



DIGITAL

einfach erklärt

• VERSTEHEN. NUTZEN. SICHER SEIN. •

BAND 1

DIE CLOUD

Dein verständlicher Einstieg in die Welt der Cloud



Dateien sicher
speichern



Überall
zugreifen



Datenschutz
verstehen



Synchronisation
einfach erklärt



Sicher nutzen –
aber richtig



OneDrive



Google Drive



iCloud



Dropbox



NAS &
Eigene Cloud

FÜR EINSTEIGER – VERSTÄNDLICH – PRAXISNAH – AKTUELL
MIT VIELEN TIPPS, VERGLEICHEN UND EMPFEHLUNGEN



WAS IST
DIE CLOUD?



SICHERHEIT &
DATENSCHUTZ



SYNC &
BACKUP



TEILEN &
ZUSAMMENARBEIT



VORTEILE &
NACHTEILE



TIPPS &
BEST PRACTICES

Verstehen macht sicher. ♥

Vorwort

Dieses Buch ist aus einer einfachen Idee entstanden:

Die Freude daran, Wissen verständlich weiterzugeben.

Was mit einer kleinen Sammlung anschaulicher Infografiken begann, entwickelte sich Schritt für Schritt zu einem umfassenden Leitfaden rund um das Thema Cloud. Mein Ziel war dabei nie, ein technisches Fachbuch zu schreiben, sondern komplexe Zusammenhänge so zu erklären, dass sie jeder nachvollziehen kann – unabhängig von Vorkenntnissen.

Die Cloud begleitet heute unseren Alltag fast überall: auf dem Smartphone, dem Tablet, dem Computer oder im Smart Home. Trotzdem bleibt vieles für viele Menschen undurchsichtig. Genau hier setzt dieses Buch an. Es soll Orientierung geben, Begriffe verständlich erklären und dabei helfen, die Möglichkeiten moderner Cloud-Dienste sicher und sinnvoll zu nutzen.

Ich hoffe, dieses Buch macht Mut, Neues auszuprobieren, technische Zusammenhänge besser zu verstehen und die Cloud bewusster, sicherer und mit mehr Freude zu nutzen.

Denn Wissen wird erst dann wertvoll, wenn man es teilt.

Inhaltsverzeichnis

Grundlagen

- Was ist die Cloud?
- Welche Cloud passt zu mir
- Cloud # Backup
- Die 3-2-1 Regel
- Welche Daten gehören überhaupt in die Cloud
- Daten sicher teilen – So geht's richtig
- Gemeinsame Ordner richtig nutzen
- Cloud synchronisieren oder nur speichern?
- Cloud-Speicher sparen
- Cloud-Ordnung
- Cloud umziehen
- Cloud und Datenschutz
- Die größten Cloud-Fehler
- Cloud + NAS
- Cloud + Smartphone
- Cloud + Windows & MacOS
- Cloud + KI
- Cloud + Familienfreigabe

Cloud-Dienste

- iCloud
- Google Drive
- Dropbox
- OneDrive

Eigene Cloud

- NAS
- Self Hosted Cloud
- Cloud vs. NAS

Sicherheit

- Cloud-Sicherheit
- Cryptomator
- VeraCrypt
- Cyberduck
- Mountain Duck

Abschluss

- Die perfekte Cloud für Zuhause
- Die 10 größten Cloud-Irrtümer
- Fazit

WAS IST DIE CLOUD?

Einfach erklärt.

Die Cloud ist ein Dienst, über den du deine Daten sicher im Internet speicherst, darauf zugreifst und sie mit anderen teilst.



WIE FUNKTIONIERT DIE CLOUD?

DEINE GERÄTE

- PC / Laptop
- Smartphone
- Tablet
- und mehr ...



INTERNET



RECHENZENTRUM
(Cloud-Anbieter)

DEINE DATEN

- Dateien
- Fotos
- Videos
- Musik
- und mehr ...



DU SPEICHERST DEINE DATEN

Die Daten werden sicher in der Cloud gespeichert.



SYNCHRONISATION

Änderungen werden automatisch mit allen deinen Geräten abgeglichen.



ÜBERALL ZUGREIFEN

Du kannst jederzeit und von überall auf deine Daten zugreifen.



DER ANBIETER KÜMMERT SICH

Um Server, Sicherheit, Wartung, Backups und Verfügbarkeit.

WAS IST DIE CLOUD NICHT?



KEINE FESTPLATTE IN DEN WOLKEN
Deine Daten liegen in Rechenzentren auf echten Servern – nicht „irgendwo“.



KEIN BACKUP
Die Cloud schützt nicht vor versehentlichem Löschen, Ransomware oder Hardware-Defekten. Ein echtes Backup ist weiterhin wichtig!



NICHT AUTOMATISCH UNSICHER
Mit den richtigen Einstellungen ist die Cloud sicher – wie dein Online-Banking.



NICHT NUR FÜR FIRMEN
Die Cloud ist für jeden – privat, in der Familie oder im Beruf.

TYPISCHE CLOUD-DIENSTE



OneDrive

Von Microsoft. Ideal für Windows-Nutzer. Integriert in Office.



Google Drive

Von Google. Perfekt vernetzt mit Gmail, Docs, Fotos u.v.m.



iCloud

Von Apple. Optimal für iPhone, iPad und Mac. Einfache Bedienung.



Dropbox

Einfach, zuverlässig und plattformunabhängig. Teilen leicht gemacht.



VORTEILE DER CLOUD



ÜBERALL VERFÜGBAR
Zugriff auf deine Daten von überall auf der Welt.



MEHRERE GERÄTE
Einmal speichern – überall verfügbar.



EINFACH TEILEN
Dateien und Ordner mit anderen teilen.



AUTOMATISCHE SYNCHRONISATION
Änderungen werden automatisch übernommen.



PLATZ SPAREN
Weniger Speicherplatz auf deinen Geräten nötig.

NACHTEILE DER CLOUD



INTERNET VERBINDUNG
Für den Zugriff wird meistens eine Internetverbindung benötigt.



DATENSCHUTZ BEACHTEN
Deine Daten liegen bei einem Anbieter – die Bedingungen prüfen!



ANBIETERABHÄNGIGKEIT
Änderungen bei Preisen, Speichern oder Bedingungen möglich.



KEIN ERSATZ FÜR BACKUPS
Ein Backup auf einem zweiten System bleibt unerlässlich.



KOSTEN
Kostenlose Tarife haben oft Speicher- oder Funktionslimits.

FÜR WEN IST DIE CLOUD?



PRIVATNUTZER
Fotos sichern, Dateien speichern, mit Familie teilen und überall verfügbar haben.



FAMILIEN
Gemeinsame Ordner, Kalender, Fotos und vieles mehr – für alle einfach.



