Technische und organisatorische Massnahmen

W&W trifft die nachfolgenden geeigneten technischen und organisatorischem Massnahmen zur Gewährleistung einer angemessenen Datensicherheit.

1. Vertraulichkeit

Zugriffskontrolle

Massnahmen, die gewährleisten, dass berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

Technische Massnahmen	**Organisatorische Massnahmen**
Login mit Benutzername und Passwort	Verwaltung Benutzerrechte durch Administratoren
Abschliessbare Schränke	Vergabe von Administratorrechten an minimale Anzahl Personen
Login mit Benutzername und Passwort	Einsatz von Rollen- und Berechtigungskonzepten
Anti-Viren-Software	Auswahl sicherer Passwörter
Firewall	Regelung für das Ausscheiden von Mitarbeitenden, insbesondere Sperrung von Zugriffen
Verschlüsselter Zugriff auf interne Systeme	Sicheres Löschen / Vernichten nicht mehr benötigter Unterlagen
Verschlüsselung von Datenträgern	
Verschlüsselung von Notebooks / Tablet	
Ausschluss nicht signierter externer Geräte und IT-Systeme	
Verschlüsselung von mobilen Datenträgern	

Zugangskontrolle

Massnahmen, die gewährleisten, dass nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden.

Technische Massnahmen	Organisatorische Massnahmen
Elektronisches Schliesssystem	Regelmässige Schulung aller Mitarbeiter über Richtlinien, Policies und Vorgaben
Sicherheitsschlösser an wichtigen Türen	Badgeregelung mit Berechtigungskonzept
	Externe nur in Begleitung durch Mitarbeiter
	Auswahl sicherer Passwörter
	Regelung für das Ausscheiden von Mitarbeitenden, insbesondere Sperrung von Zugängen

2. Verfügbarkeit und Integrität

Datenträgerkontrolle

Massnahmen, die gewährleisten, dass unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können.

Technische Massnahmen	Organisatorische Massnahmen
Login mit Benutzername und Passwort	Einsatz eines externen Dienstleisters zur Vernichtung von Datenträger
Einsatz von Verschlüsselungsmassnahmen entsprechend dem aktuellen Stand der Technik	
Physische Löschung von Datenträgern	

Speicherkontrolle

Massnahmen, die gewährleisten, dass unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können.

Technische Massnahmen	Organisatorische Massnahmen
Login mit Benutzername und Passwort	Einsatz Rollen- und Berechtigungskonzepte
E-Mail-Verschlüsselung	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Einsatz von VPN	
Eingesetzte Verschlüsselungsmassnahmen entsprechend dem aktuellen Stand der Technik	

Transportkontrolle

Massnahmen, die gewährleisten, dass unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können.

Technische Massnahmen	**Organisatorische Massnahmen**
Einsatz von Verschlüsselungsmassnahmen entsprechend dem aktuellen Stand der Technik	Ausschluss jeglicher Datenträger-Transporte
Passwortsicherung	

Wiederherstellung

Massnahmen, die gewährleisten, dass die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Technische Massnahmen	**Organisatorische Massnahmen**
Doppelte Datensicherung durch Backups	Unterbringung von Backupsystemen in separaten Räumlichkeiten
RAID -System / Festplattenspiegelung	Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb der Arbeitsräumlichkeiten
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien	Vorgabe zur Kontrolle von Datensicherungsvorgängen
Sichere und ausreichende Default-Einstellung für die Server, durch die ein abgesicherter Wiederanlauf des Serversystems in der vorgesehenen Zeit durchgeführt werden kann.	Regelmässige Tests zur Datenwiederherstellung
Lagerung von Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	

Verfügbarkeit, Zuverlässigkeit und Datenintegrität

Massnahmen, die gewährleisten, dass alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Technische Massnahmen	**Organisatorische Massnahmen**
Feuerlöscher	Vertretungsregelungen für Mitarbeiter
Serverräumlichkeiten in separaten Räumlichkeiten	Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen
RAID -System / Festplattenspiegelung	Durchführung regelmässiger Risikoanalysen
USV-Anlage (Unterbrechungsfreie Stromversorgung)	Unverzügliche und regelmässige Aktivierung von verfügbaren Soft- und Firmwareupdates
Einsatz von Firewall und regelmässige Aktualisierung	Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation
Einsatz von Spamfilter und regelmässige Aktualisierung	Zentrale Dokumentation aller Verfahrensweisen
Einsatz von Virenscanner und regelmässige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Störfällen
Intrusion Detection / Prevention System	Freigabeverfahren für Änderungen bei Rollenwechsel

Systemsicherheit

Massnahmen, die gewährleisten, dass Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.

Technische Massnahmen	**Organisatorische Massnahmen**
Unverzügliche und regelmässige Aktivierung von verfügbaren Soft- und Firmwareupdates	Vertretungsregelungen für Mitarbeiter
Regelmässige Aktualisierung der Firewall	Es besteht ein automatisierter Prozess zum Ausschluss von Einzelsystemen bei identifizierten Sicherheitsverletzungen (Angriffen).
Regelmässige Aktualisierung von Spamfiltern	Dokumentierte Vorgehensweise zum Umgang mit Störfällen
Regelmässige Aktualisierung von Virenscanner	Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmassnahmen risikobezogen angepasst, erneuert und umgesetzt.
Intrusion Detection / Prevention System	

3. Nachvollziehbarkeit

Eingabekontrolle

Massnahmen, die gewährleisten, dass überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden.

Technische Massnahmen	**Organisatorische Massnahmen**
Protokollierung des elektronischen Zugangssystem	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Kennzeichnung erfasster Daten anhand von Schlüssel-IDs	Protokollierung von Eingaben, Veränderungen und Löschungen
Protokollauswertungssystem	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
Über OS-Standard hinausgehendes Log-Konzept	
Dezidierter Logserver mit kontrolliertem Zugriff	
Schutz der Protokolldaten vor unbefugtem Zugriff und unbefugter Manipulation	

Bekanntgabekontrolle

Massnahmen, die gewährleisten, dass überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden.

Technische Massnahmen	**Organisatorische Massnahmen**
Authentisierte und hinreichend verschlüsselte Übertragung von Daten vor der Weitergabe bei nicht gesicherten Übertragungswegen	Dokumentierte Vergabe von Berechtigungen an Mitarbeiter von Kunden
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	Verpflichtung auf Vertraulichkeit/Datengeheimnis
Dateiseparierung bei Datenbanken	Vorherige Prüfung der von Unterauftragsbearbeitern getroffenen Sicherheitsmassnahmen und deren Dokumentation
Logische Datentrennung	Sorgfältige Auswahl von Unterauftragnehmern
Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem	Abschluss notwendiger datenschutzrechtlicher Vereinbarung mit Unterauftragsbearbeitern

Erkennung und Beseitigung

Massnahmen, die gewährleisten, dass Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

Technische Massnahmen	**Organisatorische Massnahmen**
Einsatz von Firewall und regelmässige Aktualisierung	Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation
Einsatz von Spamfilter und regelmässige Aktualisierung	Vertretungsregelungen für Mitarbeiter
Einsatz von Virenscannern und regelmässige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Störfällen
Intrusion Detection / Prevention System	Notfallplan (z.B. Hackerangriffe, Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)
	Getroffene Sicherheitsmassnahmen werden einer regelmässigen Kontrolle unterzogen.
	Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmassnahmen risikobezogen angepasst, erneuert und umgesetzt.