

Technische und organisatorische Massnahmen

Stand 30.10.2026

Fairwalter trifft die nachfolgenden geeigneten technischen und organisatorischen 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	Regelmässige Schulung aller Mitarbeitenden über Richtlinien und Vorgaben
Zwei-Faktor-Authentifizierung (TOTP) für alle Nutzer verfügbar	Verwaltung Benutzerrechte durch Administratoren
Vorübergehende Sperre der Anmeldung nach wiederholten Fehlversuchen	Vergabe von Administratorrechten an minimale Anzahl Personen
Speicherung von Passwörtern nur als Hash	Einsatz von Rollen- und Berechtigungskonzepten
Firewall bei Cloud-Providern	Auswahl sicherer Passwörter
Verschlüsselter Zugriff auf interne Systeme	Regelung für das Ausscheiden von Mitarbeitenden, insbesondere Sperrung von Zugriffen
Verschlüsselung von Notebooks und 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
Produkktivsysteme in Rechenzentren von Microsoft Azure in der Schweiz	Regelmässige Schulung aller Mitarbeitenden über Richtlinien und Vorgaben
Sicherheitsschlösser an wichtigen Türen	Regelung für das Ausscheiden von Mitarbeitenden, insbesondere Sperrung von Zugängen
	Externe nur in Begleitung durch Mitarbeitende

Benutzerkontrolle

Massnahmen, die gewährleisten, dass unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können.

Technische Massnahmen	Organisatorische Massnahmen
Login mit Benutzername und Passwort	Verwaltung Benutzerrechte durch Administratoren
Zwei-Faktor-Authentifizierung (TOTP) für alle Nutzer verfügbar	Regelung für das Ausscheiden von Mitarbeitenden, insbesondere Sperrung von Zugängen
Vorübergehende Sperre der Anmeldung nach wiederholten Fehlversuchen	
Zentrales Beenden aktiver Sitzungen durch den Support	
Zugangsschlüssel und Begrenzung der Anzahl Abfragen für Schnittstellen	

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
Verschlüsselung der gespeicherten Daten (Datenbank, Dateiablage, Backups)	Keine Dokumente in Papierform aufbewahren
Verschlüsselung von Notebooks und mobilen 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 von Rollen- und Berechtigungskonzepten
Verschlüsselung der gespeicherten Daten	

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
Verschlüsselte Übertragung (TLS) für alle Verbindungen zur Software	Bekanntgabe an Dienstleister nur gemäss Liste der Unterauftragsverarbeiter
Verschlüsselung von mobilen Datenträgern	

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	Aufbewahrung der Backups an einem sicheren Ort ausserhalb der Arbeitsräumlichkeiten
Verwendung eines sicheren externen Backupdienstleisters	Regelmässige Tests zur Datenwiederherstellung

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
Server in sicheren Cloud-Rechenzentren	Vertretungsregelungen für Mitarbeitende
Web Application Firewall und DDoS-Schutz	Durchführung regelmässiger Risikoanalysen
Firewall bei Cloud-Providern	Dokumentierter Prozess zur Erkennung und Meldung von Störfällen
Automatische Fehler- und Systemüberwachung	

Systemsicherheit

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

Technische Massnahmen	Organisatorische Massnahmen
Zeitnahe und regelmässige Aktivierung von verfügbaren Soft- und Firmwareupdates	Code-Review vor jeder Änderung an der Software
Regelmässige Prüfung der eingesetzten Softwarebibliotheken auf Sicherheitslücken	Vertretungsregelungen für Mitarbeitende
Getrennte Umgebungen für Entwicklung, Test und Produktion	
Einsatz von Spamfilter und regelmässige Aktualisierung	

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
Kennzeichnung erfasster Daten anhand von Schlüssel-IDs	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Protokollierung von Anmeldungen, fehlgeschlagenen Anmeldungen und Änderungen der Zwei-Faktor-Authentifizierung	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Protokollierung des Erstellens, Ändern und Löschs von Verträgen, Rechnungen, Personen, Bankkonten und Mandaten	
Protokollierung, wenn der Support in ein Benutzerkonto wechselt	

Bekanntgabekontrolle

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

Technische Massnahmen	Organisatorische Massnahmen
Login mit Benutzername und Passwort	Sorgfältige Auswahl von Unterauftragnehmern
Authentisierte und verschlüsselte Übertragung von Daten	Verpflichtung auf Vertraulichkeit/Datengeheimnis
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	
Logische Datentrennung	
Begrenzung der Anzahl Abfragen über Schnittstellen	

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
Automatische Fehler- und Systemüberwachung	Vertretungsregelungen für Mitarbeitende
Protokollierung von Anmeldungen und fehlgeschlagenen Anmeldungen	Dokumentierte Vorgehensweise zum Umgang mit Störfällen
Firewall bei Cloud-Providern	Getroffene Sicherheitsmassnahmen werden einer regelmässigen Kontrolle unterzogen