



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Im bisher geltenden BDSG wurden die technisch-organisatorischen Maßnahmen (TOM's) wie folgt festgelegt:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

Nach der EU-DSVGO versteht man unter technisch-organisatorischen Maßnahmen:

1. Vertraulichkeit
 - Zutrittskontrolle
 - Zugangskontrolle'
 - Zugriffskontrolle
 - Trennungskontrolle
 - Pseudonymisierung
2. Integrität
 - Weitergabekontrolle
 - Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit
 - Verfügbarkeitskontrolle
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
 - Datenschutz-Management
 - Incident-Response-Management
 - Datenschutzfreundliche Voreinstellungen
 - Auftragskontrolle



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Im Unternehmen umgesetzte technische und organisatorische Maßnahmen nach § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG.

Unternehmensangaben des Auftragnehmers	
Name des Unternehmens	COS Computer GmbH
Anschrift	Am Pfahlgraben 4-10, 35415 Pohlheim
Ansprechpartner	Christoph Runge (Geschäftsführer COS)
Nachfolgende Angaben gelten für den Standort	Baesweiler, Pohlheim

Datenschutzbeauftragter	
<input checked="" type="checkbox"/> Ja, es muss ein Datenschutzbeauftragter gem. § 4f BDSG schriftlich bestellt werden	
<input type="checkbox"/> Ja, es wurde ein Datenschutzbeauftragter freiwillig und schriftlich bestellt	
Name des Datenschutzbeauftragten	Peter Engel
Kontaktdaten	datenschutz@cos-computer.com
Schriftliche Bestellung vom	02.10.2018

Adressänderungen oder Änderungen zu den Bestellvoraussetzungen eines Datenschutzbeauftragten werden dem Auftraggeber unverzüglich mitgeteilt.



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Verpflichtung der Mitarbeiter
<input checked="" type="checkbox"/> Die Verpflichtung gemäß § 5 BDSG aller Mitarbeiter, die auf personenbezogene Daten des Auftraggebers zugreifen können, werden vor Auftragsbeginn durchgeführt
<input checked="" type="checkbox"/> Wo zutreffend, sind die beteiligten Mitarbeiter auch auf das Fernmeldegeheimnis verpflichtet
<input type="checkbox"/> Die Mitarbeiter sind auf den § 17 UWG verpflichtet
<input type="checkbox"/> Die Verpflichtungen sind dokumentiert und werden dem Auftraggeber auf Verlangen vorgelegt
<input checked="" type="checkbox"/> Zur Auftragsvergabe werden die beteiligten Mitarbeiter über die sich aus dem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung nachvollziehbar belehrt
<input type="checkbox"/> Weitere Verpflichtungen gem.:

1 Zutrittskontrolle

Der unbefugte räumliche Zutritt ist zu verhindern.

Gelände		
<input checked="" type="checkbox"/> Das Betriebsgelände liegt in einem Gewerbegebiet	<input type="checkbox"/> Das Betriebsgelände liegt in einem Wohngebiet	<input checked="" type="checkbox"/> Das Betriebsgelände ist eingezäunt
<input type="checkbox"/> Die Geländegrenzen werden videoüberwacht	<input checked="" type="checkbox"/> Sicherheitsdienst führt Kontrollgänge auf dem Betriebsgelände durch	<input checked="" type="checkbox"/> Zwei zentrale überwachte Zugänge zum Gelände
<input checked="" type="checkbox"/> Die Besucher müssen sich anmelden und werden begleitet	<input checked="" type="checkbox"/> Das Gebäude wird videoüberwacht	



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Gebäude		
<input checked="" type="checkbox"/> Die Gebäudetüren sind einbruchhemmend	<input checked="" type="checkbox"/> Die Gebäudetüren sind mit einer Alarmanlage gesichert	<input checked="" type="checkbox"/> Sicherheitsdienst führt Kontrollgänge innerhalb der Gebäude durch
<input checked="" type="checkbox"/> Die Gebäudetüren sind mit einem Zugangskontrollsystem gesichert	<input checked="" type="checkbox"/> Die Besucher müssen sich anmelden und werden begleitet	