BERUF & TEAM
Zusammenarbeiten, Projekte teilen und produktiver im Team arbeiten.

FAZIT

Die Cloud macht unser digitales Leben einfacher, flexibler und sicherer – wenn man sie richtig versteht und bewusst nutzt.



VERSTEHEN. NUTZEN. SICHER SEIN.



TIPP: Die Cloud ist ein mächtiges Werkzeug – aber kein Ersatz für gesunden Menschenverstand. Informiere dich, prüfe Einstellungen und sichere wichtige Daten zusätzlich.





WELCHE CLOUD PASST ZU MIR?



Drei Wege in die Cloud – je nach Bedarf und Anspruch



PUBLIC CLOUD

Einfach. Flexibel. Anbieter-verwaltet.



Microsoft OneDrive
von Microsoft



Google Drive
von Google



Dropbox
von Dropbox



iCloud
von Apple



Einfach zu nutzen



Keine eigene Infrastruktur nötig



Von überall erreichbar



Wartung, Updates und Sicherheit übernimmt der Anbieter



Flexibel und skalierbar



FÜR WEN?

Ideal, wenn du eine unkomplizierte Lösung suchst, schnell starten möchtest und die Verwaltung an den Anbieter überlassen willst.



PRIVATE CLOUD

Mehr Kontrolle. Eigene Verantwortung.



Synology
DiskStation



QNAP
NAS Systeme



Nextcloud
Selbst gehostet



Volle Kontrolle über deine Daten und Konfiguration



Eigene Administration erforderlich



Regelmäßige Updates und Wartung nötig



Eigene Backups für Datensicherheit



Individuell anpassbar und erweiterbar



Unabhängig von Anbietern und Internetdiensten



FÜR WEN?

Geeignet, wenn du maximale Kontrolle möchtest und bereit bist, Administration, Updates und Backups selbst zu übernehmen.



HYBRID CLOUD

Das Beste aus beiden Welten.



Kombination aus eigener Infrastruktur und Public-Cloud Diensten



Vereinigt die Vorteile beider Welten



Mehr Flexibilität bei Datenspeicherung und Zugriff



Geeignet z. B. für Backup, Archivierung oder geteilte Daten



Höhere Komplexität in Planung, Administration und Kosten



Sorgfältige Abstimmung von Sicherheit, Zugriffsrechten und Datenflüssen nötig



FÜR WEN?

Sinnvoll, wenn du bestimmte Daten lokal halten und gleichzeitig die Flexibilität der Public Cloud nutzen möchtest – und die zusätzliche Komplexität bewältigen kannst.

KURZ & KNAPP



PUBLIC CLOUD

- Schnell startklar
- Anbieter-verwaltet
- Flexibel und kostengünstig
- Ideal für den Alltag



PRIVATE CLOUD

- Mehr Kontrolle
- Eigene Verantwortung
- Wartung und Backups nötig
- Individuell anpassbar



HYBRID CLOUD

- Kombination beider Ansätze
- Mehr Flexibilität
- Auch höhere Komplexität
- Für spezielle Anforderungen



UNSER TIPP:

Überlege dir, was dir am wichtigsten ist: Komfort und einfache Nutzung – oder maximale Kontrolle? Oft ist eine Kombination aus beiden der beste Weg für deine persönliche Situation.





1 CLOUD ≠ BACKUP

DER GRÖSSTE IRRTUM ÜBERHAUPT.

Viele glauben: „Meine Daten sind in der Cloud – also sind sie sicher.“ **FALSCH!**



Cloud ist in erster Linie ein Synchronisations- und Zugriffsdienst. Backup ist eine Sicherheitskopie für den Ernstfall.

CLOUD
= KOMFORT



BACKUP
= SICHERHEIT



1 LÖSCHEN = ÜBERALL GELÖSCHT



Löschst du eine Datei in der Cloud oder auf einem Gerät, wird sie auf allen verbundenen Geräten ebenfalls gelöscht.

Beispiel:

Du löschst versehentlich einen wichtigen Ordner → überall weg.

Fazit:

Ohne Backup ist die Datei endgültig verloren.



2 VERSCHLÜSSELUNG SCHÜTZT NICHT VOR BEDIENFEHLERN



Verschlüsselung schützt deine Daten vor Fremdzugriff – aber nicht vor dir selbst.

Wenn du etwas löschst, überschreibst oder beschädigst, hilft auch die beste Verschlüsselung nicht weiter.

Beispiel:

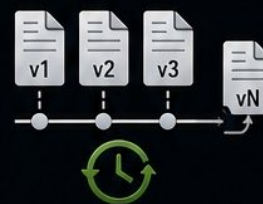
Du löschst eine wichtige verschlüsselte Datei → sie ist trotzdem weg.

Fazit:

Sicherheit vor Außen, aber kein Schutz vor eigenen Fehlern.



3 VERSIONIERUNG HILFT NUR BEGRENZT



Viele Cloud-Dienste bieten Versionierung oder Papierkorb an – aber nur für einen begrenzten Zeitraum (7, 30 oder 90 Tage).

Danach werden alte Versionen automatisch gelöscht.

Beispiel:

Du bemerkst nach 3 Monaten, dass eine Datei falsch überschrieben wurde – die alte Version ist nicht mehr verfügbar.

Fazit:

Versionierung ist praktisch – aber kein vollständiges Backup.



4 WARUM EIN BACKUP TROTZDEM PFLICHT IST



Ein richtiges Backup schützt dich vor Ereignissen, die die Cloud nicht abdecken kann.

Dazu gehören:

- 👤 Löschen oder Überschreiben
- 👤 Hackerangriffe & Ransomware
- 🔥 Cloud-Ausfälle oder Provider-Probleme
- 📧 Dateibeschädigung / -korruption
- 🔒 Kündigung oder Sperrung des Kontos

Fazit:

Nur ein Backup gibt dir echte Sicherheit & Kontrolle über deine Daten.



WARUM EIN BACKUP UNVERZICHTBAR IST



SCHÜTZT VOR DATENVERLUST

Ermöglicht die Wiederherstellung bei Löschfehlern, Angriffen oder technischen Defekten.



UNABHÄNGIGKEIT

Du bist nicht vom Cloud-Anbieter abhängig. Deine Daten bleiben deine Daten.



LANGFRISTIGE SICHERHEIT

Backups können dauerhaft aufbewahrt werden – länger als die Cloud-Versionierung erlaubt.



MEHRERE KOPIEN

Ein Backup kann nach der 3-2-1-Regel erstellt werden: 3 Kopien, 2 Medienarten, 1 Kopie außer Haus.



