



## Recovery Checkliste

Diese Anleitung zeigt Ihnen, wie Sie als KMU systematisch reagieren, wenn Daten verloren gehen  
- von der Sofortmassnahme bis zur Wiederherstellung.

### 1 - Sofortmassnahmen - Ruhe bewahren

- IT Verantwortlicher informieren
- Betroffene Geräte vom Netzwerk trennen
- Dokumentation der betroffenen Systeme / Daten
- Keine Eigenversuche oder Wiederherstellungen ohne IT-Verantwortung

### 2 - Analyse - den Vorfall verstehen

- Prüfung der betroffenen Daten (Backup, lokale Daten, Cloud-Dienste)
- Identifizierung der Ursache (Hardware-Defekt, Ransomware, menschlicher Fehler)
- Erfassung der Zeitpunkte und Symptome um das Ausmass festzustellen
- Festhalten, welche Systeme für den Geschäftsbetrieb kritisch sind

### 3 - Wiederherstellung - Backup nutzen

- Wiederherstellung der Daten aus dem letzten funktionierenden Backup
- Prüfung ob das Backup vollständig und intakt ist
- Priorisierung der kritischen Systeme
- Test der Daten und Systeme nach der Wiederherstellung vor der Freigabe

### 4 - Kommunikation - intern und extern

- Mitarbeitende klar über den Vorfall und die nächsten Schritte informieren
- Bei Kundenrelevanz: sachlich informieren, keine Panik verbreiten
- Management laufend auf dem aktuellen Stand halten
- Nutzung vorbereiteter Textvorlagen (z. B. MOUNT10 KI-Prompt) für konsistente Kommunikation





## Recovery Checkliste

Diese Anleitung zeigt Ihnen, wie Sie als KMU systematisch reagieren, wenn Daten verloren gehen  
- von der Sofortmassnahme bis zur Wiederherstellung.

### 5 - Sicherheitsmassnahmen - zukünftige Risiken minimieren

- Prüfung wie es zum Datenverlust gekommen ist (Sicherheitslücke, fehlende Isolation)
- Optimierung der Backup-Strategie (regelmässige Backups, Immutable Backup, getrennte Systeme)
- Regelmässige Schulung der Mitarbeitenden im Bereich Datensicherheit
- Durchführen von regelmässigen Recovery-Tests

### 6 - Nachbereitung - Lessons learned

- Dokumentation des Vorfalls (Ursache, Dauer, betroffene Daten, ergriffene Massnahmen)
- Anpassung interner Prozesse und Notfallpläne
- Internes Review um Verantwortlichkeiten und Reaktionszeiten zu verbessern
- Aktualisierung der Backup- und IT-Notfall-Checklisten

### Bei Datendiebstahl

In der Schweiz gelten die Meldepflichten gemäss Datenschutzrecht nDSG Kapitel 4 Art. 24 (z. B. Meldung an den EDÖB bei Datenschutzverletzungen) Weitere Informationen: <https://www.edoeb.admin.ch/de/databreach>

### Einbezug externer Spezialisten

Bei komplexen Sicherheitsvorfällen kann der Beizug einer **externen Incident-Response- und Forensik-Firma** sinnvoll sein. Externe Spezialisten unterstützen bei: Ursachenanalyse und Beweissicherung, Einschätzung des Schadens, rechtssicherem Vorgehen, Wiederherstellung und Härtung der Systeme

