TOMs nach Art. 8 nDSG / Art. 32 DSGVO

Björn Ramseger Consulting (BRC)

Stand: Juni 2026

Datenschutz, technisch-organisatorische Massnahmen

Die folgenden technisch-organisatorischen Massnahmen beschreiben, wie Björn Ramseger Consulting personenbezogene Daten im Rahmen von Coaching-Mandaten schützt. BRC ist dabei datenschutzrechtlich Verantwortlicher (Art. 4 Nr. 7 DSGVO / Art. 5 lit. j revFADP). Sie gelten für alle Verarbeitungstätigkeiten und werden regelmässig überprüft und aktualisiert.

01 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

02 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	Apple Passwörter (E2E) für alle Zugänge
Gerätesicherheit	Festplattenverschlüsselung	FileVault (macOS) auf allen Arbeitsgeräten aktiviert
	Aktuelle Betriebssysteme	Automatische Sicherheitsupdates aktiviert

03 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

04 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	Transport- und Speicherverschlüsselung	Google Meet, verschlüsselt in der Übertragung und im ruhenden Zustand. Keine Aufzeichnung ohne Einwilligung.
Dateitransfer	Verschlüsselter Cloud-Speicher	Google Drive (Google Workspace Business Standard) mit Zugriffsbeschränkung; EU-Speicherort für ruhende Daten konfiguriert (Datenregionen = Europa); Auftragsverarbeitung gemäss Google Workspace Data Processing Amendment; US-Transfer zusätzlich über das EU-US Data Privacy Framework gedeckt (Google zertifiziert).
Website	HTTPS	SSL/TLS-Zertifikat auf bjoernramseger.de und .ch
Web-Analyse	Einwilligungsbasiert	GA4 via Google Tag Manager nur nach Einwilligung (Consent-Banner); IP-Kürzung aktiv; US-Transfer über DPF gedeckt. Der Website-Selbst-Check übergibt keine Antwort- oder Score-Daten an Analyse-Tools.

05 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

Kategorie	Massnahme	Umsetzung
	Keine Mehrbenutzer-Systeme	Einzelunternehmer: Eingaben sind eindeutig dem Coach zuzuordnen

06 Auftragskontrolle

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

Kategorie	Massnahme	Umsetzung
Auftragsverarbeiter	Sorgfältige Auswahl	Bevorzugt Dienstleister mit EU-/CH-Hosting; bei US-Anbietern nur mit DPF-Zertifizierung oder geeigneten Garantien (SCC) 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
KI-gestützte Tools	Datenminimierung	Personenbezogene Klientendaten werden nicht in KI-Tools (z. B. Claude, ChatGPT, Gemini) eingegeben. KI wird ausschliesslich für nicht-personenbezogene Aufgaben (Recherche, Textentwürfe, Marketing) genutzt; etwaige Klientenbezüge werden vorab entfernt oder pseudonymisiert.

07 Verfügbarkeitskontrolle

Massnahmen gegen zufällige Zerstörung oder Verlust von Daten.

Kategorie	Massnahme	Umsetzung
Backup	Automatische Sicherung	Verschlüsselte externe Festplatte (FileVault-verschlüsselt), tägliche Sicherung (Time Machine); Aufbewahrung im abschliessbaren Arbeitsraum. Halbjährlicher Wiederherstellungstest, dokumentiert.
	Georedundanz	Cloud-Daten in mindestens zwei Rechenzentren (EU) gespiegelt
Virenschutz	Endpoint Protection	Integrierte Sicherheitslösung des Betriebssystems und regelmässige Scans

08 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

09 Löschkonzept

Datenkategorie	Löschfrist
Coaching-Notizen	Spätestens 12 Monate nach Abschluss des Mandats

Datenkategorie	Löschfrist
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

10 Umgang mit Datenschutzverletzungen

Erkannte Datenschutzverletzungen werden unverzüglich bewertet. Besteht ein Risiko für die Rechte und Freiheiten betroffener Personen, erfolgt die Meldung an die zuständige Aufsichtsbehörde binnen 72 Stunden sowie, sofern erforderlich, die Benachrichtigung der betroffenen Personen. Jeder Vorfall wird dokumentiert (Hergang, Bewertung, getroffene Massnahmen).

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: Juni 2026.**

> ***Hinweis:*** *Dieses Dokument dient der Transparenz gegenüber Auftraggebenden und Aufsichtsbehörden. Es ersetzt keine individuelle Rechtsberatung.*

Adresse
Ida-Sträuli-Strasse 71
8404 Winterthur · CH

Online
www.bjoernramseger.com
br@bjoernramseger.com

Telefon
+41 76 690 19 10 (CH)
+49 160 342 70 90 (D)

UID
CHE-425.235.509