SEELENFRIEDEN

Ein gutes Backup gibt dir das beruhigende Gefühl: „Was auch immer passiert – ich habe meine Daten.“

GUTE BACKUP-PRAKIS FÜR PRIVATNUTZER

- ✓ Nutze mindestens 2 verschiedene Speichermedien (z. B. externe Festplatte + Cloud/NAS).
- ✓ Automatisiere deine Backups (regelmäßig & zuverlässig).
- ✓ Prüfe regelmäßig, ob dein Backup funktioniert (Test-Wiederherstellung).
- ✓ Bewahre Backups an einem sicheren Ort auf (z. B. offline oder außer Haus).
- ✓ Versioniere Backups (z. B. täglich, wöchentlich, monatlich).

3-2-1-REGEL

- 3x 3 Kopien deiner Daten
- 2x 2 verschiedene Speichermedien
- 1x 1 Kopie außer Haus (z. B. in der Cloud oder bei Familie)

BEISPIEL: WAS KANN SCHIEF GEHEN?

- 👤 **RANSOMWARE**
Deine Dateien werden verschlüsselt – auch in der Cloud.
- 👤 **BEDIENFEHLER**
Eine Datei wird versehentlich gelöscht oder überschrieben.
- 👤 **CLOUD-AUSFALL**
Der Anbieter hat Probleme – du hast keinen Zugriff auf deine Daten.
- 🔒 **KONTO GESPERRT**
Verstoß gegen AGB oder Hack – Zugriff gesperrt oder Daten verloren.

OHNE BACKUP = VERLOREN!



MERKE DIR:

Cloud ist super für Zugriff & Synchronisation. Aber nur ein Backup ist echte Sicherheit!



FAZIT:

Cloud kann löschen, verlieren oder ausfallen. Ein Backup bleibt – und rettet deine Daten.



DEINE DATEN.

DEINE VERANTWORTUNG.
DEIN BACKUP.



DIE 3-2-1-REGEL

EINE ROBUSTE RICHTLINIE FÜR ZUVERLÄSSIGE BACKUPS

Die 3-2-1-Regel ist eine bewährte **Best Practice**, um deine Daten vor Verlust zu schützen. Sie ist **keine** einzige Definition von „Backup“ und **keine Garantie für maximale Sicherheit** – aber ein hervorragender Standard, der Risiken deutlich reduziert.



3 KOPIEN INS GESAMT

Halte mindestens 3 Kopien deiner Daten:

- ✓ 1 Original
- ✓ + 2 Backups
- ✓ = 3 Kopien



2 VERSCHIEDENE SPEICHERMEDIEN ODER SYSTEME

Speichere die Kopien auf mindestens 2 unterschiedlichen Speichermedien oder Systemen, z. B. Festplatte und Cloud-Speicher.



1 KOPIE AUSSER HAUS

Bewahre mindestens eine Kopie an einem anderen physischen Standort auf – z. B. in der Cloud oder an einem zweiten Standort (Familie, Büro, Tresor).



SO KANN DIE 3-2-1-REGEL IN DER PRAXIS AUSSEHEN

1. ORIGINAL

Dein Arbeitsgerät



PC / LAPTOP



Regelmäßige Backups

2. LOKALES BACKUP

Zweite Kopie auf anderem Medium



NAS / EXTERNE FESTPLATTE



Zusätzliche Kopie außer Haus

3. OFFSITE-BACKUP

Dritte Kopie an anderem Standort



CLOUD-SPEICHER
(z. B. OneDrive, Google Drive, Backblaze, Dropbox etc.)

WORAUF DU ACHTEN SOLLTEST

GERÄTEDEFEKT

Hardware kann ausfallen – jederzeit.



Ein Backup schützt deine Daten.

DIEBSTAHL / VERLUST

Geräte können gestohlen oder verloren werden.



Eine Kopie außer Haus schützt dich.

BRAND / WASSER

Feuer, Wasser oder andere Katastrophen können alles vor Ort zerstören.



Verteilte Kopien minimieren das Risiko.

RANSOMWARE

Daten können verschlüsselt oder manipuliert werden.



Offline- oder unveränderliche Kopien helfen, wiederherzustellen.

BEDIENTEHLER

Dateien können versehentlich gelöscht oder überschrieben werden.



Versionen und Backups ermöglichen die Wiederherstellung.

PRAKTISCHE TIPPS

- ✓ Mindestens eine Kopie offline oder unveränderlich (immutable) aufbewahren, wo möglich.
- ✓ Backups regelmäßig und automatisch erstellen.
- ✓ Wiederherstellung regelmäßig testen („Restore-Tests“).
- ✓ Synchronisation und Versionsverlauf sind kein vollständiger Backup-Ersatz.
- ✓ Backup-Strategie dokumentieren und aktuell halten.



GEEIGNETE SPEICHERMEDIEN

- Externe Festplatte (HDD)**
Viel Speicherplatz, günstig
- Externe SSD**
Schnell, robust, ideal für wichtige Daten
- NAS-System**
Zentral, sicher, für mehrere Geräte
- Cloud-Speicher**
Außer Haus, automatisch, skalierbar
- Band / WORM-Speicher**
Sehr langlebig, unveränderlich (immutable)

BEISPIELE FÜR 3-2-1-SETUPS

- PC → NAS → Cloud
(z. B. OneDrive, Google Drive)
- Laptop → Externe HDD → Cloud
- Mac → Time Machine HDD → Cloud
- PC → Externe SSD → NAS → Cloud

★ Passe die Lösung an deine Bedürfnisse, deine Daten und dein Budget an.



BACKUPS GEBEN DIR KONTROLLE – NICHT NUR IM NOTFALL, SONDERN JEDEN TAG.



REGELMÄSSIG TESTEN STATT NUR HOFFEN.



EINE STARKE RICHTLINIE FÜR MEHR SICHERHEIT.

ES GEHT NICHT DARUM, OB ETWAS PASSIERT, SONDERN DASS DU DANN BEREIT BIST.

SICHERE HEUTE, WAS DIR MORGEN WICHTIG IST.

WELCHE DATEN GEHÖREN ÜBERHAUPT IN DIE CLOUD?

Nicht alle Daten sind gleich. Hier siehst du, welche Daten sich gut für die Cloud eignen – und welche du besser schützen oder sogar komplett draußen lassen solltest.



