DKSCHV SCHWEIZ · AUDIT-DOSSIER

# Sicherheits- & nDSG-Auditbericht

Ganzheitliche Bestandsaufnahme, Schutzbedarfsanalyse und Massnahmenplan nach Schweizer Datenschutzgesetz (nDSG & VDSG).

| | |
|---|---|
| **Auftraggeber:** | **[Muster KMU AG, Naters / Brig]** |
| **Auditor / Prüfer:** | Andreas Dini, DKSchV Schweiz |
| **Datum des Audits:** | 22. November 2026 |
| **Vertraulichkeitsstufe:** | **STRENG VERTRAULICH (Klasse 3)** |

**Prüfstandard:** revDSG (SR 235.1) & BACS-KMU-Richtlinien **Gültigkeit:** 12 Monate

# 1. Executive Summary: Reifegrad & Gesamtergebnis

Im Rahmen des Audits wurde die bestehende IT-Infrastruktur, die Datenflüsse und die organisatorischen Abläufe der **[Muster KMU AG]** auf den Prüfstand gestellt.

| Prüfbereich | Status | Bewertung / Kernbefund |
|---|---|---|
| **1. Kronjuwelen-Schutz** | HANDLUNGSBEDARF | ERP- und Finanzdaten sind unzureichend vor Ransomware isoliert. |
| **2. nDSG-Konformität (TOM)** | KRITISCH | Laptops im Außendienst unverschlüsselt; 2FA bei M365 nur für Admins aktiv. |
| **3. Lieferanten-Risiken** | HANDLUNGSBEDARF | Auftragsbearbeitungsverträge (ABV) mit IT-Dienstleistern fehlen teilweise. |
| **4. Mitarbeiter & Richtlinien** | KONFORM | 4-Augen-Prinzip bei Banküberweisungen vorbildlich etabliert. |

> **Gesamt-Reifegrad: 64 % (Bedingt konform).** Es bestehen keine Hinweise auf akute Angriffe, jedoch existieren zwei strukturelle Sicherheitslücken (fehlende Geräteverschlüsselung und ungeschützte Backups), die im Ernstfall zu existenzbedrohendem Datenverlust oder Bussen nach Art. 60 nDSG führen können.

## 2. Identifikation der «Kronjuwelen» & Schutzbedarf

Gemeinsam mit der Geschäftsleitung wurden die wichtigsten Unternehmenswerte und deren maximal tolerierbare Ausfallzeit (RTO) definiert:

| System / Datensatz | Speicherort | Schutzklasse | Max. Ausfallzeit (RTO) | Sicherheitsmassnahme |
|---|---|---|---|---|
| **ERP- & Faktura-Daten** | Lokaler Server | **Prio 1 (Vital)** | Max. 4 Stunden | Tägliches Offline-Backup (Air-Gapped) |
| **CAD- & Konstruktionspläne** | Cloud (SharePoint) | **Prio 1 (Vital)** | Max. 24 Stunden | Zero-Knowledge-Verschlüsselung |
| **Personal- & Lohndaten** | Lohnprogramm | **Prio 2 (Sensibel)** | Max. 48 Stunden | Strikte Rollentrennung & 2FA |
| **E-Mail-Korrespondenz** | Microsoft 365 | **Prio 2 (Wichtig)** | Max. 24 Stunden | Zentrale M365-Archivierung |

## 3. nDSG-Konformitätsprüfung (TOM-Check)

| Vorgeschriebene Massnahme | Ist-Zustand | Soll-Zustand (nDSG) | Bewertung |
|---|---|---|---|
| **Geräteverschlüsselung** Art. 8 nDSG / Art. 1 VDSG | 5 von 12 Laptops unverschlüsselt. | 100% BitLocker/FileVault für alle mobilen Arbeitsgeräte. | MANGELHAFT |
| **Zugriffskontrolle & 2FA** Art. 2 VDSG | 2FA nur für 2 Administratoren aktiv. | Zwingende MFA für sämtliche Cloud-Zugänge (M365). | MANGELHAFT |
| **Passwort-Sicherheit** Art. 2 VDSG | Passwörter in Browsern & Chats. | Zentraler Passwortmanager (Bitwarden / 1Password). | OPTIMIEREN |
| **Lösch- & Aufbewahrung** Art. 6 nDSG | Bewerberdaten werden manuell gelöscht. | Definierter Löschprozess nach 6 Monaten. | KONFORM |

## 4. Third-Party Risk (Lieferanten & IT-Partner)

Externe Dienstleister haben oft weitgehende Zugriffsrechte auf die Systeme der [Muster KMU AG]:

| Dienstleister / Partner | Art des Zugriffs | Serverstandort | ABV-Vertrag | Empfehlung |
|---|---|---|---|---|
| **IT-Support MusterPartner** | Dauerhafter VPN & AnyDesk | Schweiz | FEHLT | Standard-ABV sofort unterzeichnen. |
| **Microsoft (M365)** | E-Mail & Office Cloud | Schweiz (Zürich/Genf) | VORHANDEN | Kein Handlungsbedarf (DPA aktiv). |
| **Treuhand-Büro Wallis** | Lesezugriff ERP | Schweiz | VERALTET | Aktualisierung auf nDSG 2026. |

## 5. Der 14-Tage-Sofortmassnahmenplan (Quick Wins)

Zur schnellen Schliessung der kritischsten Lücken ohne Budgetsprengung empfehlen wir folgende drei Massnahmen:

1. **Sofort-Aktivierung von BitLocker / FileVault (Aufwand: ca. 2 Stunden):**
   Alle 12 Firmenlaptops mit Festplattenverschlüsselung absichern. Damit wird bei Verlust oder Diebstahl ein meldepflichtiger Datenschutzvorfall an den EDÖB rechtlich abgewendet.
2. **Erzwingung von 2FA / MFA für alle Microsoft 365 Konten (Aufwand: 1 Stunde):**
   Verhindert 99 % aller Account-Übernahmen und CEO-Fraud-Angriffe über kompromittierte Passwörter.
3. **Abschluss des beiliegenden Auftragsbearbeitungsvertrags (ABV):**
   Unterzeichnung des standardisierten nDSG-Vertrags mit dem externen IT-Dienstleister zur rechtlichen Absicherung der Geschäftsführung.

**Bericht erstellt durch:**
Andreas Dini · Inhaber & IT-Sicherheitsberater · DKSchV Schweiz · Naters
E-Mail: info@dkschv.ch · Web: https://dkschv.ch