Gebäudefenster		
<input checked="" type="checkbox"/> Die Gebäudefenster sind durch eine Alarmanlage gesichert	<input type="checkbox"/> Die Gebäudefenster sind mit Rollläden gesichert	<input checked="" type="checkbox"/> Die Gebäudefenster sind einbruchhemmend
<input type="checkbox"/> Die Fenster befinden sich oberhalb des Erdgeschosses		

Türen innerhalb des Gebäudes		
<input checked="" type="checkbox"/> Die Türen (Logistikbereich) sind mit einer Alarmanlage gesichert	<input checked="" type="checkbox"/> Die Türen sind einbruchhemmend	

Schlüssel		
<input checked="" type="checkbox"/> Dokumentierte Schlüsselaus- und -rückgabe (Schlüsselbuch)	<input checked="" type="checkbox"/> Dokumentierte Transponderaus- und -rückgabe (Transponderbuch)	



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Einbruchmeldeanlage		
<input type="checkbox"/> Aufschaltung zur Polizei	<input checked="" type="checkbox"/> Aufschaltung zum Sicherheitsdienst	<input type="checkbox"/> Aufschaltung zum Firmeninhaber/ zu Firmenangehörigen
<input checked="" type="checkbox"/> Glasbruchdetektoren an den Fenstern installiert	<input checked="" type="checkbox"/> Bewegungsmelder	<input type="checkbox"/> Ansprache durch Sicherheitsdienst möglich

Brandmeldeanlage		
<input checked="" type="checkbox"/> Feuer- und Rauchmelder sind in den Betriebsräumen installiert	<input checked="" type="checkbox"/> Aufschaltung zur Feuerwehr	<input checked="" type="checkbox"/> Feuerlöscher vorhanden

2 Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Benutzeranmeldung		
<input checked="" type="checkbox"/> Jeder Anwender hat einen eigenen Benutzernamen und ein eigenes Passwort	<input type="checkbox"/> Anmeldung per Magnetkarte	<input type="checkbox"/> Anmeldung per Chipkarte
<input type="checkbox"/> Automatische Anmeldung	<input type="checkbox"/> Anmeldung nur innerhalb bestimmter Zeiten möglich	

Passwortkonventionen		
<input checked="" type="checkbox"/> Sperrung bei wiederholter Fehleingabe	<input checked="" type="checkbox"/> Festgelegte Mindestlänge	<input checked="" type="checkbox"/> Ausschluss von Trivialpassworten
<input checked="" type="checkbox"/> Festgelegte Gültigkeitsdauer	<input checked="" type="checkbox"/> Verwendung von Sonderzeichen	<input checked="" type="checkbox"/> Änderung bei der ersten Anmeldung
<input checked="" type="checkbox"/> Ausschluss bereits benutzter Passwörter (3 alte Passwörter)	<input checked="" type="checkbox"/> Kontrolle der Passwortkonventionen	



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Bildschirmschoner		
<input type="checkbox"/> Automatische Aktivierung des Bildschirmschoners	<input checked="" type="checkbox"/> Deaktivierung des Bildschirmschoners nur mit Passworteingabe möglich	

Firewall		
<input checked="" type="checkbox"/> Das LAN ist mit einer Firewall gegen das Internet abgeschottet	<input checked="" type="checkbox"/> Die Firewall ist mit einem Anti-Viren-Programm ausgestattet	<input checked="" type="checkbox"/> Das Anti-Viren-Programm der Firewall wird automatisch mit den neusten Anti-Viren-Signaturen versehen
<input checked="" type="checkbox"/> Aktives IDS (Intrusion Detection System) Nur Skype	<input checked="" type="checkbox"/> Aktives IPS (Intrusion Prevention System) Nur Skype	<input checked="" type="checkbox"/> Stateful Packet Inspection
<input checked="" type="checkbox"/> Deep Packet Inspection	<input type="checkbox"/> Dokumentierte Penetrationstests	

