Technisch Organisatorische Maßnahmen (TOM) i. S. d. Art. 32 DSGVO

officePLUS
Beratungs- und Vertriebs GmbH für Büroorganisation Chemnitz
Kopernikusstraße 2, 09117 Chemnitz

Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität Stand 24.05.2018

Die o. g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

§1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen , mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Alarmanlage	Schlüsselregelung/ Liste
Schließsystem mit Transponder	Empfang
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter
Sicherheitsschlösser	separater Besucher-/ Kundenbereich
Türen mit Knauf Außenseite	
Fenster Werkstattbereich vergittert	
verschlossener Serverschrank	

1.2 Zugangskontrolle

Maßnahmen, zu verhindern, dass Datenverarbeitungssysteme (Computer, Server, Datenverabeitungsanlagen von Unbefugten genutzt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Anti-Viren-Software Server	Erstellen von Benutzerprofilen
Anti-Virus-Software Clients	Richtlinie „Sicheres Passwort“
Anti-Virus-Software mobile Geräte	Richtlinie „Löschen/ Vernichten“
Firewall	Allg. Richtlinie Datenschutz und/ oder Sicherheit
Einsatz VPN bei Remote-Zugriffen	Anleitung „Manuelle Desktopsperre“
Automatische Desktopsperre	
WLAN verschlüsselter Zugang	
Separates verschlüsseltes Gäste-WLAN	

1.3 Zugriffskontrolle

Maßnahmen, 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.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Aktenschredder (mind. Stufe 3, cross cut)	Funktionsbezogene Vergabe und Verwaltung von Zugriffsrechten (Verzeichnis, Dateien, Anwendungsprogramme)
kontrollierte Löschung und Vernichtung von Datenträgern	Minimale Anzahl an Administratoren
	Verwaltung der Benutzerrechte durch Administratoren
Protokollierung von Zugriffen in Anwendungsprogrammen, konkret bei der Eingabe, Änderung und Löschung von Daten	Funktionsbezogene Vergabe und Verwaltung von Zugriffsrechten in Anwendungsprogrammen (Datensätze, Datenfelder)

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Test-Umgebung durch Testmandanten in Datenbank	Funktionstrennung bei Vergabe von Benutzerrechten (je nach Aufgabenbereich)
Logische Mandantentrennung (softwareseitig)	Festlegung von Datenbankrechten
	Datensätze sind mit Zweckattributen versehen
	Zweckmäßige Verarbeitung von Daten in entsprechenden Anwendungsprogrammen

§2 Integrität (Art. 32 Abs. 1 lit. B DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, 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.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Email-Verschlüsselung	
Einsatz von VPN	
Bereitstellung über verschlüsselte Verbindungen wie https	

2.2 Eingabekontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis der Vergabe von Benutzerrechten
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

2.3 Auftragskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
	sorgfältige Auswahl des Auftragnehmers
	eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen
	klare und eindeutige Erteilung von Weisungen (im besten Fall in schriftlicher Form)
	Festlegung der zur Erteilung und zum Empfang von Weisungen berechtigten Personen
	Verpflichtung der Beschäftigten des Auftragnehmers auf das Datengeheimnis gemäß § 5 BDSG

§3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuerlöscher Serverraum	Backup & Recovery-Konzept
	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
USV	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Schutzsteckdosenleisten Serverraum	
RAID System / Festplattenspiegelung	
schnelle Wiederherstellung der Daten durch virtualisierte Serversysteme	

§4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

Ausgefüllt für die Organisation durch:

Name: Jens Klier
Funktion: Leiter Technik
Rufnummer: 0371 -- 80 80 68 0
Email: j.klier@officeplusgroup.de

Chemnitz, 24.05.2018
Ort, Datum

Vom Auftraggeber auszufüllen:

Geprüft am: _____ durch: _____ Ergebnis(se): _____

☑ Es besteht noch Klärungsbedarf zu _____
☑ TOM sind für den angestrebten Schutzzweck ausreichend
☑ Auftragsverarbeitungsvertrag kann geschlossen werden