KATEGORIE	BEISPIELE	EIGNUNG FÜR CLOUD	EMPFEHLUNG	BEGRÜNDUNG
GUT GEEIGNET FÜR DIE CLOUD Diese Daten kannst du bedenkenlos in der Cloud speichern (bei einem seriösen Anbieter).	Fotos • Urlaubsbilder • Familienfotos • Screenshots	ALLTÄGLICH Geringes Risiko	JE NACH INHALT SCHÜTZEN	Normale Fotos können mit normalem Kontoschutz gespeichert werden. Private, intime oder identifizierende Bilder besser clientseitig verschlüsseln oder nicht hochladen.
	Dokumente • Briefe • Rechnungen • Notizen	ALLTÄGLICH Geringes Risiko	JE NACH INHALT SCHÜTZEN	Alltägliche Dokumente können normal gespeichert werden. Dokumente mit persönlichen oder vertraulichen Informationen besser clientseitig verschlüsseln.
	Steuerunterlagen • Steuererklärungen • Belege • Bescheinigungen	SENSIBEL Erhöhtes Risiko	CLIENTSEITIG VERSCHLÜSSELN	Steuerunterlagen enthalten regelmäßig Steuer-ID, Einkommen, Bank- und persönliche Daten. Vor dem Upload clientseitig verschlüsseln.
	Musik • MP3 / FLAC • Playlists • Alben	ALLTÄGLICH Geringes Risiko	UNVERSCHLÜSSELT MÖGLICH	Einfach zu ersetzen, Streaming & Zugriff von überall.
BEDENKLICH – NUR MIT VORSICHT Diese Daten sind sensibel. Wenn du sie in der Cloud speicherst, dann nur verschlüsselt (z. B. mit Cryptomator).	Passwortdatenbank • Passwort-Manager Tresor (verschlüsselt) • Verschlüsseltes Backup	SENSIBEL Erhöhtes Risiko	NUR VERSCHLÜSSELT SPEICHERN	Nur den verschlüsselten Passwort-Manager-Tresor oder ein verschlüsseltes Backup speichern. Niemals unverschlüsselte Exporte im Klartext.
	Ausweiskopien • Personalausweis • Reisepass • Führerschein	SENSIBEL Erhöhtes Risiko	CLIENTSEITIG VERSCHLÜSSELN	Enthalten hochsensible Identitätsdaten. Clientseitig verschlüsseln, Schlüssel selbst verwalten und nur bei Bedarf mit vertrauenswürdigen Personen teilen.
	Verträge • Mietverträge • Arbeitsverträge • Versicherungen	SENSIBEL Erhöhtes Risiko	CLIENTSEITIG VERSCHLÜSSELN	Wichtige Dokumente enthalten oft persönliche und finanzielle Informationen. Clientseitig verschlüsseln und nur bei Bedarf teilen.
NICHT IN DIE CLOUD – ODER NUR VERSCHLÜSSELT & EXTREM SICHER Diese Daten sind hochsensibel. Bewahre sie am besten lokal & verschlüsselt auf. WENN Cloud – DANN nur mit starker Verschlüsselung (z. B. mit Cryptomator oder VeraCrypt).	Gesundheitsdaten • Arztberichte • Diagnosen • Laborwerte	HOCHSENSIBEL Sehr hohes Risiko	CLIENTSEITIG VERSCHLÜSSELN	Sehr sensible Daten mit höchstem Schutzbedarf. Clientseitig verschlüsseln, Schlüssel selbst verwalten und nur bei Bedarf teilen.
	Kryptowallets • Wallet-Backups • Seed Phrases • Private Keys	HOCHSENSIBEL Sehr hohes Risiko	NIE IN DER CLOUD Nur lokal & offline sichern	Seed Phrases und Private Keys niemals in normaler Cloud-Speicherung. Offline und separat geschützt in einem Notfallplan aufbewahren.
	Passwort-Export / CSV • Export-Dateien • Backup-Dateien aus Passwort-Managern	HOCHSENSIBEL Sehr hohes Risiko	NIE UNVERSCHLÜSSELT SPEICHERN Temporäre Exporte sicher löschen	Eine Datei kann alle deine Konten kompromittieren. Niemals unverschlüsselt speichern. Temporäre Exporte nach der Verwendung sicher löschen.

BEST PRACTICE: SICHER IN DER CLOUD SPEICHERN



Verschlüsselung nutzen
Sensible Daten immer vor dem Upload mit Cryptomator oder VeraCrypt verschlüsseln.



Starke Passwörter & 2FA
Schütze dein Cloud-Konto mit starken Passwörtern und Zwei-Faktor-Auth.



Zugriffsrechte prüfen
Teile Daten nur mit vertrauenswürdigen Personen und prüfe regelmäßig Berechtigungen.



Backups nicht vergessen
Cloud ersetzt kein Backup! Halte immer ein zusätzliches Backup vor.



MERKE DIR:
Cloud = Komfort
Backup = Sicherheit
Nutze beides – aber richtig!



FAZIT: DIE CLOUD IST PRAKTISCH – ABER NICHT ALLES GEHÖRT HINEIN. DENKE NACH, WAS DU SPEICHERST. SCHÜTZE, WAS DIR WICHTIG IST.



DATEN SICHER TEILEN SO GEHT'S RICHTIG!

Dateien mit anderen zu teilen ist praktisch – aber auch ein Risiko, wenn du es falsch machst. Mit diesen Empfehlungen teilst du sicher, behältst die Kontrolle und schützt deine Daten und die Privatsphäre anderer.



DIE 6 WICHTIGSTEN EMPFEHLUNGEN FÜR SICHERES TEILEN

1 NAMENTLICH TEILEN STATT ÖFFENTLICHER LINK



- Teile möglichst direkt mit bestimmten Personen oder Konten (E-Mail, Benutzername).
- Vergib nur die minimal nötigen Rechte (z. B. nur anzeigen statt bearbeiten).

TIPP
Nur die Personen einladen, die es wirklich brauchen.

2 WENN ÖFFENTLICHER LINK NOTIG IST – MIT SCHUTZMASSNAHMEN



- Nutze einen Link nur, wenn keine namentliche Freigabe möglich ist.
- Wenn vom Anbieter/Tarif unterstützt: Passwort, Ablaufdatum und Download-Beschränkung aktivieren.
- Link nur über einen sicheren Kanal (z. B. verschlüsselte Nachricht) weitergeben.

TIPP
Je mehr Schutzoptionen du nutzt, desto geringer das Risiko.

3 ABLAUFDATUM FESTLEGEN



- Setze ein Ablaufdatum (wenn vom Anbieter/Tarif unterstützt).
- Der Zugriff endet dann automatisch.
- So vermeidest du, dass Links unbeabsichtigt dauerhaft aktiv bleiben.

TIPP
Nur so lange teilen, wie es wirklich nötig ist.

4 DOWNLOADS BESCHRÄNKEN (WENN MÖGLICH)



- Wenn vom Anbieter/Tarif unterstützt: Downloads deaktivieren oder auf die Web-Ansicht beschränken (z. B. nur anzeigen, nicht herunterladen).
- Das verhindert, dass Kopien unkontrolliert weitergegeben werden.

