Technisch-Organisatorische Massnahmen

(TOMs nach Art. 32 DSGVO / Art. 8 nDSG)

Björn Ramseger Consulting (BRC) | Stand: Dezember 2025

Die folgenden technisch-organisatorischen Massnahmen beschreiben, wie Björn Ramseger Consulting personenbezogene Daten im Rahmen von Coaching-Mandaten schützt. Sie gelten für alle Verarbeitungstätigkeiten und werden regelmässig überprüft und aktualisiert.

1. Zutrittskontrolle

Massnahmen, die verhindern, dass Unbefugte Zugang zu Datenverarbeitungsanlagen erhalten.

Kategorie	Massnahme	Umsetzung
Arbeitsplatz	**Zugangsgesichertes Home-Office**	Abschliessbarer Arbeitsraum, keine öffentlich zugänglichen Räumlichkeiten
	Clean-Desk-Prinzip	Physische Unterlagen werden nach Gebrauch verschlossen aufbewahrt
Mobile Arbeit	**Sichtschutzfolie**	Privacy-Filter auf Laptop bei Arbeit im öffentlichen Raum

2. Zugangskontrolle

Massnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

Kategorie	Massnahme	Umsetzung
Authentifizierung	**Starke Passwörter + 2FA**	Alle Systeme mit Zwei-Faktor-Authentifizierung (TOTP/Hardware-Key) gesichert
	Biometrische Gerätesperre	Touch ID / Face ID auf allen mobilen Endgeräten
	Automatische Bildschirmsperre	Nach 3 Minuten Inaktivität
Passwortverwaltung	**Passwort-Manager**	[Tool einsetzen, z. B. 1Password / Bitwarden] für alle Zugänge
Gerätesicherheit	**Festplattenverschlüsselung**	FileVault (macOS) auf allen Arbeitsgeräten aktiviert
	Aktuelle Betriebssysteme	Automatische Sicherheitsupdates aktiviert

3. Zugriffskontrolle

Massnahmen, die gewährleisten, dass nur berechtigte Personen auf Daten zugreifen können.

Kategorie	Massnahme	Umsetzung
Berechtigungskonzept	**Einzelunternehmer-Prinzip**	Ausschliesslich der Coach hat Zugriff auf Klientendaten. Keine Mitarbeitenden, keine externen Dienstleister mit Datenzugang.
Datenminimierung	**Need-to-know**	Nur die für das jeweilige Coaching-Mandat notwendigen Daten werden erhoben und gespeichert
Testdaten	**Pseudonymisierung**	Kurzskalen-Ergebnisse werden pseudonymisiert gespeichert (Klientencode statt Klarname)

Ida-Sträuli-Strasse 71
8404 Winterthur - CH
+41 76 690 19 10

Eylauerstraße 19
10965 Berlin - D
+49 160 342 70 90

www.bjoernramseger.de
info@bjoernramseger.de

UID: CHE-425.235.509

4. Weitergabekontrolle

Massnahmen, die verhindern, dass Daten bei der Übertragung unbefugt gelesen oder kopiert werden.

Kategorie	Massnahme	Umsetzung
E-Mail	**Transportverschlüsselung**	TLS-Verschlüsselung über Google Workspace (smtp.gmail.com, Port 587)
Videokonferenz	**Ende-zu-Ende-Verschlüsselung**	[Tool einsetzen, z. B. Zoom E2EE / Microsoft Teams]. Keine Aufzeichnung ohne schriftliche Einwilligung.
Dateitransfer	**Verschlüsselter Cloud-Speicher**	[Tool einsetzen, z. B. Google Drive / Tresorit] mit Zugangsbeschränkung
Website	**HTTPS**	SSL/TLS-Zertifikat auf bjoernramseger.de und .ch

5. Eingabekontrolle

Massnahmen, die nachträglich prüfbar machen, ob und von wem Daten eingegeben, verändert oder entfernt wurden.

