aban news

DSGVO-AI-Checkliste

20 Punkte für DACH-Solopreneure

Stand: 2026
abannews.com

Vorbemerkung

Diese Checkliste ist eine Praxishilfe — keine Rechtsberatung. Sie deckt die häufigsten Stolpersteine beim AI-Einsatz für Solo-Selbständige in DE, AT und CH ab. Bei kritischen Punkten (Konzern-Anfragen, Behörden-Auskunft, Klagen): Anwalt einbeziehen.

Subprocessor-Audit

■ 1. Liste aller AI-Anbieter, die du nutzt

Wie: Spreadsheet: Tool-Name, Anbieter, Sitz, was sie verarbeiten.

Häufiger Fehler: *Vergessen: Browser-Plugins, IDE-Extensions, automatische Transkripte.*

■ 2. Auftragsverarbeitungsverträge (AVV/DPA) abgeschlossen

Wie: Bei jedem Anbieter, der personenbezogene Daten verarbeitet, AVV abschliessen.

Häufiger Fehler: *OpenAI hat DPA-Template. Anthropic hat DPA. Beide MUSST du aktiv abschliessen.*

■ 3. US-Übermittlungen geprüft (EU-US Data Privacy Framework)

Wie: Anbieter zertifiziert? Standardvertragsklauseln (SCC) im AVV?

Häufiger Fehler: *Nicht alle US-Anbieter sind DPF-zertifiziert. Liste prüfen auf dataprivacyframework.gov.*

■ 4. Subdienstleister deiner Subdienstleister bekannt

Wie: Anbieter listet sub-processors. Du musst sie kennen (z.B. AWS, GCP).

Häufiger Fehler: *Übersehen: Anthropic nutzt AWS und GCP. Beides musst du in deinem Verzeichnis listen.*

Datenfluss

■ 5. Welche personenbezogenen Daten gehen an AI?

Wie: Pro Tool dokumentieren: Kunden-Emails? Namen? Adressen? Gesundheitsdaten?

Häufiger Fehler: *Wenn du Kunden-Texte in ChatGPT pastest, gehen personenbezogene Daten an OpenAI.*

■ 6. Pseudonymisierung wo möglich

Wie: Vor AI-Upload: Namen ersetzen durch [Kunde-1], Emails durch [Email-1] etc.

Häufiger Fehler: *Hier verlierst du wenig Qualität. Aber massive Reduktion des Risikos.*

■ 7. Sensitive Daten (Art. 9 DSGVO) NIEMALS ohne Einwilligung

Wie: Gesundheit, Religion, politische Meinung, Sexualleben: separater Rechtsgrund nötig.

Häufiger Fehler: *Coaches: NIEMALS Therapie-Notizen in normale LLMs. Auch nicht 'anonymisiert'.*

■ 8. Datenfluss-Diagramm existiert

Wie: Eine A4-Seite: Wo entstehen Daten → wo werden sie verarbeitet → wo gelöscht.

Häufiger Fehler: *Vorlage: draw.io oder Excalidraw. Behörde fragt im Ernstfall danach.*

Einwilligung

■ 9. Cookie-Banner DSGVO-konform

Wie: Opt-in vor Tracking (nicht nur Banner anzeigen). Granular pro Kategorie. Ablehnen so einfach wie zustimmen.

Häufiger Fehler: *'OK'-Knopf riesig, 'Ablehnen' versteckt = Abmahnrisiko. CNIL-Bussgelder in FR sind hoch.*

■ 10. Datenschutzerklärung erwähnt AI-Verarbeitung

Wie: Welche AI-Tools? Welche Daten? Warum? Rechtsgrund? Speicherdauer?

Häufiger Fehler: *Generische Texte ohne AI-Erwähnung sind veraltet. Spezifisch sein.*

■ 11. Newsletter-Einwilligung trennt Marketing von AI-Nutzung

Wie: Wenn du Newsletter-Daten an AI gibst (z.B. für Personalisierung): separate Einwilligung.