TIPP
Besonders wichtig bei vertraulichen oder personenbezogenen Daten.

5 FÜR SENSIBLE DATEN ZUSÄTZLICH ENDE-ZU-ENDE-VERSCHÜSSELUNG



- Für besonders sensible Dateien zusätzlich Ende-zu-Ende-Verschlüsselung oder Client-seitige Verschlüsselung nutzen (z. B. verschlüsselte Archive).
- Dabei werden die Daten schon auf deinem Gerät verschlüsselt – nur die berechtigten Personen können sie öffnen.

TIPP
Passwörter separat über einen anderen Kanal mitteilen.

6 FREIGABEN REGELMÄSSIG PRÜFEN UND WIDERRUFEN



- Überprüfe regelmäßig, wer Zugriff hat.
- Nicht mehr benötigte Freigaben sofort widerrufen.
- Achte auf Änderungen (z. B. wenn Personen das Team verlassen).
- Behalte auch geteilte Ordner im Blick.

TIPP
Mindestens einmal im Quartal alle Freigaben prüfen.

WAS BEDEUTET DAS KONKRET?



Link kann weitergegeben werden
Ein Link ist wie ein digitaler Schlüssel. Jede Person, die den Link erhält, kann ihn an andere weiterleiten – auch unbeabsichtigt. Du verlierst schnell die Kontrolle.



Transport-/Server-Verschlüsselung ≠ Ende-zu-Ende
Die meisten Cloud-Dienste verschlüsseln deine Daten auf dem Weg zum Server und im Ruhezustand auf ihren Servern. Das schützt vor Mitlesen auf dem Weg – aber der Anbieter kann in der Regel auf die Daten zugreifen. Ende-zu-Ende-Verschlüsselung bedeutet, dass nur du und die berechtigten Empfänger die Daten entschlüsseln können.



Nicht jeder Anbieter unterstützt alle Funktionen
Optionen wie Passwortschutz, Ablaufdatum oder die Deaktivierung von Downloads sind nicht bei allen Diensten oder Tarifen verfügbar. Prüfe die Möglichkeiten in deinem Dienst und nutze, was unterstützt wird.

WAS KANN PASSIEREN, WENN DU ES FALSCH MACHST?



Unbeabsichtigte Weitergabe
Ein Link wird weitergeleitet und gelangt in falsche Hände.

Folge: Ungewollter Zugriff auf vertrauliche Daten.



Datenlecks und Missbrauch
Geteilte Dateien können kopiert, weiterverbreitet oder für andere Zwecke genutzt werden (z. B. Identitätsdiebstahl, Betrug).

Folge: Finanzieller Schaden, Reputationsverlust.



Zu weitreichende Rechte
Empfänger können Dateien verändern oder löschen, wenn sie Bearbeitungsrechte haben.

Folge: Datenverlust oder unbeabsichtigte Änderungen.



Dauerhaft aktive Links
Ohne Ablaufdatum bleiben Links oft unbegrenzt gültig – auch wenn du sie nicht mehr brauchst.

Folge: Langfristige Risiken und Kontrollverlust.



Fehlende Verschlüsselung bei sensiblen Daten
Ohne Ende-zu-Ende-Verschlüsselung kann der Anbieter auf die Daten zugreifen.

Folge: Erhöhtes Risiko bei besonders sensiblen oder personenbezogenen Daten.

ZUSÄTZLICHE TIPPS FÜR MEHR SICHERHEIT

- Teile nur das Nötigste und vermeide unnötig große Dateien.
- Nutze starke, einzigartige Passwörter (wenn unterstützt).
- Aktiviere Zwei-Faktor-Authentifizierung (2FA) für deinen Account.
- Sei besonders vorsichtig bei personenbezogenen, vertraulichen oder geschäftskritischen Daten.
- Nutze professionelle Lösungen mit guten Sicherheitsfunktionen und informiere dich über die Optionen deines Anbieters.

FUNKTIONSÜBERSICHT (JE NACH ANBIETER/TARIF)

FUNKTION				
Namentlich teilen	✓	✓	✓	✓
Öffentlicher Link	✓	✓	✓	✓
Passwortschutz	✓	✓	✓	–
Ablaufdatum	✓	✓	✓	–
Downloads deaktivieren	✓	✓	✓	–
Ende-zu-Ende-Verschlüsselung (Client-seitig)	✓	✓	✓	✓
Freigaben verwalten/widerrufen	✓	✓	✓	✓

Verfügbare Funktionen können je nach Anbieter und Tarif variieren.



MERKE DIR

- Möglichst namentlich teilen, nicht öffentlich.
- Nur so viele Rechte wie nötig.
- Ablaufdatum und Download-Beschränkung – wenn unterstützt.
- Bei sensiblen Daten: Ende-zu-Ende-Verschlüsselung nutzen.
- Freigaben regelmäßig prüfen und widerrufen.

Sicher teilen schützt dich, und die Menschen, deren Daten dir anvertraut sind.



SICHER TEILEN. MEHR KONTROLLE. MEHR VERTRAUEN.

DIE RICHTIGEN EINSTELLUNGEN MACHEN DEN UNTERSCHIED.



GEMEINSAME ORDNER RICHTIG NUTZEN

Zusammenarbeiten, teilen und organisieren – sicher, strukturiert und effizient.
So holst du das Beste aus der Cloud für dich und andere heraus.



DIE 5 WICHTIGSTEN GRUNDSÄTZE



KLARE VERANTWORTUNG

Lege eine oder mehrere Verantwortliche (Owner) fest, die Struktur, Rechte und Ordnung koordinieren.



NUR NOTIGE ZUGRIFFSRECHTE

Gib nur die minimal notwendigen Rechte – so wenig wie möglich, so viel wie nötig.



SINNVOLLE ORDNERSTRUKTUR

Halte Ordner klein, verständlich und logisch strukturiert – für weniger Suchen und mehr Übersicht.



ÄNDERUNGEN IM BLICK

Nutze Benachrichtigungen und den Versionsverlauf (sofern verfügbar), um Änderungen nachzuvollziehen.



DATENSCHUTZ UND SICHERHEIT

Teile nur, was wirklich geteilt werden muss, und trenne interne und externe Inhalte klar voneinander.

PRAKTISCHE TIPPS NACH BEREICHEN



ORGANISATION & STRUKTUR



EINDEUTIGE ORDNERSTRUKTUR

- Klare, verständliche Namen
- Einheitliche Struktur für alle
- Nicht zu viele Unterordner



NAMENSKONVENTIONEN

- Eindeutige, kurze Namen
- Optional mit Datum oder Projekt
- Sonderzeichen vermeiden



INTERN UND EXTERN TRENNEN

- Separate Ordner für interne und externe Zusammenarbeit
- Sensible Inhalte nur intern teilen



REGELMÄSSIG ÜBERPRÜFEN

- Zugriffsrechte regelmäßig prüfen
- Nicht mehr benötigte Zugriffe entfernen (z. B. ehemalige Teammitglieder)

TIPP: Weniger ist mehr – eine einfache, klare Struktur wird langfristig besser genutzt.



