Datenschutz und Datensicherheit

der gemeinsam verantwortlichen Stelle COSMO CONSULT Gruppe, gemäß Artikel 26 DSGVO

Version: 3.2 | Date: 14.03.2023

Erstellt von: Michael Makowski

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

dataprotection@cosmoconsult.com
www.cosmoconsult.com

Inhaltsverzeichnis

1 Maßnahmen zur Datensicherheit bei COSMO CONSULT

Dieses Dokument beschreibt die bei COSMO CONSULT getroffenen technischen und organisatorischen Maßnahmen, mit denen die Umsetzung gemäß Art. 32 DSGVO gewährleistet wird.

1.1. COSMO CONSULT hat Maßnahmen getroffen, die in baulicher, personeller, organisatorischer und in technischer Hinsicht die Sicherheit von Objekten und Daten sowie den ungestörten Betriebsablauf gewährleisten.

1.2. COSMO CONSULT verpflichtet sich gegenüber seinen Kunden zur Geheimhaltung. Alle Mitarbeiter der COSMO CONSULT verpflichten sich bei deren Einstellung auf das Datengeheimnis.

1.3. Der Schutzbereich umfasst bei COSMO CONSULT jeglichen Umgang mit Daten von natürlichen oder juristischen Personen und sonstigen vertraulichen oder sicherungsbedürftigen Daten (z. B. Unternehmens-/Finanzdaten).

1.4. An allen Standorten und in allen Büroräumen von COSMO CONSULT wurden Vorkehrungen für Brandschutz und Verlustsicherung getroffen.

1.5. Anforderungen der Zu- und Abgangskontrolle werden an allen Standorten durch bauliche Absicherung der Büroräume und in der Regel elektronisch überwachte Sicherheitsbereiche gewährleistet. Die Entsorgung vertraulicher Unterlagen erfolgt ausschließlich über eine Schredder-Anlage oder über Aktenvernichter.

1.6. COSMO CONSULT setzt auf modernste Microsoft-Technologie, die sämtliche Datenschutzanforderungen erfüllt. Dies belegen diverse Datenschutz-Siegel für Microsoft-Produkte.

1.7. COSMO CONSULT beschäftigt mehrere IT-Verantwortliche (zertifiziert; in der Regel Microsoft Certified), um Sicherheitsvorkehrungen zu überprüfen, entsprechend den Herausforderungen zu ergänzen und unter Berücksichtigung der neuesten technischen Maßnahmen weiterzuentwickeln.

1.8. COSMO CONSULT verarbeitet die Daten während der Software-Implementierung zu Datenübernahme- und Testzwecken. Des Weiteren setzt COSMO CONSULT in Abstimmung mit den Kunden Testsysteme auf. Testsysteme werden so lange aufrechterhalten, wie eine Betreuung durch COSMO CONSULT stattfindet, oder je nach Vereinbarung. Zudem kann der Datenbestand der Testsysteme nach Absprache mit dem Kunden ein um sensible Daten bereinigter und zu Testzwecken simulierter Datenbestand sein. COSMO CONSULT empfiehlt Test- und Entwicklungssysteme auf Systemen oder gehostet in einer Cloudumgebung des Kunden zu betreiben.

1.9. Bei Fernwartungen/-zugriffen auf Kundensysteme besteht immer ein Sicherungssystem (Verschlüsselungsmaßnahmen usw.), das vor unbefugtem Zugriff schützt.

1.10. Zum Schutz vor Computerviren werden alle eingehenden Datenträger, E-Mails und Attachments auf Viren geprüft. Zudem sind alle PC und Server durch zentral verwaltete Virenprogramme geschützt.

1.11. Zentrale Dienste und Datensicherungserfordernisse hat COSMO CONSULT nahezu vollständig in ein zentrales Rechenzentrum verlagert.

1.12. Die Datenverarbeitung wird ausschließlich im Anwendungsbereich der DSGVO durchgeführt.

1.13. Liegt eine Auftragsverarbeitungsvereinbarung mit unserem Auftraggeber vor, sind zusätzlich folgende Datensicherungsmaßnahmen zutreffend:

1.13.1. In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung. Von Datenverarbeitung betroffene Bereiche sind funktionell und organisatorisch getrennt. Sämtliche Kundensysteme sind nur berechtigten Mitarbeitern, dem jeweiligen Projekt- oder Kundenbetreuungsteam, zugänglich. Die Zugriffsrechte werden durch den zuständigen Projektleiter vergeben und regelmäßig überprüft.

