

CL-03 | CHECKLISTE · 22.07.2026 · V.1.0.0

Datensicherung, die im Ernstfall wirklich hält

Backup-Checkliste für Privatpersonen und Kleinbetriebe – einmal einrichten, viermal im Jahr prüfen.

Fast jeder Datenverlust, den wir sehen, wäre vermeidbar gewesen. Nicht weil kein Backup existierte, sondern weil es unvollständig war, am selben Gerät lag oder nie getestet wurde. Diese Liste schließt genau diese drei Lücken.

Die 3-2-1-Regel

3 Kopien Ihrer Daten · auf 2 verschiedenen Medientypen · davon 1 Kopie außer Haus. Für Betriebe ergänzt um 1 Kopie, die offline oder unveränderbar liegt, und 0 Fehler beim letzten Wiederherstellungstest.

01

Was überhaupt gesichert werden muss

Gehen Sie die Liste einmal komplett durch – die Überraschungen stecken in den letzten Punkten.

- ☐ Benutzerordner: Dokumente, Bilder, Videos, Musik, Desktop, Downloads
- ☐ E-Mail-Archiv, Kontakte, Kalender
Bei lokal gespeicherten Postfächern (Outlook PST, Thunderbird-Profil) besonders wichtig.
- ☐ Browser-Lesezeichen, gespeicherte Passwörter, Passwort-Tresor
- ☐ Buchhaltung, Steuerprogramme, Fakturierung, Kassensystem
Diese Programme legen ihre Datenbank oft in einem eigenen Pfad ab – Speicherort im Programm nachschlagen, nicht raten.
- ☐ Branchensoftware und deren Datenbanken
Ordination, Werkstatt, Warenwirtschaft, Zeiterfassung.
- ☐ Projektdateien aus Bild-, Video-, Audio- und CAD-Programmen
- ☐ Lizenzschlüssel, Rechnungen, Aktivierungsdateien
- ☐ Konfigurationen: Netzwerkpläne, Router-Einstellungen, Zertifikate, VPN-Profile
- ☐ Website, Onlineshop und deren Datenbank
Ein Hosting-Backup allein reicht nicht – ziehen Sie eine eigene Kopie.
- ☐ Zwei-Faktor-Wiederherstellungscodes
Ohne sie sperren Sie sich nach einem Gerätewechsel selbst aus.

02

Medien und Ziele festlegen

Zwei verschiedene Technologien schlagen zwei gleiche Festplatten.

- ☐ Externe Festplatte oder SSD für die tägliche bzw. wöchentliche Sicherung
Nach dem Backup abstecken. Eine dauerhaft verbundene Platte wird von Verschlüsselungstrojanern mitverschlüsselt.
- ☐ Zweites Medium, das im Wechsel betrieben wird
Zwei Platten im Tausch: eine im Einsatz, eine außer Haus.
- ☐ Cloud-Backup mit Versionierung
Achtung: Ein Sync-Dienst wie OneDrive, iCloud oder Dropbox ist kein Backup – gelöschte oder verschlüsselte Dateien werden mitsynchronisiert.
- ☐ NAS oder Server mit eigenem Backup
Ein NAS ersetzt keine externe Kopie.
- ☐ Aufbewahrungsort außer Haus festlegen
Zweitwohnsitz, Büro, Bankschließfach, Familie. Feuer und Einbruch treffen sonst beide Kopien gleichzeitig.
- ☐ Backup-Medien verschlüsseln
Eine verlorene unverschlüsselte Platte ist ein meldepflichtiger Datenschutzvorfall.

- ☐ Speicherplatz prüfen: mindestens das Doppelte der Datenmenge

03 Rhythmus und Aufbewahrung

Die Frage lautet nicht „wie oft“, sondern: wie viele Stunden Arbeit können Sie verschmerzen?

- ☐ Sicherungsintervall festgelegt und aufgeschrieben
- ☐ Automatische Ausführung eingerichtet
Manuelle Backups werden zuverlässig vergessen – spätestens im stressigen Monat.
- ☐ Versionsstände aufbewahren, nicht nur den letzten Stand
Sonst überschreibt das Backup vom Dienstag den heilen Stand vom Montag.
- ☐ Monatlicher Vollstand wird zusätzlich archiviert
- ☐ Aufbewahrungsfristen berücksichtigt
Steuerlich relevante Unterlagen sind in Österreich sieben Jahre aufzubewahren – prüfen Sie das mit Ihrer Steuerberatung.
- ☐ Systemabbild des kompletten Rechners vorhanden
Spart im Ernstfall einen ganzen Tag Neuinstallation.