ZUSAMMENARBEIT & INHALTE



ZUGRIFFSRECHTE

- Rollen wie Lesen, Bearbeiten oder Verwalten – je nach Bedarf
- Rollen und deren Möglichkeiten unterscheiden sich je nach Anbieter und Tarif



VERSIONEN UND SICHERHEIT

- Versionsverlauf nutzen (sofern verfügbar)
- Wichtige Dateien zusätzlich unabhängig sichern (z. B. lokale Kopie oder Backup-Lösung)



DATEIFREIGABEN

- Links mit Ablaufdatum verwenden (sofern verfügbar)
- Zugriff bei Bedarf widerrufen
- Geteilte Links nicht unnötig weit verbreiten



ÜBERGABE UND AUFRÄUMEN

- Bei Rollenwechseln Eigentum übertragen (sofern möglich)
- Zugriffe ehemaliger Mitglieder zeitnah entfernen
- Gelöschte Dateien landen meist im Papierkorb – Aufbewahrungsdauer hängt vom Anbieter und Tarif ab

TIPP: Vereinbart gemeinsame Regeln und haltet sie schriftlich fest – das vermeidet Missverständnisse.



KONKRETE ANWENDUNGSFÄLLE



IM TEAM

- Gemeinsame Dokumente bearbeiten
- Protokolle und Vorlagen teilen
- Projekte transparent halten



MIT EXTERNEN

- Nur notwendige Ordner teilen
- Zeitlich begrenzte Links nutzen (sofern verfügbar)
- Sensible Daten besonders schützen



FÜR UNTERWEGS

- Auf allen Geräten aktuell zugreifen
- Offline-Funktionen nutzen (sofern verfügbar)



FÜR LANGFRISTIGE ARBEIT

- Wichtige Dateien geordnet aufbewahren
- Versionen nachvollziehen
- Unabhängige Sicherung einplanen

TIPP: Halte geteilte Ordner aufgeräumt und entferne regelmäßig Altes – das erleichtert die Zusammenarbeit für alle.

BEST PRACTICE – KURZ UND KNAPP



KLARE VERANTWORTUNG

Mindestens einen eindeutigen Owner festlegen.



GERINGSTE RECHTE

Nur die minimal notwendigen Zugriffe vergeben.



GETRENNTE ORDNER

Interne und externe Inhalte separat halten.



REGELMÄSSIGE PRÜFUNG

Zugriffe und geteilte Links regelmäßig überprüfen und nicht mehr benötigte Zugriffe entfernen.



VERSIONEN + BACKUP

Versionsverlauf nutzen und wichtige Daten zusätzlich unabhängig sichern.



NACH DEM AUSTITT

Zugriffe ehemaliger Mitglieder zeitnah entfernen und Eigentum übertragen.

TYPISCHE FUNKTIONEN BEI CLOUD-DIENSTEN*

FUNKTION	BASIC	STANDARD	BUSINESS	ENTERPRISE
Ordner teilen	✓	✓	✓	✓
Rollen/Rechte	—	✓	✓	✓
Versionsverlauf	—	✓	✓	✓
Ablaufdatum für Links	—	✓	✓	✓
Papierkorb/Wiederherstellung	—	✓	✓	✓
Eigentum übertragen	—	—	✓	✓

*Funktionsumfang, Bezeichnungen und Verfügbarkeit unterscheiden sich je nach Anbieter und Tarif.

SICHER ZUSAMMENARBEITEN



DATEN BEWUSST TEILEN

Nur das teilen, was wirklich nötig ist.



SENSIBLE INHALTE SCHÜTZEN

Vertrauliche Informationen besonders sorgfältig behandeln.



MENSCHEN IM BLICK

Zugriffe regelmäßig prüfen und aktuell halten.

KEINE EINZIGE SICHERUNG

Auf den Versionsverlauf verlassen, aber zusätzlich eigene Backups einplanen.



GEMEINSAM NUTZEN. GEMEINSAM MEHR ERREICHEN.

Mit klarer Struktur, verantwortungsvollem Umgang und einem wachsamen Blick bleibt die Cloud ein echter Teamplayer.



6 CLOUD SYNCHRONISIEREN ODER NUR SPEICHERN?

Sehr häufig falsch verstanden.

Nicht jede Datei muss überall sein – aber du solltest wissen, was wirklich passiert. Hier sind die 3 wichtigsten Modi im Vergleich:



1 SYNCHRONISIEREN



⇔ Datei existiert lokal **UND** online

WIE ES FUNKTIONIERT

- Dateien werden automatisch zwischen deinem Gerät und der Cloud abgeglichen.
- Änderungen werden überall übernommen.
- Dateien nehmen Speicherplatz auf deinem Gerät ein.

BESTE VERWENDUNG FÜR

- Aktiv arbeitest du an Dateien
- Ordner, die du oft brauchst
- Teams oder gemeinsame Arbeit

BEISPIELE

- OneDrive – Synchronisieren
- Google Drive – Streamen & synchronisieren
- Dropbox – Synchronisierung



MERKE DIR:

Idealer Modus für aktive Arbeit und schnellen Zugriff – aber verbraucht lokalen Speicher!

2 NUR ONLINE



☁ Datei nur in der Cloud

WIE ES FUNKTIONIERT

- Die Datei bleibt nur in der Cloud gespeichert.
- Auf deinem Gerät siehst du nur eine Verknüpfung (Platzhalter).
- Die Datei wird erst heruntergeladen, wenn du sie öffnest.
- Spart viel Speicherplatz auf deinem Gerät.

BESTE VERWENDUNG FÜR

- Große Dateien, die du selten brauchst
- Archive und Backups
- Wenig Speicherplatz auf dem Gerät

BEISPIELE

- OneDrive – Nur online
- Google Drive – Nur online
- Dropbox – Online-only



MERKE DIR:

Perfekt für große Datenmengen – dein Gerät bleibt schlank!

3 OFFLINE VERFÜGBAR



↓ Download bei Bedarf

WIE ES FUNKTIONIERT

- Datei bleibt online, wird aber auf deinem Gerät gespeichert.
- Du kannst sie auch ohne Internet nutzen.
- Änderungen werden später automatisch synchronisiert, wenn du wieder online bist.