1.13.2. Die für die Fernwartung erforderlichen Einwahldaten sind entsprechend der Kundenanforderungen entweder personalisiert, von COSMO CONSULT empfohlen, oder nur berechtigten Mitarbeitern, des jeweiligen Projekt- oder Kundenbetreuungsteams, zugänglich.

1.14. Datenschutz und Datensicherheit sind für COSMO CONSULT von hoher Bedeutung. Daher lässt COSMO CONSULT seine internen Prozesse regelmäßig auditieren.

2 Maßnahmen zum Datenschutz bei COSMO CONSULT

2.1. Bei den technischen und organisatorischen Datenschutzmaßnahmen (TOM) handelt es sich um Maßnahmen hinsichtlich.

2.1.1. Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und des Trennungsgebots

2.1.2. Art des Datenaustauschs, Bereitstellung von Daten, Art und Umstände der Verarbeitung, der Datenhaltung sowie Art und Umstände beim Datenversand

2.1.3. Maßnahmen zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

2.1.4. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen.

2.2. Soweit einzelne Dienste bei Auftragnehmern gehostet werden, wird COSMO CONSULT diese ausschließlich gemäß den gesetzlichen Vorgaben auswählen, schriftlich beauftragen und hierüber die Kunden im zu schließenden Vertrag über die Auftragsdatenverarbeitung informieren.

2.3. Die COSMO CONSULT Gruppe gewährleistet und überprüft regelmäßig die Einhaltung der getroffenen technisch und organisatorischen Maßnahmen durch alle dem Joint Controllership Agreement gem. Artikel 26 DSGVO beigetretenen Gesellschaften.

2.4. Generell unterliegen die technischen und organisatorischen Maßnahmen der COSMO CONSULT dem technischen Fortschritt und der Weiterentwicklung. COSMO CONSULT wird sämtliche Maßnahmen ergreifen, die zu einer Erhöhung der Sicherheit erforderlich sind.

Die aktuelle Dokumentation der technischen und organisatorischen Maßnahmen **"Data Protection and Data security at COSMO CONSULT"** wird auf der Website https://www.cosmoconsult.com/data-protection zum Download angeboten.

3 Standorte der Datenverarbeitung

3.1 Zentrales Rechenzentrum von COSMO CONSULT

COSMO CONSULT betreibt alle zentralen Dienste und Server in Microsoft Azure

Siehe: https://azure.microsoft.com

3.2 Standorte von COSMO CONSULT

Die COSMO CONSULT ist eine internationale Unternehmensgruppe mit mehreren Standorten und realisiert IT-Projekte weltweit. Die hier dokumentierten Regelungen und Maßnahmen gelten für alle Standorte der gemeinsam verantwortlichen Stelle COSMO CONSULT.

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

3.3 Datenverarbeitung in Microsoft Azure

COSMO CONSULT betreibt seiner cloudbasierten Dienste und Server in der Microsoft Azure Plattform. Als Location für die Datenverarbeitung ist vorwiegend West Europe (Amsterdam, Niederlande) ausgewählt, vereinzelte Dienste werden in anderen europäischen Lokalisationen gehostet.

Soweit im Rahmen von Kundenaufträgen die Daten auf der Azure-Plattform gehostet werden und es zu einer Übermittlung von personenbezogenen Daten in ein Drittland innerhalb der Microsoft Azure Cloud kommen, so hat COSMO CONSULT hierfür mit Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford

Industrial Estate, Dublin 18, Ireland einen Vertrag nach den gesetzlichen Vorgaben auf Basis der EU Standardvertrags-klauseln geschlossen sowie die zusätzlich durch Microsoft getroffenen Schutzmaßnahmen überprüft..

4 Technische und organisatorische Maßnahmen

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1.1 Zutrittskontrolle

Im Folgenden werden die Maßnahmen beschrieben, die das gewaltsame oder unberechtigte Eindringen in die Büroräume der COSMO CONSULT verhindern.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Besucheranmeldung beim Empfang
- Lokale Serverräume (sofern zutreffend) sind an allen Standorten innerhalb der Bürogebäude zusätzlich gesichert.
- Persönliche/beaufsichtige Besucherführung
- Schließsystem
- Schlüsselregelung und Schlüsselbuch (Verwendung von Sicherheitsschlüsseln)

4.1.2 Zugangskontrolle

COSMO CONSULT sichert die Benutzung der DV-Anlagen durch diverse Zugangskontrollen, so dass ausschließlich befugte Personen zugreifen können. Jeder Zugang erfordert die Identifikation und die Authentifikation des Benutzers. Zugänge von außen sind an allen Standorten mittels Firewall gesichert.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Authentifikation mit Benutzername und Passwort
- Benutzerprofile
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie
- Passwortvergabe/Passwortregeln
- Pflicht für automatische Bildschirmsperre (lokal)
- Schlüsselregelung und Schlüsselbuch (Verwendung von Sicherheitsschlüsseln)
- Verschlüsselung externer/mobiler Datenträger
- Verschlüsselung interner Datenträger
- Verwaltete Benutzer und Benutzerberechtigungen