Häufiger Fehler: *'Wir nutzen AI zur Personalisierung deines Newsletters' — als Checkbox + Erklärung.*

■ 12. Widerrufbarkeit der Einwilligung dokumentiert

Wie: Wie kann jemand widerrufen? Klick im Footer reicht oft nicht. Email-Adresse + Self-Service.

Häufiger Fehler: *Wenn niemand jemals widerrufen hat: das ist verdächtig, nicht erfolgreich.*

Speicherdauer

■ 13. Pro Datenkategorie Speicherdauer festgelegt

Wie: Newsletter-Subscriber: bis Widerruf. Kundendaten: 10 Jahre nach §147 AO. AI-Logs?

Häufiger Fehler: *AI-Anbieter speichern Logs meist 30 Tage. Frag, ob du das verkürzen kannst (Enterprise).*

■ 14. Löschroutinen automatisiert oder dokumentiert

Wie: Make/Zapier-Workflow oder Kalendererinnerung: einmal pro Monat Löschungen prüfen.

Häufiger Fehler: *Manuell vergessen ist Standardproblem. Automatisierung lohnt sich hier.*

■ 15. Backup-Strategie berücksichtigt Löschung

Wie: Wenn du löschst, aber Backup behält: Verstoss. Backup-Rotation < 90 Tage hilft.

Häufiger Fehler: *Wer mit Cloud-Backups arbeitet: prüfen, wie Anbieter mit Löschanfragen umgeht.*

Auskunft

■ 16. Auskunftsanfrage-Prozess existiert

Wie: Email an dich → wo greifst du nach Daten? Welche Tools, welche Logs, welche Backups?

Häufiger Fehler: *Frist: 30 Tage. Ohne Prozess wird das schnell stressig.*

■ 17. Berichtigung / Löschung umsetzbar

Wie: Pro System dokumentiert: wo, wer, wie wird gelöscht / berichtigt.

Häufiger Fehler: *Daten in AI-Trainingsdaten: kannst du nicht löschen. Daher von vornherein nicht uploaden.*

■ 18. Datenportabilität (Art. 20) geklärt

Wie: Auf Anfrage: maschinenlesbares Export-Format (CSV, JSON).

Häufiger Fehler: *Beehiiv exportiert CSV. Tally exportiert JSON. Notion exportiert HTML/CSV/JSON.*

Sicherheit

■ 19. API-Keys nicht im Code / Browser-Storage

Wie: Secrets in Env-Vars, Vault, oder Cloud-Secret-Managern. Niemals committen.

Häufiger Fehler: *.env in .gitignore. Pre-commit-Hooks wie gitleaks finden vergessene Keys.*

■ 20. Zugriffsrechte minimal (Need-to-know)

Wie: Wer hat Zugriff auf welche Daten? Solo = du. Aber Freelancer, VAs, Cloud-Backups?

Häufiger Fehler: *Wenn du eine VA einsetzt: AVV mit ihr. Read-only-Zugriff wo möglich.*

■ 21. Meldepflicht-Plan bei Datenpanne (72h)

Wie: Bei DSGVO-Verstoss: 72h zur Meldung an Aufsichtsbehörde. Was machst du, wenn ein Laptop weg ist?

Häufiger Fehler: *Vorlage: Beim Schweiz (EDÖB) und DE-Aufsichtsbehörden online. Im Vorfeld lesen.*

Brauchst du Hilfe?

DSGVO-Compliance ist nicht kompliziert — aber lückenhaft kann teuer werden. Wenn dir bei einem dieser Punkte unklar ist, was du tun sollst: schreib mir.

aban news — abannews.com

Diese Checkliste ist Praxishilfe, keine Rechtsberatung. Bei spezifischen Risiken: Datenschutzanwalt oder Datenschutzbeauftragten einbeziehen.