ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Technische und organisatorische Maßnahmen gemäß Artikel 32 der Verordnung (EU) 2016/679 - "DSGVO"				
Zutrittskontrolle und Zugangskontrolle Dieses Kapitel behandelt mögliche Maßnahmen um Unbefugten den Zutritt zu Anlagen, in denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. (Schutz vor unbefugtem Zutritt: z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen)				
		Ja	**Nein**	**Sonstige Anmerkungen**
1.	Sind die Gebäude mit einer Einbruchmeldeanlage und Videoüberwachung gesichert?			
2.	Gibt es ein geregeltes Konzept für die Zugangsberechtigung?			
3.	Wird die Anwesenheit überprüft (zB Schichtbuch, Stechuhren, Portier)?			
4.	Ist der Eingang mit einem Schließsystem ausgestattet? Falls ja, mit welchem (z.B. ein manuelles Schließsystem oder ein Chip-Card basiertes Schließsystem)?			
5.	Wird dokumentiert, wer eine Zugangsberechtigung für das eben erwähnte Schließsystem besitzt?			
6.	Wird dokumentiert, welche externen Personen Zugang zum Gebäude hatten?			
7.	Sind die Datenzentren und Serverräume verschlossen oder werden die physischen Zugänge zu ihnen überwacht?			

8.	Ist die Entziehung der Zugangsberechtigung und der Zugriffsrechte auf die Computersysteme im Falle der Beendigung eines Arbeitsverhältnisses geregelt und wird dokumentiert?			
9.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Zugriffskontrolle Dieses Kapitel behandelt mögliche vorbeugende Maßnahmen, die eine unautorisierte Nutzung von Datenverarbeitungssystemen verhindern sollen.				
		Ja	**Nein**	**Sonstige Anmerkungen**
10.	Ist das Unternehmensnetzwerk vor Zugriffen aus dem öffentlichen Netzwerk durch eine Hardware-Firewall geschützt und wird diese aktuelle gehalten.			
11.	Werden alle IP-Adressen mit Zugang zum Internet regelmäßig Penetrationstests unterzogen?			
12.	Werden Mitarbeiter dazu angehalten, Passwörter mit folgenden Spezifikationen zu verwenden:			
	• Individuelles Passwort, welches geheim gehalten werden muss			
	• Mindestlänge			
	• Änderungsrhythmus			
	• Bildschirmsperre nach einer gewissen Zeit			
13.	Haben Mitarbeiter lokale Verwaltungsrechte?			
14.	Werden Virus Scanner an einem oder mehreren der folgenden Übergängen zum Unternehmensnetzwerks verwendet: • Internet • Email			

