://azure.microsoft.com

3.2 locations of COSMO CONSULT

COSMO CONSULT is an international group of companies with several locations and implements IT projects worldwide. The regulations and measures documented here apply to all locations of the jointly responsible entity COSMO CONSULT.

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

3.3 data processing in Microsoft Azure

COSMO CONSULT operates its cloud-based services and servers in the Microsoft Azure platform. West Europe (Amsterdam, Netherlands) has been selected as the main location for data processing, with individual services hosted in other European locations.

Insofar as data is hosted on the Azure platform within the scope of customer orders and there is a transfer of personal data to a third country within the Microsoft Azure Cloud, COSMO CONSULT has concluded a contract for this with Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland in accordance with the legal requirements on the basis of the EU standard contractual clauses and has checked the additional protective measures taken by Microsoft.

4 technical and organisational measures

4.1 confidentiality (Art. 32 para. 1 lit. b GDPR)

4.1.1 physical access control

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

Description of the measures taken by COSMO CONSULT:

- visitor registration at the reception
- local server rooms (if applicable) are additionally secured at all locations within the office buildings.
- personal/supervised visitor guidance
- locking system
- key rules and key book (use of security keys)

4.1.2 logical access control

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.

Description of the measures taken by COSMO CONSULT:

- authentication with username and password
- user profiles
- usage of end point protection software
- usage of firewalls
- usage of VPN technology
- password assignment/password rules
- mandatory for automatic screen lock (local)
- key rules and key book (use of security keys)
- encryption of external/mobile devices
- encryption of internal data carriers
- managed users and user permissions

4.1.3 data access control

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.

Description of the measures taken by COSMO CONSULT:

- authorization concept (AD groups, role definitions)
- use of document shredders or collection containers (document disposal system)
- password policy
- management of user rights by administrators

4.1.4 separation control

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

Description of the measures taken by COSMO CONSULT:

- database and multi-tenant separation
- definition of access rights for different clients/customers
- separation of productive and test system

4.2 integrity (Art. 32 para. 1 lit. b GDPR)

4.2.1 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.

Description of the measures taken by COSMO CONSULT:

- usage regulations for external/mobile data carriers
- careful selection of personnel
- VPN connection to the COSMO CONSULT network

Description of the measures to be taken by the controller:

- logging of data transfers
- VPN connection to the controller's network

4.2.2 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.

The technical and organizational measures with regard to input control are to be taken on the part of the controller.
For example, the assignment of individual user names instead of collective logins for entire employee groups or teams (of COSMO CONSULT; for the support of the controller) as well as the logging of data entries/changes etc. is the responsibility of the controller, so that a traceability of entries, changes and deletions of data in the productive system is possible.

- traceability of input, modification and deletion of data through individual user names (not user groups)
- logging of the entry, change and deletion of data (change log or similar)
- assignment of rights to enter, change and delete data based on an authorization concept

4.3 availability and resilience (Art. 32 para. 1 lit. b GDPR)

4.3.1 availability control

The following are measures taken by COSMO CONSULT to ensure that personal data is protected against accidental destruction or loss or can be quickly restored in the event of an incident.

The technical and organizational measures with regard to input control are to be taken on the part of the controller.
The technical and organizational measures taken by COSMO CONSULT serve exclusively internal/own purposes of COSMO CONSULT and a guarantee of operability and availability.

Description of the measures taken by COSMO CONSULT:

- keeping backups in a safe place
- fire extinguishers in local server rooms (or in required proximity)
- Backup & Recovery Precautions

4.4 procedures for periodic review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.4.1 order control

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.cosmocon-sult.com/data-protection. In the event of a change, customers will be informed in ad-vance by email.

Description of the measures taken by COSMO CONSULT:

- selection of the contractor under due diligence aspects (in particular with regard to data security)
- contractual definition of the type and scope as well as the purpose of the com-missioned processing and use of personal data of the controller
- only on written order processing agreements
- only on written instructions to the contractor
- obligation of the contractor's employees to maintain data secrecy

4.4.2 organizational control

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

Description of the measures taken by COSMO CONSULT:

- observance of data protection-friendly default settings (Art. 25 para. 2 GDPR)
- data protection management
- involvement of the global data protection coordinator and the external data protection officer if the operational processes require this
- organization manual at the site
- regular audits to ensure compliance with TOMs
- regular training sessions
- standards and regulations for IT security
- standards and regulations for securing the data stock

5 contact

5.1 global privacy coordinator

COSMO CONSULT SSC GmbH

Michael Makowski

Von-Steuben-Strasse 10/12

48143 Münster

Germany

email: dataprotection@cosmoconsult.com

web: https://www.cosmoconsult.com

5.2 external data protection officer

2b Advice GmbH

Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

email: cosmoconsult@2b-advice.com

web: https://www.2b-advice.com