BESTE VERWENDUNG FÜR

- Dateien, die du unterwegs brauchst
- Reisen, Flugmodus, Offline-Arbeit
- Wichtige Dokumente und Projekte

BEISPIELE

- OneDrive – Immer auf diesem Gerät behalten
- Google Drive – Offline verfügbar
- Dropbox – Offlinezugriff



MERKE DIR:

Ideal für unterwegs oder offline – Datei ist lokal vorhanden!

SCHELLER VERGLEICH

MODUS	DATEI LOKAL	DATEI ONLINE	SPEICHERPLATZ AUF GERÄT	ZUGRIFF OHNE INTERNET	ÄNDERUNGEN WERDEN SYNCHRONISIERT	BESTE NUTZUNG
Synchronisieren	✓	✓	Hoch ■■■■■	✓ Ja	↻ Sofort	Aktive Arbeit, häufige Nutzung
Nur Online	☁ Nur Platzhalter	✓	Sehr gering ■	✗ Nein	🕒 Beim Öffnen / Online	Selten genutzte Dateien, große Archive
Offline verfügbar	✓ Ja (kopiert)	✓	Mittel bis hoch ■■■■■	✓ Ja	↻ Beim nächsten Online	Untwegs, ohne Internet

WICHTIGE HINWEISE

- Gelöschte Dateien: Wenn du eine Datei löschst, wird sie je nach Dienst auch in der Cloud gelöscht (Papierkorb beachten!).
- Speicherplatz im Blick behalten: Synchronisieren und „Offline verfügbar“ verbrauchen lokalen Speicher.
- Einstellungen prüfen: In OneDrive, Google Drive und Dropbox kannst du je Ordner den Modus festlegen.
- Papierkorb & Versionen: Auch hier unterscheiden sich die Dienste. Informiere dich über Aufbewahrungsfristen.

SO ÄNDERST DU DEN MODUS (BEISPIEL: ONEDRIVE)

- 1 Rechtsklick auf Datei oder Ordner
- 2 „Immer auf diesem Gerät behalten“ = Offline verfügbar
- 3 „Platz sparen und nur online verwenden“ = Nur Online
- 4 Im OneDrive-Einstellungen-Menü unter „Synchronisierung und Backup“ anpassen

TIPP ★

Nutze den für dich passenden Modus je nach Datei und Situation. Du kannst den Modus jederzeit ändern!



DIE RICHTIGE EINSTELLUNG = MEHR KOMFORT & SICHERHEIT

Verstehe, was passiert – und nutze die Cloud genau so, wie du es brauchst!



CLOUD-SPEICHER SPAREN

MEHR PLATZ FÜR DAS, WAS WIRKLICH ZÄHLT.

Dein Cloud-Speicher ist begrenzt.

Mit ein paar einfachen Maßnahmen schaffst du Platz, behältst die Kontrolle über deine Daten und nutzt die Cloud effizienter.



1 PAPIERKORB LEEREN

Gelöschte Dateien bleiben oft noch eine Zeit im Papierkorb und belegen weiter Speicher.



- ✓ Leere den Papierkorb in deiner Cloud regelmäßig.
- ✓ Prüfe auch Papierkörbe in geteilten Ordnern, falls möglich.

TIPP: Gelöschte Dateien werden erst nach dem endgültigen Entfernen wieder gutgeschrieben (frühere Löschung im Papierkorb zählt oft weiterhin als belegt).

2 GROSSE DATEIEN ÜBERPRÜFEN

Wenige große Dateien belegen oft den meisten Platz.



- ✓ Sortiere deine Dateien nach Größe, um Speicherfresser zu finden.
- ✓ Entferne oder archiviere Dateien, die du nicht mehr brauchst.
- ✓ Prüfe besonders große Videos, Projekte, Backups oder alte Installationsdateien.

TIPP: Die meisten Cloud-Dienste bieten eine Ansicht zum Sortieren nach Dateigröße.

3 DOPPELTE DATEIEN LOKAL FINDEN

Duplikate entstehen schnell – zum Beispiel durch mehrfaches Hochladen oder auf verschiedenen Geräten.



- ✓ Suche auf deinem Gerät nach doppelten Dateien und entferne diese mit Bedacht.
- ✓ Prüfe den Inhalt, denn nicht jede gleichnamige Datei ist identisch.
- ✓ Lade anschließend nur die benötigten Dateien in die Cloud.

TIPP: Nutze Tools zur Duplikatsuche auf deinem Gerät. Dubletten nur löschen, wenn du sicher bist, dass sie nicht mehr benötigt werden.

4 FOTOS UND VIDEOS OPTIMIEREN

Fotos und Videos belegen häufig viel Speicher. Mit optimierten Formaten sparst du Platz, ohne deine Originaldateien zu verlieren.



- ✓ Erstelle bei Bedarf optimierte Kopien in effizienteren Formaten (z. B. HEIC, AVIF, H.265).
- ✓ Bewahre deine Originaldateien sicher auf, falls du sie später brauchst.
- ✓ Entferne verwackelte, doppelte oder nicht gelungene Aufnahmen.

TIPP: Qualität anpassen statt einfach löschen – so sparst du Platz und behältst wertvolle Erinnerungen.

5 SELEKTIVE SYNC NUTZEN

Mit selektiver Synchronisation oder „Dateien bei Bedarf“ speicherst du Dateien nur bei Bedarf auf deinem Gerät.



- ✓ Wähle gezielt aus, welche Ordner lokal verfügbar sein sollen.
- ✓ Das spart Speicherplatz auf deinem Gerät (nicht unbedingt in der Cloud).

TIPP: Ideal für große Archive, selten genutzte Dateien oder mehrere Geräte.

6 DATEN AUSSERHALB DER CLOUD ARCHIVIEREN

Nicht alles muss in der Cloud bleiben. Für selten benötigte Daten eignen sich externe Speicher mit Backup.



- ✓ Verschiebe alte oder selten genutzte Dateien auf eine externe Festplatte oder NAS.
- ✓ Erstelle zusätzlich ein Backup.
- ✓ Behalte in der Cloud nur, was du regelmäßig benötigst.

TIPP: Die 3-2-1-Regel beachten: 3 Kopien, auf 2 verschiedenen Medien, davon 1 extern.

7 GETEILTE DATEIEN UND BESITZ PRÜFEN

Geteilte Dateien können auf den Speicherplatz des Besitzers anfallen – je nach Anbieter und Tarif unterschiedlich.



- ✓ Prüfe, welche Dateien du selbst besitzt und welche mit dir geteilt wurden.
- ✓ Bitte den Besitzer, nicht mehr benötigte geteilte Dateien zu entfernen.
- ✓ Kläre, wie geteilte Inhalte bei deinem Anbieter auf den Speicher angerechnet werden.

TIPP: Geteilte Ordner regelmäßig überprüfen und aufräumen.