	• FTP – (File Transfer Protocol)			
15.	Werden auf allen Servern Virus Scanner verwendet?			
16.	Werden an allen individuellen Arbeitsplätzen Virus Scanner verwendet?			
17.	Werden die sicherheitsrelevanten Software-Patches regelmäßig und automatisch in die bestehende Software eingespielt?			
18.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Schutz vor Veränderung und Löschung Dieses Kapitel behandelt mögliche Maßnahmen, die gewährleisten sollen, dass Personen mit Zugang zu Datenverarbeitungssystemen nur im Rahmen ihrer Autorisierung Zugang zu den Daten haben, und dass personenbezogene Daten während der Bearbeitung, Nutzung und nach Aufzeichnung ohne Autorisierung nicht gelesen, kopiert, verändert oder gelöscht werden können.				
		Ja	**Nein**	**Sonstige Anmerkungen**
19.	Ist der Zugriff nur von personalisierten Accounts möglich?			
20.	Folgen Zugriffsrechte auf die IT-Systeme dem Least-Privilege-Prinzip? (Rechteminimierung)			
21.	Gibt es Fernwartung/Fernzugriff für Service Provider, Mitarbeiter oder andere?			
22.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Weitergabekontrolle Dieses Kapitel behandelt mögliche Maßnahmen, die (i) verhindern sollen, dass personenbezogene Daten während einer elektronischen Übertragung oder Übermittlung oder während ihrer Speicherung, unbefugt gelesen, kopiert, verändert oder gelöscht werden, und (ii) es ermöglichen sollen, festzustellen und zu überprüfen, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.				
		Ja	**Nein**	**Sonstige Anmerkungen**
23.	Wird der Datenabtausch zwischen Kunde und Provider verschlüsselt?			
24.	Sind Daten, die von einem Datenträger versendet werden (z.B. USB-Sticks) verschlüsselt?			
25.	Werden die Daten der Kunden verschlüsselt gespeichert?			
26.	Wurden Maßnahmen zum Schutz von Kundendaten (inkl. temporärer Daten) auf mobilen Arbeitsplätzen eingerichtet?			
27.	Wurden Maßnahmen zum Schutz von Kundendaten (inkl. temporärer Daten) auf mobilen Datenträgern (zB USB-Sticks, PDAs, externe Festplatten, Tablets, Smartphones) eingerichtet?			
28.	Werden die Daten der Kunden nach Auftragserfüllung gelöscht?			
29.	Gibt es ein Gesamtkonzept für die Entsorgung sämtlicher elektronischer Datenträger und Papierdokumente?			
30.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Eingabekontrolle Dieses Kapitel behandelt mögliche Maßnahmen, die gewährleisten sollen, dass es möglich ist, nachträglich zu überprüfen und festzustellen, ob und von wem personenbezogene Daten angesehen, geändert oder gelöscht wurden.				
		Ja	**Nein**	**Sonstige Anmerkungen**
31.	Werden Logfiles für die Nachvollziehbarkeit der Löschung oder Änderung von Kundendaten erstellt?			
32.	Werden diese Logfiles vor Änderungen geschützt?			
33.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Auftragskontrolle Dieses Kapitel behandelt mögliche Maßnahmen, die gewährleisten sollen, dass der Auftragsdatenverarbeiter die Daten nur im Rahmen und für die Zwecke der Auftragserfüllung verarbeitet.				
		Ja	**Nein**	**Sonstige Anmerkungen**
34.	Gibt es eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (insbesondere auch bei der Datensicherung und beim Datenträgertransport)?			
35.	Ist sichergestellt, dass Mitarbeiter Geheimhaltungspflichten unterliegen? Falls ja, wie (z.B. mittels gesonderter Geheimhaltungsvereinbarung oder generell, mit einer Geheimhaltungsklausel in den Verträgen der Mitarbeiter)?			
36.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Verfügbarkeitskontrolle Dieses Kapitel beschäftigt sich mit Maßnahmen, die sicherstellen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.				
		Ja	**Nein**	**Sonstige Anmerkungen**
37.	Sind Einrichtungen zum Brandschutz vorhanden (zB Feuerlöscher, Rauch- oder Brandmelder, allenfalls Rauchverbot)?			
38.	Ist eine unterbrechungsfreie Stromversorgung etabliert?			
39.	Ist der Backup-Server / Das Backup getrennt vom Standort des Rechenzentrum?			
40.	Werden Backups erstellt?			
41.	Werden Speichermedien sicher aufbewahrt?			
42.	Ist ein Neustart möglich, nachdem das komplette Datencenter zerstört wurde? Wie lange?			
43.	Bestehen Verträge über die Instandhaltung der IT Systeme mit externen Anbietern?			
44.	Gibt es zusätzliche Maßnahmen oder Informationen?			

	Trennungsgebot Dieses Kapitel beschäftigt sich mit möglichen Maßnahmen, um sicherzustellen, dass für verschiedene Zwecke erhobene Daten auch getrennt verarbeitet werden.			
		Ja	**Nein**	**Sonstige Anmerkungen**
45.	Werden die Kundendaten in einem separaten Teil der Datenbank aufbewahrt, der ausdrücklich der Auftragsabwicklung dient?			
46.	Gibt es ein Berechtigungskonzept, das verhindert, dass unberechtigte Personen auf Kundendaten zugreifen?			
47.	Werden die Arbeitnehmer angewiesen, keine Daten des Kunden in anderen Projekten oder für andere Zwecke zu verwenden?			
48.	Gibt es zusätzliche Maßnahmen oder Informationen?			

Organisationskontrolle Dieses Kapitel beschäftigt sich mit möglichen Maßnahmen zur Implementierung von umfassenden Datenschutzkonzepten und Informationssicherungsmethoden.				
		Ja	**Nein**	**Sonstige Anmerkungen**
49.	Bestehen schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen (zB Arbeitsanweisungen, Stellenbeschreibungen, Richtlinien)?			
50.	Findet eine interne Revision der Datenverarbeitung statt?			
51.	Wird auf etablierte Standards für die IT-Sicherheit bzw zur Abwicklung von IT-Projekten zurückgegriffen (IT-Grundschutz, etc)?			
52.	Hält der Auftragsverarbeiter derzeit folgende Zertifizierungen / Datenschutzkonzepte, die er diesem Fragebogen beifügt:			
	• ISO 27001/27002			
	• ISO 27018			
	• PCI DSS (amerikanische Datenschutzgrundnorm)			
	• Andere			