PRAXIS-LEITFADEN FÜR SELBSTSTÄNDIGE

Der Datensicherheits-Blueprint

In 4 Schritten zu sicheren Kundendaten, automatischem Backup und ruhigem Schlaf — ohne IT-Fachchinesisch.

> **Enthält:** Klick-für-Klick Anleitungen für Festplattenverschlüsselung, Cryptomator-Cloudtresore, lautloses 3-2-1-Backup und die 1-Seiten-Notfallkarte.

Ausgabe: 1. Auflage

Fokus: DSGVO-Sicherheit & Datenrettung

1. Das Grundprinzip: Entspannung durch Struktur

95 % aller IT-Sicherheitsvorfälle bei Selbstständigen sind **keine** gezielten Hackerangriffe, sondern alltägliche Pannen:

- Ein Laptop wird im Zug, Café oder Auto gestohlen oder vergessen.
- Eine Festplatte quittiert ohne Vorwarnung von heute auf morgen den Dienst.
- Passwörter werden mehrfach genutzt und tauchen nach Datenlecks im Netz auf.
- Sensible Kundendaten liegen unverschlüsselt in Standard-Clouds (DSGVO-Haftungsfalle).

Mit den folgenden vier Schritten eliminierst du diese Risiken dauerhaft. Einmal eingerichtet, läuft das System verlässlich und lautlos im Hintergrund.

Schritt 1: Der unknackbare Laptop (Vollverschlüsselung)

> **Die wichtigste DSGVO-Regel:** Wenn dein Laptop gestohlen wird und die Festplatte verschlüsselt ist, handelt es sich um einen reinen Hardwareverlust – **nicht** um eine meldepflichtige Datenschutzpanne. Niemand kann ohne dein Passwort an die Daten.

1.1 Für Windows (BitLocker / Geräteverschlüsselung)

1. Öffne das Startmenü und tippe `BitLocker verwalten` oder `Geräteverschlüsselung` ein.
2. Klicke auf **„BitLocker aktivieren“**.
3. **Wichtig:** Beim Wiederherstellungsschlüssel: Drucke ihn auf Papier aus oder speichere ihn in deinem Passwortmanager (siehe Schritt 4). Speichere ihn niemals unverschlüsselt auf dem Desktop.
4. Wähle *„Gesamtes Laufwerk verschlüsseln“*. Der Laptop kann während des Vorgangs normal weitergenutzt werden.

1.2 Für macOS (FileVault)

1. Öffne die **Systemeinstellungen** > **Datenschutz & Sicherheit**.
2. Scrolle zu **FileVault** und klicke auf **„Aktivieren“**.
3. Notiere den Wiederherstellungsschlüssel und lege ihn sicher im Passwortmanager ab.

1.3 Sofort-Maßnahmen für jeden Arbeitsplatz:

- **Automatische Bildschirmsperre:** Sperre nach maximal 3–5 Minuten Inaktivität.

- **Kein Autologin:** Beim Einschalten muss zwingend ein Kennwort oder biometrischer Login (Fingerabdruck / Windows Hello / Touch ID) verlangt werden.

Schritt 2: Sichere Cloud-Ablage mit Cryptomator

Viele Selbstständige nutzen Dropbox, Google Drive oder Microsoft OneDrive. Das Problem: Aus DSGVO-Sicht liegen sensible Kundendaten dort oft unverschlüsselt auf fremden Servern.

Die Lösung heißt **Client-seitige Verschlüsselung mit Cryptomator** (kostenlos, quelloffen, unabhängig zertifiziert).



In der Cloud liegt nur unlesbarer Datensalat. Weder Hacker noch der Cloudanbieter können mitlesen.

So richtest du deinen Tresor in 5 Minuten ein:

1. Lade **Cryptomator** von `cryptomator.org` herunter und installiere es.
2. Klicke auf das **+** Symbol (*„Neuen Tresor erstellen“*).
3. Wähle als Speicherort einen Ordner **innerhalb deiner bestehenden Cloud** (z. B. `OneDrive/Tresor_Kunden`).
4. Vergib ein starkes Tresor-Passwort (im Passwortmanager sichern).
5. Klicke auf **„Tresor entsperren“**:
   - Cryptomator bindet ein virtuelles Laufwerk ein (funktioniert wie ein normaler USB-Stick).
   - Alle Dateien, die du dort ablegst, werden **automatisch vor dem Upload verschlüsselt**.
   - Sobald du den Tresor sperrst, verschwindet das Laufwerk.

