Anlage „Technische und organisatorische Maßnahmen (TOM)“, mit Stand 19.06.2023, in Verbindung mit der Rahmenvereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Das Dokument beinhaltet die allgemeinen technischen und organisatorischen Maßnahmen (TOM) der IT Rechenwerk GmbH, Eichenkamp 14, 32479 Hille. Wie in der Rahmenvereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO vereinbart, können abweichende, ergänzende oder abweichende Maßnahmen in der jeweiligen verarbeitungsspezifischen Anlage dokumentiert sein.

1. Zutrittskontrolle

- Das Gebäude ist mit einem manuellem Schließsystem ausgestattet (Espelkamp + Hille).
- Türen mit Knauf Außenseite (Hille, Espelkamp ab ca. 17 Uhr).
- Es erfolgt eine organisierte Ausgabe und Rückgabe von Schlüsseln.
- Die Besucher werden durch Beschäftigte in Räume begleitet, welche nicht für den Publikumsverkehr (Espelkamp) vorgesehen sind.

2. Zugangskontrolle

- Der Zugang zu Geräten ist mit Zugangsdaten geschützt (je nach Gerät Benutzername + Passwort, PIN, Biometrie).
- Bei von uns genutzten Online-Anwendungen und Online-Zugriffen kommt, wenn möglich und sinnvoll, eine 2-Faktor-Authentifizierungen zum Einsatz.
- Auf relevanten Geräten (Windows-Clients, NAS) und Diensten (E-Mail) kommt eine Virenschutz-Software zum Einsatz.
- Für relevante Dienste (E-Mail, Kontaktformulare) kommt eine Spam-Schutz-Lösung zum Einsatz.
- Es kommen Firewalls zum Einsatz, z. B. für den Internetzugang, sowie auch twl. Software-Firewalls auf Servern, Online-Anwendungen und Webseiten).
- Bei einigen relevanten (Online)-Anwendungen, Systeme und Dienste kommen Intrusion Detection Funktionalitäten zum Einsatz.
- Zugänge in das Unternehmensnetzwerk oder ggf. externe Netzwerke (Rechenzentrum, Kunden, Lieferanten) erfolgt teilweise über VPN-Zugänge oder anderweitig abgesicherte Zugänge.
- Die Datenträger von relevanten Geräten (Notebooks, Smartphones, Tablets, div. NAS-Verzeichnisse) sind bzw. werden verschlüsselt.
- Es erfolgt bei relevanten Geräten eine automatische Sperre nach einer festgelegten Zeit an Inaktivität.
- Die Verwaltung von Benutzerberechtigungen und deren Anpassung, Deaktivierung bzw. Löschung ist geregelt.
- In den allgemeinen Sicherheitsvorgaben sind Vorgaben zur Vergabe von Passwörtern enthalten.
- In den allgemeinen Sicherheitsvorgaben sind Vorgaben zur Aufbewahrung von Dokumenten und Geräten bei Abwesenheit vom Arbeitsplatz enthalten.
- In den allgemeinen Sicherheitsvorgaben sind Vorgaben zur Sperrung von Geräten bei Abwesenheit enthalten.
- Es stehen abschließbare Stahl-Schränke zur Aufbewahrung von relevanten Unterlagen und digitalen Datenträgern zur Verfügung.

3. Zugriffskontrolle

- Bei relevanten Anwendungen, Diensten bzw. Systemen erfolgt eine Protokollierung von (unberechtigten) Zugriffsversuchen.
- Bei relevanten Anwendungen, Diensten bzw. Systemen erfolgt ein Monitoring von (unberechtigten) Zugriffsversuchen.

- Bei der Vergabe von Benutzerkonten werden angepasste Benutzerberechtigungen vergeben, sowie auf eine Trennung zwischen administrativen und produktiven Benutzerkonten geachtet, sofern dies jeweils möglich und sinnvoll ist.
- Die Vernichtung von Dokumenten (Papier) im Arbeitsalltag erfolgt mit Aktenschreddern (Stufe P5).
- Die Vernichtung größerer Mengen von Dokumenten (Papier) erfolgt über einen Fachdienstleister.
- Die Vernichtung größerer (gesammelte) Mengen digitaler Datenträger mit relevanten Daten erfolgt über einen Fachdienstleister.
- Bei der Rückgabe (Support) oder Außerbetriebnahme erfolgt eine Rücksetzung der Geräte auf Werkseinstellung und eine Löschung Daten, außer es ist im jeweiligen Einzelfall (z. B. Support, Defekt) nicht möglich. In diesem Fällen werden die praktikabelsten Sicherheitsmöglichkeiten angewendet.

4. Trennungskontrolle

- Es erfolgt eine Trennung bei Produktiv-, Test- und Entwicklungsumgebung je nach System und Dienst physikalisch, virtuell oder durch Mandantentrennung.
- Bei der Konzeption und Inbetriebnahme erfolgt eine Prüfung eines direkten Datenbankzugriffs, z. B. per ODBC, und entsprechende Deaktivierung oder Absicherung.
- Es stehen für Besucher und die privaten Geräte von Beschäftigten separate Gäste-WLANs zur Verfügung.

5. Pseudonymisierung und Anonymisierung

- Es erfolgt die Prüfung - und wenn möglich und sinnvoll Umsetzung - des Einsatzes von Pseudonymisierung bei der Konzeption und Inbetriebnahme von Anwendungen, Diensten und Systemen, sowie Reports, z. B. für statistische Auswertungen über kurze bis mittelfristige Zeiträume.
- Es erfolgt die Prüfung - und wenn möglich und sinnvoll Umsetzung - des Einsatzes von Anonymisierung bei der Konzeption und Inbetriebnahme von Anwendungen, Diensten und Systemen, sowie Reports, z. B. für statistische Auswertungen über längere Zeiträume.