Kategorie	Massnahme	Umsetzung
Dokumentation	**Versionierung**	Coaching-Notizen und Berichte mit Zeitstempel und Versionshistorie
	Keine Mehrbenutzer-Systeme	Einzelunternehmer: Eingaben sind eindeutig dem Coach zuzuordnen

6. Auftragskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten nur gemäss den Weisungen des Verantwortlichen verarbeitet werden.

Kategorie	Massnahme	Umsetzung
Auftragsverarbeiter	**Sorgfältige Auswahl**	Nur Dienstleister mit EU-/CH-Hosting und eigenem DSGVO-/nDSG-Nachweis
	AVV	Auftragsverarbeitungsverträge mit allen relevanten Dienstleistern (Hosting, E-Mail, Cloud)
Dual-KPI-System	**Vertragliche Trennung**	NDA und Dual-KPI-Vereinbarung stellen sicher, dass vertrauliche Daten nie an HR/Sponsor gelangen

7. Verfügbarkeitskontrolle

Massnahmen gegen zufällige Zerstörung oder Verlust von Daten.

Kategorie	Massnahme	Umsetzung
Backup	**Automatische Sicherung**	[Tool/Rhythmus einsetzen, z. B. Time Machine lokal + Cloud-Sync täglich]
	Georedundanz	Cloud-Daten in mindestens zwei Rechenzentren (EU) gespiegelt
Virenschutz	**Endpoint Protection**	Integrierte Sicherheitslösung des Betriebssystems + regelmässige Scans

Ida-Sträuli-Strasse 71
8404 Winterthur - CH
+41 76 690 19 10

Eylauerstraße 19
10965 Berlin - D
+49 160 342 70 90

www.bjoernramseger.de
info@bjoernramseger.de

UID: CHE-425.235.509

8. Trennungsgebot

Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Kategorie	Massnahme	Umsetzung
Mandantentrennung	**Separate Ordnerstruktur**	Jeder Klient hat einen eigenen, verschlüsselten Ordner. Keine mandantenübergreifenden Dateien.
	Getrennte Kommunikationskanäle	Keine Gruppen-E-Mails oder -Chats zwischen verschiedenen Klienten
Zweckbindung	**Marketing ≠ Coaching**	Kontaktdaten aus Lead-Generierung werden strikt getrennt von Coaching-Daten verarbeitet

9. Löschkonzept

Datenkategorie	Löschfrist
Coaching-Notizen	Spätestens 12 Monate nach Abschluss des Mandats
Testdaten (Kurzskalen)	Spätestens 12 Monate nach Abschluss, sofern keine längere Einwilligung
Aggregierte KPI-Reports	Verbleiben beim Klienten/Sponsor; Coach-Kopie wird mit Mandat gelöscht
Vertragsdaten / Rechnungen	10 Jahre (gesetzliche Aufbewahrungspflicht, OR Art. 958f / § 147 AO)
Lead-Magnet-Kontaktdaten	Bei Widerruf der Einwilligung oder spätestens 24 Monate nach letzter Interaktion

REGELMÄSSIGE ÜBERPRÜFUNG

Diese TOMs werden mindestens jährlich sowie anlassbezogen (z. B. bei Einführung neuer Tools, nach Sicherheitsvorfällen oder bei Änderungen der Rechtslage) überprüft und bei Bedarf aktualisiert. Letzte Überprüfung: April 2026.

Hinweis: Dieses Dokument dient der Transparenz gegenüber Auftraggebenden und Aufsichtsbehörden. Es ersetzt keine individuelle Rechtsberatung. Angaben in eckigen Klammern [Tool einsetzen] sind Platzhalter und müssen vor Verwendung mit den tatsächlich eingesetzten Werkzeugen ergänzt werden.

Ida-Sträuli-Strasse 71
8404 Winterthur - CH
+41 76 690 19 10

Eylauerstraße 19
10965 Berlin - D
+49 160 342 70 90

www.bjoernramseger.de
info@bjoernramseger.de

UID: CHE-425.235.509