COSMO CONSULT
Business-Software für Menschen

DATENSCHUTZ UND DATENSICHERHEIT BEI COSMO CONSULT

Version: 3.1| 27.11.2018

Inhaltsverzeichnis

1. Allgemeine Datensicherungsmaßnahmen bei COSMO CONSULT

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 ihren 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 der 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 i. d. R. 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; i. d. R. 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 solange aufrecht erhalten, 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.

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 EU 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 oder nur berechtigten Mitarbeitern, des jeweiligen Projekt- oder Kundenbetreuungsteams, zugänglich.

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

2. Technische und organisatorische Datenschutzmaßnahmen

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 des 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.

2.5 Standorte der Datenverarbeitung

2.5.1 Zentrales Rechenzentrum der COSMO CONSULT

COSMO CONSULT betreibt alle zentralen Dienste und Server in Microsoft Azure

Siehe auch: https://azure.microsoft.com

2.5.2 Standorte der 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 Gruppe.

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

2.5.3 Datenverarbeitung in Microsoft Azure

Soweit im Rahmen von Kundenaufträgen die Daten auf der Azure-Plattform gehostet werden und eine Übermittlung auch von personenbezogenen Daten außerhalb Europas nicht ausgeschlossen werden kann, wurde mit Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland ein Vertrag nach den gesetzlichen Vorgaben geschlossen. Die Angemessenheit des Datenschutzniveaus wird zusätzlich über eine aktuell gültige Zertifizierung nach dem sog. Privacy Shield gewährleistet.

Nähere Informationen unter:

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

2.6 Zutrittskontrolle

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

Lokale Serverräume (sofern zutreffend) sind an allen Standorten innerhalb der Bürogebäude zusätzlich gesichert.

2.6.1 Technisch

Art	Maßgabe
Zutrittskontrolle	Ja
Schließsystem	Ja

2.6.2 Organisatorisch

Art	Maßgabe
Besucheranmeldung beim Empfang	Ja
Persönliche/beaufsichtige Besucherführung	Ja
Schlüsselregelung und Schlüsselbuch (Verwendung von Sicherheitsschlüsseln)	Ja

2.7 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.

2.7.1 Technisch

Art	Maßgabe
Authentifikation mit Benutzername und Passwort	Ja
Einsatz von Anti-Viren-Software	Ja
Einsatz von Firewalls	Ja
Einsatz von VPN-Technologie	Ja
Verschlüsselung interner Datenträger (int. HD)	Ja
Verschlüsselung externer (mobiler) Datenträger (USB-Sticks, ext. HD, DVD usw.)	Ja

2.7.2 Organisatorisch

Art	Maßgabe
Verwaltete Benutzer und Benutzerberechtigungen	Ja
Passwortvergabe/Passwortregeln	Ja
Benutzerprofile	Ja
Pflicht für automatische Bildschirmsperre (lokal)	Ja
Schlüsselregelung und Schlüsselbuch (Verwendung von Sicherheitsschlüsseln)	Ja

2.8 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.

2.8.1 Technisch

Art	Maßgabe
Einsatz von Aktenvernichtern oder Sammelbehältern (Aktenentsorgungssystem)	Ja
Brechtigungskonzept	Ja

2.8.2 Organisatorisch

Art	Maßgabe
Berechtigungskonzept (AD-Gruppen, Rollendefinitionen)	Ja
Passwortrichtlinie inkl. Länge und Wechsel	Ja
Verwaltung der Benutzerrechte durch Systemadministratoren	Ja

2.9 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.

2.9.1 Technisch

Art	Maßgabe
Protokollierung von Datenübermittlungen	Auftraggeber
VPN-Tunnel (sichere Leitung) ins Netzwerk der COSMO CONSULT	Ja
VPN-Tunnel (sichere Leitung) ins Netzwerk der Auftraggeber	Auftraggeber

2.9.2 Organisatorisch

Art	Maßgabe
Sorgfältige Auswahl von Personal	Ja
Nutzungsregelung für externe (mobile) Datenträger	Ja

2.10 Eingabekontrolle

Im Folgenden werden Maßnahmen der 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.

2.10.1 Besonderheiten/Hinweise

Die TOM im Hinblick auf die Eingabekontrolle sind auf Seiten des Auftraggebers (Kunde) 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.

2.10.2 Technisch

Art	Maßgabe
Protokollierung der Eingabe, Änderung und Löschung von Daten (Änderungsprotokoll o. ä.)	Auftraggeber

2.10.3 Organisatorisch

Art	Maßgabe
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	Auftraggber
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	Auftraggeber

2.11 Auftragskontrolle

Im Folgenden werden Maßnahmen der COSMO CONSULT aufgeführt, die gewährleisten, dass personenbezogene Daten, die im Auftrag der 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 Email vorab informiert.

2.11.1 Organisatorisch

Art	Maßgabe
Nur auf schriftliche Auftragsverarbeitungsvereinbarungen	Ja
Schriftliche Weisungen an den Auftragnehmer	Ja
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	Ja
Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis	Ja

2.12 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.

2.12.1 Besonderheiten/Hinweise

Die TOM im Hinblick auf die Verfügbarkeitskontrolle sind auf Seiten des Auftraggebers (Kunde) zu treffen. Die getroffenen TOM dienen ausschließlich internen/eigenen Zwecken der COSMO CONSULT und einer Gewährleistung der Arbeitsfähigkeit und Verfügbarkeit.

2.12.2 Technisch

Art	Maßgabe
Feuerlöschgeräte in lokalen Serverräumen (oder in erforderlicher Nähe)	Ja

2.12.3 Organisatorisch

Art	Maßgabe
Aufbewahrung von Datensicherung an einem sicheren Ort	Ja
Vorkehrungen für Backup- & Recovery	Ja

2.13 Trennungskontrolle

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

2.13.1 Technisch

Art	Maßgabe
Trennung von Produktiv- und Testsystem	**Ja**
Datenbank- und Mandantentrennung	**Ja**

2.13.2 Organisatorisch

Art	Maßgabe
Festlegung der Zugriffsrechte für unterschiedliche Mandanten/Kunden	Ja

2.14 Organisationskontrolle

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

2.14.1 Organisatorisch

Art	Maßgabe
Standards und Regelungen für IT-Sicherheit	Ja
Standards und Regelungen zur Sicherung des Datenbestandes	Ja
Organisationshandbuch am Standort	Ja
Reglmäßige Audits zur Einhaltung der TOMs	Ja
Regelmäßige Belehrungen	Ja

3. Datenschutzbeauftragter

Marco Schröder

Kontaktdaten:
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