Empfohlene Ordnerstruktur im Tresor:

```
Tresor_Kunden/
├── 01_Aktive_Projekte/
│   ├── Kunde_Mustermann/
│   └── Kunde_Schmidt/
├── 02_Finanzen_Buchhaltung/
│   ├── Ausgangsrechnungen_2026/
│   └── Belege_Eingang/
└── 03_Verträge_DSGVO/
    └── Auftragsverarbeitungsverträge_AVV/
```

Schritt 3: Das unzerstörbare 3-2-1-Backup

Manuelle Backups per USB-Stick scheitern immer an der Disziplin. Ein funktionierendes Backup muss **automatisch und unbemerkt im Hintergrund** laufen.

> **Die 3-2-1-Regel:**
> • **3 Kopien** aller wichtigen Daten (1 Original + 2 Backups).
> • **2 verschiedene Speichermedien** (z. B. interne SSD + externe SSD / Cloud).
> • **1 Kopie an einem anderen Ort** (Offsite – schützt vor Diebstahl, Feuer oder Wasserschaden).

Das schlanke Setup für Selbstständige:

Kopie	Speicherort	Empfohlenes Tool	Ablauf
Kopie 1 (Lokal)	Externe SSD am Schreibtisch	macOS: **Time Machine** Windows: **Veeam Agent** oder **Kopia**	Läuft vollautomatisch im Hintergrund, sobald die Festplatte angesteckt ist.
Kopie 2 (Offsite)	Verschlüsselter Cloudspeicher	**Kopia**, **BorgBackup** oder **Hetzner Storage Box**	Läuft 1x täglich nachts verschlüsselt über das Internet.

> **Der 10-Minuten-Rettungstest:** Ein Backup existiert erst, wenn du es einmal erfolgreich wiederhergestellt hast. Lösche testweise eine unkritische Testdatei und stelle sie aus deinem Backup wieder her. Erst wenn das klappt, ist dein Backup verifiziert.

Schritt 4: Kunden-Zugänge & Passwörter sicher teilen

4.1 Der zentrale Passwortmanager (Bitwarden)

- Nutze **Bitwarden** (quelloffen, unabhängig geprüft, synchronisierbar auf PC, Mac und Smartphone).
- **Das Master-Passwort:** Wähle eine *Passphrase* aus 4–5 zufälligen Wörtern (z. B. `Kaffeetasse-Flugzeug-Sommerregen-42`).
- **Zwei-Faktor-Authentifizierung (2FA):** Sichere deinen Tresor mit einer Authenticator-App (z. B. 2FAS, Aegis) ab.

4.2 Nie wieder Passwörter per WhatsApp oder E-Mail!

Wenn du Zugangsdaten an Kunden senden oder von ihnen empfangen musst, nutze **Bitwarden Send**:

1. Öffne Bitwarden und klicke auf den Reiter **Send**.
2. Erstelle einen neuen Eintrag mit dem Passwort oder Text.
3. Stelle die **maximale Abrufanzahl auf 1** (Link verfällt sofort nach dem ersten Öffnen) und das **Ablaufdatum auf 2 Tage**.
4. Schicke dem Kunden nur den generierten Link. Sensible Daten bleiben niemals im Mailpostfach liegen.

NOTFALLKARTE: IT-WIEDERHERSTELLUNG

Stand / Aktualisiert am: _____

1. ARBEITSGERÄT (LAPTOP / RECHNER)
Modell / Name: _____
Verschlüsselung: [ ] BitLocker [ ] FileVault [ ] LUKS
Wiederherstellungsschlüssel: _____

2. PASSWORTMANAGER (BITWARDEN / 1PASSWORD)
E-Mail-Adresse: _____
Hinweis Master-Passwort: _____
2FA-Notfall-Recovery-Code: _____

3. VERSCHLÜSSELTE CLOUD (CRYPTOMATOR)
Cloud-Anbieter / Pfad: _____
Tresor-Name: _____
Passwort-Hinweis: _____

4. BACKUP-INFRASTRUKTUR
Lokale Backup-Festplatte: _____
Cloud-Backup (Offsite): _____
Verschlüsselungs-Passphrase: _____

5. NOTFALLKONTAKT / TECHNISCHER BEISTAND
Name / Telefonnummer: _____

Ausdrucken, handschriftlich ausfüllen und im physischen Notfallordner / Schließfach aufbewahren.