Checkliste für DSGVO Empfehlungen

Zielgruppe: Fitnesstrainer, Fitnesscoaches und selbstständige Einzelunternehmer

	Was gilt für die bestimmten Flächen?	**Was sollte ich einhalten in den jeweiligen Räumen?**
	Bürofläche	Aufstellen des Arbeitsplatzes sichtgeschützt Abgeschlossener Raum Daten in einem extra abgeschlossenen Behälter
	Mietwohnung	Nur Mieter hat die Schlüssel Daten dennoch in einem extra abgeschlossenen Behälter
	Öffentlicher Platz	Keinerlei Arbeiten durchführen, Sichtungsgefahr
	Bahn / Bus	Aufgrund der Videoüberwachung keinerlei Tätigkeiten!!
	Welche Schritte am Arbeitsgerät zur Erhöhung der Sicherheit?	**Was sollte ich einrichten oder benutzen?**
	Notebooks:	
	BIOS Kennwort festlegen	Nutzen Sie ein starkes BIOS Kennwort, einzigartig
	Windows Kennwort einzigartig und komplex	Anmeldekennwort sollte einzigartig sein
	Mac-OS Anmeldung einzigartig und komplex	Anmeldekennwort sollte einzigartig sein
	Tablets:	
	Kennwort und PIN festlegen, wenn möglich biometrische Entsperrung nutzen	Kennwörter auf Tablets, zusätzlich PIN festlegen, Umgehung einer einfachen Sicherheit innerhalb weniger Minuten.
	iPad – Apple-ID Kennwort	Häufiges wechseln des Kennwortes da Geräteübergreifend!
	Smartphones:	
	Android – Kennwort + biometrisch / PIN	Wenn möglich biometrisch nutzen, ansonsten PW + PIN
	iPhone – Apple ID-Kennwort + biometrisch	Nutzen Sie immer 2-Schichten! Apple erhöhte Sicherheit
	Was sollte ich bei Anwendungen und LogIns allgemein beachten?	
	Anwendungskennwörter / Programme	Komplexe, lange Kennwörter – alle 60 Tage ändern
	Banking Software	Je nach Anbieter maximale Komplexität, Kennwort häufig ändern. Nur Besitzer darf Kennwort kennen!
	Cloud-Programme und Speicher	Nur in Deutschland gehostete Produkte nutzen, Kennwort sehr häufig und regelmäßig wechseln, Beachten Sie die

		allgemeinen Geschäftsbedingen (AGB's) bezüglich Speicherort und Datenaufbewahrung!
	Kundendaten auf Notebook (Word/Excel)	Nur unter Passwortschutz, zentral an einem Ort gelagert
	CRM Programme	Passwortstärke beachten, wenn Cloud – deutsches Hosting
	Online-Anwendungen	Nur aus sicheren Netzwerken, LogOut-Time beachten, Abmeldung nach Nutzung, auf gültige SSL-Zertifikate achten und bei wichtigen Anwendungen HTTPS benutzen
	Online-Aktivitäten	Immer aktuellen Virenschutz benutzen, keine Freeware Anti-Viren-Programme, kein Besuch von unsicheren Seiten
	Zusätzliches	Immer aktuelle Browserversion nutzen, nur namentlich bekannte Browser (Firefox, Chrome und co.), vorzugsweise nur aus sicheren Netzwerken, keine öffentlichen HotSpots, nur WLANs mit starken Kennwörtern
	Verdacht auf Virus	Schnellst möglich kompetenten Service suchen, Bereinigung des Gerätes durch diesen durchführen lassen – dazu Verschwiegenheitserklärung unterschreiben lassen
	Hardware und allgemeine Tipps	
	Keine USB-Sticks/Festplatten/Cardreader oder auch SD-Cards nach Fund benutzen	Gespräche an öffentlichen Plätzen auf ein Minimum begrenzen um Kundendaten zu schützen
	Keine fremden Smartphones und Tablets anschließen	Keine Weitergabe von Kundendaten ohne vorherige Zustimmung und Einverständniserklärung
	Auf ungewünschte Webcam-Aktivität achten	Vermeintliche Microsoftanrufe in der Regel Phishing!
	Regelmäßig nach aktuellen Viren erkundigen	Interessenten und vermeintliche Kunden nur nach korrekter DSGVO konformer Kontaktaufnahme bearbeiten
	Keine unbekannten Emailanhänge öffnen	Informationen einholen zu korrektem Direktmarketing
	Excel verbieten Makros zu benutzen	Nicht mit veralteter Hardware arbeiten
	Auf Spam-Aktivitäten achten	Regelmäßig auf Updates und Firmeware-Updates prüfen
	In Netzwerken korrekte Speicherorte benutzen – nicht den Desktop	Vorsicht vor vermeintlichen DSGVO-Betrügern! Vermehrt Nachrichten per Post mit Zahlungsaufforderungen!
	Keine Kundendaten auf nicht dafür vorgesehen Speicherorten zwischenlagern	Bei unseriösen oder verdächtigen Schreiben und Anrufen Anwalt kontaktieren für juristisch-korrekte Rücksprachen
	Speichermedien bei Nichtbenutzung verschließen	Datenschutzbeauftragten nach Informationen und Durchführungsplänen fragen
	Regelmäßig BackUps und Sicherungen durchführen	Eigene Prozesse und Abläufe kennen und selbst strukturiert überarbeiten
	BackUps extern lagern, Empfehlung: doppelt	Suchen Sie sich einen IT-Partner für die Umsetzung

Für weitere Tipps und bei Rückfragen stehen wir Ihnen gerne zur Verfügung!

Weiterhin viel Erfolg bei Ihrer Arbeit und im weiteren Umgang mit der DSGVO wünschen Ihnen Patrick Oswald und Cedric Rahlff von der

VALKYRIE

IT-SOLUTIONS

Kontakt

www.it-norderstedt.de

Nutzen Sie bitte das Kontaktformular auf unserer Internetseite um einen DSGVO-konformen Kontakt herzustellen. Wir freuen uns auf Ihre Anfrage!

Gez.

Cedric Rahlff
Patrick Oswald