Checkliste mobiler Arbeitsplatz – Corona Krise – COVID 19

Dieses Dokument dient zur Absicherung des Heimarbeitplatzes um Unternehmen vor Schaden zu bewahren.

Mangelhafte IT-Sicherheit führt zu Verlust von vertraulichen Informationen und Daten, aber auch Cyber-Angriffe bzw. Cyber-Kriminalität gefährdet Ihren Betrieb!

Für den Falle eines sogenannten „Data-Breach“, also einer Datenschutzverletzung nach EU-DSGVO Art. 33, dient diese Vorlage um sicherzustellen das alle notwendigen Maßnahmen getroffen wurden um Daten mit Personenbezug zu schützen.

Bitte nehmen Sie dieses Dokument ernst! Wir helfen Ihnen rasch unter der Hotline 0800 22 44 88 auch die angeführten Themen umzusetzen!

		Erfasst am:	……../……../2020	**:**	
Mitarbeiter (Dienstnummer)		**Erfasst durch:**		Tätigkeit:	
Standort Gerät (Adresse)				Erreichbarkeit über Mobiltelefon:	
				Betroffener in Quarantäne (COVID-19) oder Verdachtsfall?	☐ Ja ☐ Nein ☐ Nicht bekannt

INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes			
Datum	Information von:	Welches Betriebssystem ist auf dem Gerät installiert, Welche Sicherheitssoftware wird verwendet Verfügen Sie über eine Auflistung der privaten Applikationen am Gerät Verfügen Sie über Auflistung der unternehmensspezifischen Applikationen am lokalen Gerät Welche Applikationen haben Zugriff via Fernzugriff auf das Unternehmensnetzwerk Welcher Internetanbieter wird für den mobilen Arbeitsplatz herangezogen (Kontaktdaten, Leitungsdaten, Vertragsnummer) Welcher Firewall befindet sich am Standort Firewall und gibt es ein lokale WLAN	Geprüft von:

INF.9.A2 Regelungen für mobile Arbeitsplätze			
Datum	Information von:	Wer nutzt das mobile Gerät (Mitarbeiter, Personen die im Haushalt leben) Können Daten von dem Gerät kopiert werden (USB Stick, CD) Mit welchen Geräten ist das „Heimarbeitsplatz“ noch vernetzt (Musik, TV, Kamera, privates NAS, etc) Können Unternehmensdaten gesondert von privaten Daten getrennt werden. Verfügen Sie über eine Vereinbarung die es ermöglicht später die Unternehmensdaten anzufordern, zu löschen	Geprüft von:

INF.9.A3 Zutritts- und Zugriffsschutz			
Datum	Information von:	Ist der mobile Arbeitsplatz physisch absperrbar Wieviel Benutzeraccounts sind angelegt Welche Rechte haben diese Accounts Gibt es sichere Passwörter für alle Accounts	Geprüft von:

INF.9.A4 Arbeiten mit fremden IT-Systemen			
Datum	Information von:	Gibt es externe Dienstleister und haben Sie deren Kontaktdaten Werden nicht unternehmenseigene Geräte benutzt, die nicht vom Heimarbeitsplatzmitarbeiter stammen Werden externe Hosting-Dienste in Anspruche genommen und haben Sie hier Kontaktdaten, sowie die Beschreibung über Sicherheit und Verfügbarkeit	Geprüft von:

INF.9.A5 Zeitnahe Verlustmeldung			
Datum	Information von:	Verfügen Sie über eine Ablaufbeschreibung wie mit dem Verlust, Diebstahl oder Defekt eines Gerätes umgegangen werden soll Wir rasch sollen und können Ersatzgeräte gestellt werden Welche Daten befinden sich auf dem Gerät und sind diese bei Verlust gegen Fremdzugriff geschützt (Verschlüsselung)	Geprüft von:

INF.9.A6 Entsorgung von vertraulichen Informationen			
Datum	Information von:	Ist es erforderlich vertrauliche Informationen nach Ihrem Verwendungszweck zu entsorgen. Verfügt der Mitarbeiter über geeignete Mittel wie Schredder (DIN 66399-2) Sind Mitarbeiter geschult und informiert wie sie mit vertraulichen Informationen umgehen müssen Wie ist der Ablauf wenn der Mitarbeiter auf Grund einer Erkrankung nicht mehr am Heimarbeitsplatz ist und Sie alle vertraulichen Dokumente sichern müssen (Notfall Nummern Verwandte, Freundeskreis)	Geprüft von:

INF.9.A7 Rechtliche Rahmenbedingungen für das mobile Arbeiten			
Datum	Information von:	Gibt es eine Betriebsanweisung das mobile Arbeiten Gibt es eine Vereinbarung die im Falle einer Kündigung, längeren Krankheit oder eines Todes die Rechte des Unternehmens regeln um an die Firmendaten zu gelangen. Sind Verhaltensregeln auf die mobile Heimarbeit angepasst worden	Geprüft von:

INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze			
Datum	Information von:	Sind die IT-Sicherheitsrichtline und die Datenschutzrichtline auf mobiles Arbeiten angepasst Sind die Mitarbeiter auf die geänderten Maßnahmen geschult worden	Geprüft von:

INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger			
Datum	Information von:	Beschreiben Sie welche Technologien zur Datenverschlüsselung zum Einsatz kommen. Sind Backup- und Recovery Abläufe vorhanden und getestet	Geprüft von:

INF.9.A10 Einsatz von Diebstahlsicherungen			
Datum	Information von:	Beschreiben Sie wie mobilen Geräte vor Diebstahl und unbefugtem Zugriff gesichert werden. Können Sie gestohlen mobile Geräte verfolgen (GPS-Tracking, Google-Accounts, etc)	Geprüft von:

INF.9.A11 Verbot der Nutzung unsicherer Umgebungen			
Datum	Information von:	Gibt es die Möglichkeit zu erkennen, dass ein mobiler Arbeitsplatz zu einem Risiko geworden ist (Software, Monitoring) Gibt es die Möglichkeit zu erkennen, dass Mitarbeiter Unternehmensdaten zweckentfremden	Geprüft von:

Erstellt von Karl Pusch zertifizierter Datenschutzbeauftragter, externer Datenschutzbeauftragter und geprüfter Auditor (Zert.Nr. 2875090

DPO Consult GmbH

Am Eisernen Tor 2/III

A-8010 Graz

+43 676 39 96 040

+43 316 43 70 00 - 200

+43 316 43 70 00 - 702

karl.pusch@dpo.at

Wir wünschen den betroffenen der Corona-Krise, aber auch jenen die mittel- und unmittelbar mit den Auswirkungen konfrontiert sind, alles Gute in der nächsten Zeit!