Datenart	Empfohlener Rhythmus	Aufbewahrung	Ziel
Laufende Arbeitsdateien	täglich, automatisch	30 Tage	Externe SSD + Cloud
E-Mail-Postfach	täglich	12 Monate	Cloud oder NAS
Buchhaltung, Rechnungen	wöchentlich + Monatsende	7 Jahre	Extern + außer Haus
Fotos und Videos	monatlich	dauerhaft	Zwei getrennte Medien
Systemabbild	vierteljährlich	letzte 2 Stände	Externe Festplatte
Website und Datenbank	wöchentlich	3 Monate	Lokal + Hosting

04 Der Test, den fast niemand macht

Ein Backup gilt erst als vorhanden, wenn eine Wiederherstellung gelungen ist.

- ☐ Vierteljährlich einzelne Dateien zurückspielen und wirklich öffnen
- ☐ Einmal jährlich eine vollständige Wiederherstellung testen
Auf einem Ersatzdatenträger, nicht auf dem Produktivsystem.
- ☐ Zeit stoppen: Wie lange dauert die Wiederherstellung tatsächlich?
Diese Zahl entscheidet im Ernstfall über Ihren Ausfalltag.
- ☐ Prüfen, ob auch die ältesten Versionsstände noch lesbar sind
- ☐ Backup-Protokolle und Fehlermeldungen kontrollieren
Viele Backups laufen monatelang mit Fehler – ohne dass es jemand merkt.
- ☐ Datum des letzten erfolgreichen Tests notieren

05 Schutz vor Verschlüsselungstrojanern

Ransomware sucht gezielt nach erreichbaren Backups.

- ☐ Mindestens eine Kopie offline halten
Abgesteckt im Schrank. Was nicht angeschlossen ist, kann nicht verschlüsselt werden.
- ☐ Backup-Ziel nicht dauerhaft als Laufwerksbuchstabe einbinden
- ☐ Für das Backup ein eigenes Konto mit eigenem Passwort verwenden

- ☐ Unveränderbare Speicherung nutzen, wenn der Anbieter sie anbietet
Stichwort Objektsperre oder Immutable Backup.
- ☐ Cloud-Papierkorb und Versionshistorie aktiviert
- ☐ Warnung einrichten, wenn ein Backup ausbleibt

06

Ihr Backup-Plan

Ausfüllen, ausdrucken, neben den Rechner hängen.

ERSTELLT VON

DATUM

NÄCHSTE PRÜFUNG AM

Was wird gesichert

Wohin

Wie oft

Wer

Zuletzt geprüft

07

Notfall-Ablauf bei Datenverlust

Diese Reihenfolge einhalten – jeder Schritt in falscher Reihenfolge kostet Daten.

- ☐ **Sofort aufhören zu arbeiten.**
Gerät nicht weiterverwenden, keine Programme installieren, keine Updates zulassen.
- ☐ **Bei Verdacht auf Verschlüsselung: Netzkabel ziehen bzw. WLAN abschalten.**
Andere Geräte und Backup-Medien vom Netz trennen, bevor sie mit betroffen sind.
- ☐ **Gerät ordentlich herunterfahren, nicht den Stecker ziehen.**
Bei Servern kann ein harter Ausschalter Folgeschäden verursachen.
- ☐ **Nichts löschen, nichts formatieren, keine Lösegeldzahlung leisten.**
- ☐ **Zustand dokumentieren: Fehlermeldungen fotografieren, Zeitpunkt notieren.**
- ☐ **Hilfe holen.**
1.wien unter +43 660 815 04 12. Betriebe zusätzlich: Cyber-Security-Hotline der Wirtschaftskammern 0800 888 133, täglich rund um die Uhr.
- ☐ **Bei Straftaten Anzeige erstatten.**
Meldestelle für Internetkriminalität des Bundeskriminalamts: against-cybercrime@bmi.gv.at. Cybercrime Helpline der Stadt Wien: 01 4000-4006, werktags 7:30–17:00 Uhr.
- ☐ **Bei betroffenen Personendaten Meldepflicht nach DSGVO prüfen.**
Innerhalb von 72 Stunden an die Datenschutzbehörde – im Zweifel rechtlich abklären lassen.

Wir richten das für Sie ein

1.wien konfiguriert Ihre Datensicherung, testet die Wiederherstellung und übergibt Ihnen einen ausgefüllten Backup-Plan. Auf Wunsch mit regelmäßiger Fernkontrolle über RS1-Fernwartung. · +43 660 815 04 12 · 1@1.wien · 1.wien