Anti-Viren-Konzept		
<input checked="" type="checkbox"/> Jeder Rechner (Server, PC, Notebook, Stand-alone etc.) ist mit einem Anti-Viren-Programm ausgestattet	<input checked="" type="checkbox"/> Automatisches Update der Anti-Viren-Signaturen	<input checked="" type="checkbox"/> Zentrale Administration der Anti-Viren-Programme



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Sicherheits- / Programmupdates		
<input checked="" type="checkbox"/> Regelmäßiges Einspielen von Sicherheitsupdates	<input checked="" type="checkbox"/> Regelmäßiges Einspielen von Programmupdates	

WLAN-Nutzung		
<input type="checkbox"/> offenes WLAN	<input type="checkbox"/> Nutzung von WEP	<input type="checkbox"/> Nutzung von WPA
<input checked="" type="checkbox"/> Nutzung von WPA2	<input checked="" type="checkbox"/> Passwortvergabe unterliegt den Passwortkonventionen	<input type="checkbox"/> Protokollierung und Auswertung der Nutzung

Fernwartung		
<input checked="" type="checkbox"/> Ja, Fernwartung wird genutzt (nur von internen Admins)	<input type="checkbox"/> Nur nach vorheriger expliziter Freischaltung durch den Auftraggeber	<input checked="" type="checkbox"/> Ja, die Übertragung erfolgt verschlüsselt
<input checked="" type="checkbox"/> Ja, die Fernwartung wird protokolliert	<input checked="" type="checkbox"/> Ja, Verträge gem. § 11 BDSG mit externen Dienstleistern liegen vor und können eingesehen werden (kein externer Dienstleister)	



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

3 Zugriffskontrolle

Mit einem Berechtigungskonzept sind unerlaubte Tätigkeiten in den DV-Systemen zu verhindern.

Berechtigungskonzept		
<input checked="" type="checkbox"/> Ja, es ist ein dokumentiertes Berechtigungskonzept vorhanden und kann eingesehen werden (Active Directory)	<input checked="" type="checkbox"/> Systemtechnische Vergabe von Berechtigungen	<input checked="" type="checkbox"/> Ja, Rollenberechtigungen werden vergeben
<input checked="" type="checkbox"/> Ja, Gruppenberechtigung werden vergeben	<input checked="" type="checkbox"/> Ja, es erfolgt eine Kontrolle der Berechtigungen	<input checked="" type="checkbox"/> Ja, es gibt ein geregeltes Verfahren zum Entzug von Berechtigungen

Systemadministration		
<input checked="" type="checkbox"/> Ja, die Administration der IT-Systeme erfolgt intern	<input type="checkbox"/> Ja, es erfolgt eine Prüfung und Wartung auch durch externe Dienstleister vor Ort	<input type="checkbox"/> Ja, es erfolgt eine Prüfung und Wartung auch durch einen externen Dienstleister per Fernwartung
<input type="checkbox"/> Ja, Verträge gem. § 11 BDSG mit externen Dienstleistern liegen vor und können eingesehen werden		



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

4 Weitergabekontrolle

Die Weitergabe (elektronische Übertragung, Datentransport, Übermittlungskontrolle etc.) personenbezogener Daten ist zu regeln.

Datenträger		
<input checked="" type="checkbox"/> Schreibender Zugriff auf externe Datenträger ist möglich (nicht Einkauf, nicht Vertrieb)	<input type="checkbox"/> Externe Datenträger sind inventarisiert	<input type="checkbox"/> Datenbestände auf externen Datenträgern sind verschlüsselt
<input checked="" type="checkbox"/> Explizites Verbot zur Nutzung privater Speichermedien (BV)		

Datenträgervernichtung		
<input checked="" type="checkbox"/> Vernichtung von Papierdokumenten mittels Schredder	<input type="checkbox"/> Vernichtung von Festplatten, CD, DVD etc. durch zertifizierten Entsorger gem. § 11 BDSG	<input type="checkbox"/> Vernichtung von Akten durch zertifizierten Entsorger gem. § 11 BDSG