4.1.3 Zugriffskontrolle

Im Folgenden werden Maßnahmen der COSMO CONSULT aufgeführt, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Berechtigungskonzept (AD-Gruppen, Rollendefinitionen)
- Einsatz von Aktenvernichtern oder Sammelbehältern (Aktenentsorgungssystem)
- Passwortrichtlinie
- Verwaltung der Benutzerrechte durch Administratoren

4.1.4 Trennungskontrolle

Im Folgenden werden Maßnahmen aufgeführt, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Datenbank- und Mandantentrennung
- Festlegung der Zugriffsrechte für unterschiedliche Mandanten/Kunden
- Trennung von Produktiv- und Testsystem

4.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.2.1 Weitergabekontrolle

Im Folgenden werden Maßnahmen der COSMO CONSULT aufgeführt, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Nutzungsregelung für externe/mobile Datenträger
- Sorgfältige Auswahl von Personal
- VPN-Verbindung in das COSMO CONSULT Netzwerk

Beschreibung der durch den Auftraggeber zu treffenden Maßnahmen:

- Protokollierung von Datenübermittlungen
- VPN-Verbindung in das Netzwerk des Auftraggeber

4.2.2 Eingabekontrolle

Im Folgenden werden Maßnahmen von COSMO CONSULT aufgeführt, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die technischen und organisatorischen Maßnahmen im Hinblick auf die Eingabekontrolle sind auf Seiten des Auftraggebers zu treffen.

Beispielsweise obliegt das Vergeben von individuellen Benutzernamen anstelle von Sammellogins für ganze Mitarbeiter-Gruppen oder -Teams (der COSMO CONSULT; zur Betreuung des Auftraggebers) sowie das Protokollieren von Daten-Eingaben/-Änderungen usw. dem Auftraggeber, so dass eine Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen von Daten im Produktivsystem möglich ist.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten (Änderungsprotokoll o. ä.)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.3.1 Verfügbarkeitskontrolle

Im Folgenden werden Maßnahmen der COSMO CONSULT aufgeführt, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind oder im Falle eines Zwischenfalles rasch wiederhergestellt werden können.

Die technischen und organisatorischen Maßnahmen im Hinblick auf die Eingabekontrolle sind auf Seiten des Auftraggebers zu treffen.

Die durch COSMO CONSULT getroffenen technischen und organisatorischen Maßnahmen dienen ausschließlich internen/eigenen Zwecken von COSMO CONSULT und einer Gewährleistung der Arbeitsfähigkeit und Verfügbarkeit.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Aufbewahrung von Datensicherung an einem sicheren Ort
- Feuerlöschgeräte in lokalen Serverräumen (oder in erforderlicher Nähe)
- Vorkehrungen für Backup- & Recovery

4.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.4.1 Auftragskontrolle

Im Folgenden werden Maßnahmen von COSMO CONSULT aufgeführt, die gewährleisten, dass personenbezogene Daten, die im Auftrag von COSMO CONSULT durch weitere Dienstleister verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Eine Auflistung der genehmigten Subunternehmen wird unter https//www.cosmoconsult.com/data-protection regelmäßig aktualisiert. Die Kunden werden im Änderungsfall per E-Mail vorab informiert.

Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Vertragliche Festlegung von Art und Umfang sowie Zweck der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers;
- Nur auf schriftliche Auftragsverarbeitungsvereinbarungen
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimniss

4.4.2 Organisationskontrolle

Im Folgenden werden Maßnahmen aufgeführt, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.

- Beschreibung der von COSMO CONSULT getroffenen Maßnahmen:
- Beachtung Datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO
- Datenschutz Management
- Einbindung des globalen Datenschutzkoordinatoren und des externen Datenschutzbeauftragten sofern die betrieblichen Prozesses dies erfordern
- Organisationshandbuch am Standort
- Regelmäßige Audits zur Einhaltung der TOMs
- Regelmäßige Belehrungen
- Standards und Regelungen für IT-Sicherheit
- Standards und Regelungen zur Sicherung des Datenbestandes

5 Ansprechpartner

5.1 Globaler Datenschutzkoordinator

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 Externer Datenschutzbeauftragter

2b Advice GmbH

Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

email: cosmoconsult@2b-advice.com

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