LISTE DER TECHNISCHEN / ORGANISATORISCHEN MASSNAHMEN

TYP	ID	Bereich	Zusammenfassung
Organisatorisch	TOM-37	Auftragskontrolle	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und DSGVO-Compliance)
Organisatorisch	TOM-38	Auftragskontrolle	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
Organisatorisch	TOM-39	Auftragskontrolle	Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-40	Auftragskontrolle	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-41	Auftragskontrolle	Verpflichtung der Mitarbeiter*in des Auftragnehmers auf das Datengeheimnis Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-43	Auftragskontrolle	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
Organisatorisch	TOM-44	Auftragskontrolle	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Technisch	TOM-64	Auftragskontrolle	Dokumentation von technischen Support-Anfragen in einem zentralen System
Technisch	TOM-32	Eingabekontrolle	Systeme zur Protokollierung der Eingabe, Änderung und Löschung von Daten.

karriere.at GmbH
Donaupromenade 1, 4020 Linz
office@karriere.at, +43 732 908200
www.karriere.at

Handelsgericht Linz, FN 256668d
UID ATU61401334
IBAN AT64 3400 0000 0272 2197

Geschäftsführer
MMag. Klaus Hofbauer, Mag. Oliver Sonnleithner, Mag.
Jürgen Smid, Georg Konjovic

Organisatorisch	TOM-35	Eingabekontrolle	”Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer*innennamen (nicht Benutzer*innengruppen)”
Organisatorisch	TOM-36	Eingabekontrolle	”Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts”
Technisch	TOM-57	Trennungsgebot	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
Technisch	TOM-58	Trennungsgebot	Trennung von Produktiv- und Testsystem
Organisatorisch	TOM-60	Trennungsgebot	Berechtigungskonzept
Organisatorisch	TOM-61	Trennungsgebot	Festlegung von Datenbankrechten
Organisatorisch	TOM-62	Trennungsgebot	Logische Mandantentrennung (softwareseitig)
Technisch	TOM-45	Verfügbarkeitskontrolle	Feuerlöschgeräte in Serverräumen
Technisch	TOM-46	Verfügbarkeitskontrolle	Feuer- und Rauchmeldeanlagen
Technisch	TOM-47	Verfügbarkeitskontrolle	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
Technisch	TOM-48	Verfügbarkeitskontrolle	Klimaanlage in Serverräumen
Technisch	TOM-49	Verfügbarkeitskontrolle	Schutzsteckdosenleisten in Serverräumen
Technisch	TOM-50	Verfügbarkeitskontrolle	Unterbrechungsfreie Stromversorgung (USV)
Organisatorisch	TOM-51	Verfügbarkeitskontrolle	”Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort”
Organisatorisch	TOM-52	Verfügbarkeitskontrolle	Backup- & Recoverykonzept
Organisatorisch	TOM-54	Verfügbarkeitskontrolle	Testen von Datenwiederherstellung
Organisatorisch	TOM-55	Verfügbarkeitskontrolle	Serverräume nicht unter sanitären Anlagen
Technisch	TOM-28	Weitergabekontrolle	Einrichtungen von VPN-Tunneln
Organisatorisch	TOM-65	Weitergabekontrolle	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Technisch	TOM-6	Zugangskontrolle	Authentifikation mit Benutzer + Passwort
Technisch	TOM-7	Zugangskontrolle	Einsatz von Anti-Viren-Software

Technisch	TOM-8	Zugangskontrolle	Einsatz von Firewalls
Technisch	TOM-9	Zugangskontrolle	Einsatz von VPN-Technologie
Technisch	TOM-10	Zugangskontrolle	Gehäuseverriegelung
Technisch	TOM-11	Zugangskontrolle	Verschlüsselung von Datenträgern
Organisatorisch	TOM-12	Zugangskontrolle	Benutzerberechtigungen verwalten
Organisatorisch	TOM-13	Zugangskontrolle	Erstellen von Benutzerprofilen
Organisatorisch	TOM-14	Zugangskontrolle	Passwortvergabe / Passwortregeln
Organisatorisch	TOM-16	Zugangskontrolle	Sorgfältige Auswahl von Sicherheitspersonal
Technisch	TOM-17	Zugriffskontrolle	Einsatz von Aktenvernichtern
Technisch	TOM-18	Zugriffskontrolle	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
Technisch	TOM-19	Zugriffskontrolle	Physische Löschung von Datenträgern vor deren Wiederverwendung
Organisatorisch	TOM-22	Zugriffskontrolle	Anzahl der Administrator*innen auf das „Notwendigste" reduzieren
Organisatorisch	TOM-23	Zugriffskontrolle	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
Organisatorisch	TOM-25	Zugriffskontrolle	Passwortrichtlinie inkl. Länge und Wechsel
Organisatorisch	TOM-26	Zugriffskontrolle	Sichere Aufbewahrung von Datenträgern
Organisatorisch	TOM-27	Zugriffskontrolle	Verwaltung der Benutzungsrechte durch Systemadministrator*innen
Technisch	TOM-2	Zutrittskontrolle	Alarmanlage
Technisch	TOM-3	Zutrittskontrolle	Automatisches Zugangskontrollsystem
Technisch	TOM-4	Zutrittskontrolle	Sicherheitsschlösser