Weitergabe von personenbezogenen Daten		
<input type="checkbox"/> Ja, es gibt eine interne Regelung für die Weitergabe von Daten	<input checked="" type="checkbox"/> Weitergabe von Daten per Internet	<input type="checkbox"/> Verschlüsselte Weitergabe
<input checked="" type="checkbox"/> Weitergabe von Daten per E-Mail	<input checked="" type="checkbox"/> Weitergabe von Daten per E-Mail mit verschlüsseltem Dateianhang	<input checked="" type="checkbox"/> Netzwerklaufwerk
<input checked="" type="checkbox"/> Nutzung VPN	<input checked="" type="checkbox"/> Weitergabe von Daten per Briefpost	<input type="checkbox"/> Weitergabe von Daten per Kurier
<input checked="" type="checkbox"/> Weitergabe von Daten per Fax		



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

Cloud-Services	
<input type="checkbox"/> Ja, es werden Cloud-Services genutzt	<input checked="" type="checkbox"/> Nein, es werden keine Cloud-Services genutzt
<input type="checkbox"/> Ja, die Daten liegen ausschließlich in der EU/EWR	<input type="checkbox"/> Nein, die Daten liegen außerhalb der EU/EWR
<input type="checkbox"/> Ja, mit dem Cloud-Service-Provider liegt ein Vertrag gemäß § 11 Bundesdatenschutzgesetz (BDSG) vor und kann eingesehen werden	

Fernwartung durch Externe
<input checked="" type="checkbox"/> Ja, Prüfung und Wartung von Datenverarbeitungsanlagen und automatisierten Verfahren erfolgt mittels Fernwartung durch Externe
<input checked="" type="checkbox"/> Ja, Verträge gem. § 11 BDSG mit den Externen liegen vor und können eingesehen werden
<input checked="" type="checkbox"/> Ja, explizite Freischalung durch den Auftraggeber
<input type="checkbox"/> Ja, die Fernwartung wird durch fachkundige Mitarbeiter beaufsichtigt
<input checked="" type="checkbox"/> Ja, es erfolgt eine Protokollierung der Fernwartung

5 Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege.

Protokollierung		
<input checked="" type="checkbox"/> An- und Abmeldung	<input checked="" type="checkbox"/> Programmausführung	<input checked="" type="checkbox"/> Schreiben von Daten
<input checked="" type="checkbox"/> Lesen von Daten	<input checked="" type="checkbox"/> Löschen von Daten	<input checked="" type="checkbox"/> auf Datenfeld-Ebene
<input checked="" type="checkbox"/> auf Datensatz-Ebene	<input checked="" type="checkbox"/> auf Datei-Ebene	<input checked="" type="checkbox"/> Systemprotokollierung
<input checked="" type="checkbox"/> Auswertung der Protokollierung		



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

6 Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung gem. § 11 BDSG ist zu gewährleisten.

Auftragsdatenverarbeitung (ADV) gem. § 11 BDSG		
<input checked="" type="checkbox"/> Ja, es liegen Vertragsverhältnisse gem. § 11 BDSG vor	<input checked="" type="checkbox"/> Ja, die Vorgaben des § 11 BDSG und die Weisungen des Auftraggebers sind bekannt, werden eingehalten und kontrolliert	<input type="checkbox"/> sonstiges

7 Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Serverraum		
<input checked="" type="checkbox"/> Separater Serverraum	<input checked="" type="checkbox"/> Brandschutzmaßnahmen (eigener Brandabschnitt, feuerhemmende Tür, Feuerlöscher)	<input checked="" type="checkbox"/> Feuer- und Rauchmelder im Serverraum installiert
<input checked="" type="checkbox"/> Klimaanlage mit Ausfallmeldung	<input checked="" type="checkbox"/> Alarmierung bei Temperaturabweichung, sonst s. unter 1	<input checked="" type="checkbox"/> Separater Schließkreis
<input checked="" type="checkbox"/> Protokollierter Zugang	<input checked="" type="checkbox"/> Einbruchhemmende Tür	<input checked="" type="checkbox"/> Unterbrechungsfreie Spannungsversorgung
<input checked="" type="checkbox"/> Separate Absicherung jedes Stromkreises	<input checked="" type="checkbox"/> Spannungsversorgung mit Netzfilter	