6. Weitergabekontrolle

- Bei der E-Mail-Kommunikation kommt zwischen Client und Server eine TLS/SSL-Verschlüsselung zum Einsatz.
- Bei der Kommunikation über das Internet kommt eine TLS/SSL-Verschlüsselung zum Einsatz, sofern dies möglich und sinnvoll ist.
- Bei Online-Anwendungen kommt eine TLS/SSL zum Einsatz, sofern dies möglich und sinnvoll ist.
- Kunden können festlegen welche Personen in ihrem Auftrag weisungsbefugt sind und - je nach beauftragter Leistung - welche Personen Zugänge (z. B. Ticket-System) oder Benachrichtigungen (z. B. Systemmeldungen, Datenschutz- und Sicherheitsvorfälle, …) erhalten sollen.

7. Eingabekontrolle

- In relevanten Anwendungen erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten.
- Es gibt organisatorische Verantwortlichkeiten und Abläufe für die Anlage, Änderung und Löschung bestimmter Daten.
- Teilweise sind technische und organisatorische Freigabeprozesse festgelegt.
- Wenn möglich und sinnvoll kommen individuelle Benutzerkonten zum Einsatz.

8. Verfügbarkeit und Belastbarkeit

- Relevante Server, Anwendungen und Dienste werden bei externen Dienstleistern, z. B. Rechenzentren, betrieben.
- Unsere Arbeitsplätze bzw. Beschäftigten werden, sofern möglich und sinnvoll, so ausgestattet, dass ein ortsunabhängiges Arbeiten möglich ist (z. B. Notebook, Smartphone).
- Bei der Konzeption und Inbetriebnahme von Anwendungen, Diensten und Systemen erfolgt eine Prüfung - und wenn möglich und sinnvoll Umsetzung - des Einsatzes von Virtualisierung.
- In den Betriebsräumen sind Rauchmelder in den relevanten Räumen vorhanden.
- Ein Konzept für die Datensicherung- und Wiederherstellung allgemein, sowie je relevantem System, Anwendung bzw. Dienst ist vorhanden.
- In den Anlagen zur Auftragsverarbeitung sind Informationen zur Datensicherung und Wiederherstellung zur individuellen Bewertung durch den Kunden vorgesehen.
- In den Anlagen zur Auftragsverarbeitung sind Informationen zur Datensicherung und Wiederherstellung vorgesehen, damit Kunden über erforderliche eigene Maßnahmen informiert werden.
- Je nach Bedarf und Möglichkeit der Datensicherungssysteme erfolgt ein Monitoring (bevorzugt) oder Prüfung der Durchführung der Datensicherung.

9. Datenschutz- & Sicherheitsmanagement

- Die Zuständigkeit für Datenschutz- und Sicherheit ist festgelegt.
- Die Dienstleister, inkl. Auftragsverarbeiter und Sub-Auftragsverarbeiter, werden sorgfältig im Hinblick auf Zuverlässigkeit, Sicherheit und Datenschutz ausgewählt.
- Es gibt ein Verzeichnis der Verarbeitungen, sowie ein Verzeichnis der Verarbeitungen im Auftrag.
- Es gibt ein Verzeichnis aller Dienstleister, inkl. Auftragsverarbeiter und Sub-Auftragsverarbeiter.
- Die Auftragsverarbeiter werden in den Anlagen zur Auftragsverarbeitung aufgeführt, zudem ist das Hinzuziehen und der Wechsel von Auftragsverarbeitern geregelt.
- Beschäftigte oder Dienstleister (sofern keine Auftragsverarbeitung vorliegt) die Zugriff auf personenbezogenen Daten erhalten werden auf Vertraulichkeit verpflichtet, sofern diese keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (z. B. Steuerberater).
- Es gibt allgemeine zentrale Sicherheitsvorgaben (inkl. Meldung von Sicherheits- und Datenschutzverletzungen, sowie Verdachtsfälle).
- Es gibt zudem spezielle Sicherheitsvorgaben für einzelne Themen (z. B. mobiles Arbeiten) oder Teams/Rollen.
- Die Beschäftigten werden zu Beginn und dann je nach Team/Rolle wiederholt im Bereich Datenschutz und Datensicherheit sensibilisiert.
- Es gibt einen Ablaufplan zur Erfüllung von Betroffenen-Rechten, inkl. Berücksichtigung der Information von Auftraggebern bei Verarbeitungen im Auftrag.
- Es gibt Regelungen zum Ablauf für (mögliche) Sicherheits- und Datenschutzverletzungen, inkl. Meldung an Auftraggeber (Auftragsverarbeitung) und/oder Aufsichtsbehörde(n).
- Neue Geräte, Anwendungen (inkl. online) und Dienste werden in Orientierung an den bzw. die Bausteine des BSI IT-Grundschutzkompendiums installiert und konfiguriert.
- Die Rahmen-Auftragsverarbeitung sieht vor, dass Auftraggeber weisungsbefugte und zu informierende Personen melden kann.
- Für relevante Systeme, Anwendungen und Dienste sind bzw. werden administrative Notfallbenutzer angelegt und Notfall-2-Faktor-Codes (sofern jeweils möglich).