Datensicherungskonzept
<input checked="" type="checkbox"/> Ja, die Daten werden gem. eines Sicherungskonzepts gesichert (noch nicht dokumentiert)
<input type="checkbox"/> Ja, dass Sicherungskonzept ist einsehbar



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

IT-Redundanzen

Ja, Systeme sind redundant ausgelegt (zweiter Serverraum noch nicht eingerichtet)

Virtualisierung

Ja, Server/Dienste sind virtualisiert

Ja, die virtualisierten Server/Dienste sind im Datensicherungskonzept eingebunden (nicht dokumentiert)

Systempassworte

Ja, Systempassworte sind für den Notfall sicher hinterlegt (mündlich fünf Administratoren)

8 Trennungsgebot

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Trennung

Mandantentrennung durch Software

Physische Trennung der Daten

Logische Trennung der Daten

Trennung über Zugriffsregelungen

Trennung von Test- / Produktionsdaten



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

9 Pseudonymisierung

Maßnahmen, die gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.

<input type="checkbox"/> Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	<input checked="" type="checkbox"/> Es werden geeignete technisch-organisatorische Maßnahmen zur Aufbewahrung der Zuordnungsdatei ergriffen	<input type="checkbox"/> Sonstiges
<input checked="" type="checkbox"/> Die Pseudonymisierung ist im Verarbeitungssystem so früh wie möglich durchzuführen	<input checked="" type="checkbox"/> Pseudonymisierung wird zum Schutz der Vertraulichkeit, wann immer möglich, praktiziert	

10 Datenschutzmanagement

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

<input checked="" type="checkbox"/> Regelmäßige Schulungen der Mitarbeiter/-innen zum Datenschutz	<input type="checkbox"/> Datum der letzten Schulung:	<input checked="" type="checkbox"/> Ein VVT ist vorhanden, vollständig und aktuell
<input type="checkbox"/> Es bestehen Standards für die IT-Sicherheit (IT Grundschutz BSI, ISO 27001, etc.)	<input checked="" type="checkbox"/> Die Aufbewahrung der elektronischen Protokolle ist geregelt	<input checked="" type="checkbox"/> Es gibt Regelungen für die Sicherung des Datenbestandes



Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

<input checked="" type="checkbox"/> Schriftliche Bestellung eines Datenschutzbeauftragten	<input checked="" type="checkbox"/> Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden	<input checked="" type="checkbox"/> Ein Datenschutzkonzept ist vorhanden
<input checked="" type="checkbox"/> Datenschutz-Folgeabschätzungen (sofern erforderlich) werden durchgeführt und protokolliert	<input checked="" type="checkbox"/> Protokoll- und Logdateien werden anlassbezogen ausgewertet	<input checked="" type="checkbox"/> Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert
<input type="checkbox"/> Es besteht ein Löschkonzept nach DIN 66398	<input checked="" type="checkbox"/> Transparenzpflichten werden eingehalten	<input checked="" type="checkbox"/> Accountabilität wird beachtet

11 Incident-Response Management

Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.

<input checked="" type="checkbox"/> Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne	<input checked="" type="checkbox"/> Ein Konzept zur Meldung von Datenpannen an den Auftraggeber ist in Arbeit	<input checked="" type="checkbox"/> Ein internes Incident-Response-Management Konzept ist in Arbeit
--	---	---



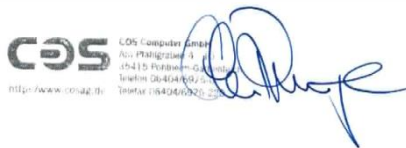
Anlage 1

Angaben des Auftragnehmers gem. § 11 BDSG zu § 9 BDSG und Anlage

12 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

<input checked="" type="checkbox"/> Privacy by Design wird beachtet	<input checked="" type="checkbox"/> Privacy by Default ist eingestellt	<input type="checkbox"/> Sonstiges



COS Computer GmbH
Am Pfahlgraben 4-10
35415 Pohlheim, Germany
Telefon 06404 6975-0
Telefax 06404 6975-220
http://www.cos-ag.de

Baesweiler, 22.05.2018

COS Computer GmbH