8 REGELMÄSSIG AUFRÄUMEN

Ein kurzer Check in festen Abständen sorgt dauerhaft für mehr Übersicht.



- ✓ Plane z. B. einmal im Monat einen kurzen Aufräum-Check.
- ✓ Entferne nicht mehr benötigte Dateien und leere Papierkörbe.
- ✓ Behalte deine Ordnerstruktur übersichtlich.

TIPP: Kleine, regelmäßige Schritte sind effektiver und stressfreier als seltene Großaktionen.

ZUSÄTZLICHE TIPPS



- ✓ Aussagekräftige Dateinamen und Ordnerstrukturen verwenden.
- ✓ Alte Projekte, Installationsdateien und unnötige Downloads entfernen.
- ✓ Bei Fotos und Videos regelmäßig aussortieren.
- ✓ Speicherplatz und Einstellungen in deinem Cloud-Konto prüfen.
- ✓ Nur die Daten in der Cloud behalten, die du wirklich brauchst.

DEIN ERGEBNIS

- ✓ Mehr freier Speicherplatz
- ✓ Bessere Übersicht
- ✓ Schnellerer Zugriff auf wichtige Dateien
- ✓ Weniger Kosten durch effiziente Nutzung
- ✓ Mehr Sicherheit und Kontrolle



Mehr Raum für das Wesentliche.



CLEVER SPEICHERN. ENTSPANNTER NUTZEN.

Weniger Ballast. Mehr Möglichkeiten. In der Cloud und auf deinen Geräten.



CLOUD-ORDNUNG

KLAR. STRUKTURIERT. SCHNELL FINDEN.

Eine gute Ordnerstruktur sorgt für Übersicht, spart Zeit und hilft, Fehler zu vermeiden.
So findest du deine Dateien schnell, behältst den Überblick und kannst Zugriffe leichter verwalten
– egal auf welchem Gerät.



ÜBERALL
ORDNUNG.
JEDERZEIT
ZUGRIFF.

DARUM LOHNT SICH ORDNUNG



Schneller finden

Du findest Dateien in Sekunden statt lange zu suchen.



Zeit sparen

Weniger Suchen, mehr erledigen.



Weniger Fehlgriffe

Du vermeidest versehentliches Teilen oder Löschen wichtiger Dateien.



Zugriffe einfacher steuern

Klare Struktur erleichtert es, Berechtigungen zu vergeben und zu prüfen.



Besser zusammenarbeiten

Alle finden sich leichter zurecht – im Team und darüber hinaus.

BEISPIEL: EMPFOHLENE ORDNERSTRUKTUR



02_Team
für geteilte Inhalte:
nur das teilen, was nötig ist.



03_Persönlich
nur für dich. Sensible oder private Dateien hier ablegen.



04_Archiv
Abgeschlossene Projekte und ältere Dateien langfristig aufbewahren.



TIPP: Halte die Struktur einfach und konsistent.
Je klarer die Ordnung, desto schneller findest du, was du suchst.

BEST PRACTICE



Einheitliche Namenskonvention

Verwende klare Namen, z. B.
2024-03-15_Projektname_v1.docx.



Geteilte und private Bereiche trennen

Lege getrennte Ordner für Team-Inhalte und persönliche Dateien an.



Nur ein zentraler Inbox

Alle neuen oder ungeordneten Dateien zuerst hier ablegen und später einsortieren.



Regelmäßig archivieren

Abgeschlossene Projekte in den Archiv-Ordner verschieben.



Regelmäßig aufräumen

Mindestens einmal pro Quartal alte, nicht mehr benötigte Dateien löschen oder archivieren.



Zugriffe regelmäßig prüfen

Mindestens einmal pro Halbjahr überprüfen, wer Zugriff auf geteilte Ordner hat, und unnötige Zugriffe entfernen.



DATEINAMEN – SO GEHT'S RICHTIG



2024-03-15_Rechnung.pdf

Gut: Datum (YYYY-MM-DD) und klarer Name – leicht auffindbar.



2025-01-10_Meeting_Notizen.docx

Gut: Beschreibt den Inhalt verständlich.



Rechnung_final2.pdf

Nicht gut: Unklarer Name und unnötige Versionen.



!!!WICHTIG!!!.docx

Nicht gut: Sonderzeichen und ohne Kontext.



Marketing_2024.zip

Gut: Thema und Jahr im Namen.

ORDNUNG IM ALLTAG – 5 EINFACHE SCHRITTE



1 Dateien in den Inbox legen

Alle neuen Dateien zuerst im 01_Inbox ablegen.



2 Regelmäßig einsortieren

Mind. 1x pro Woche die Inbox leeren und Dateien zuordnen.



3 Archivieren

Abgeschlossene Projekte ins 04_Archiv verschieben.



4 Aufräumen

Mind. 1x pro Quartal alte oder doppelte Dateien entfernen.



5 Zugriffe prüfen

Mind. 1x pro Halbjahr Berechtigungen überprüfen und unnötige Zugriffe entfernen.

SICHERHEIT – DAS MACHT DEINE DATEN WIRKLICH SICHER



- ✓ Zugriffsrechte: Nur berechtigte Personen haben Zugriff.
- ✓ Verschlüsselung: Schützt deine Daten vor unbefugtem Zugriff.
- ✓ Regelmäßige Backups: Sichern deine Daten bei Verlust oder technischen Problemen.



Wichtig: Eine gute Ordnerstruktur hilft dir beim Finden, vermeidet Fehlgriffe und erleichtert die Zugriffsverwaltung. Für echte Sicherheit sorgen Berechtigungen, Verschlüsselung und Backups.

EXTRA-TIPPS

- ✓ Vorlagen für wiederkehrende Dateien nutzen (z. B. Angebote, Protokolle).
- ✓ Klare Projekt- oder Kundennamen verwenden.
- ✓ Nicht die gesamte Ordnerstruktur zu tief verschachteln (max. 3–4 Ebenen).
- ✓ Zusammen mit dem Team gemeinsame Regeln festlegen.
- ✓ Auch auf mobilen Geräten die gleiche Struktur verwenden.



FAZIT



Mehr Überblick. Weniger Stress. Mehr Zeit für das Wesentliche.
Mit einer klaren Cloud-Ordnung findest du deine Dateien schneller, vermeidest Fehler und kannst sicher und effizient zusammenarbeiten – auf jedem Gerät und von überall.

CLOUD UMZIEHEN

PLATTFORM WECHSELN – SICHER UND STRESSFREI!

Google Drive OneDrive

Dropbox → Proton Drive

Deine Daten. Deine Kontrolle. Sicher umziehen.



WARUM UMZIEHEN?

- Mehr Datenschutz und Kontrolle
- Kosten sparen oder bessere Angebote nutzen
- Mehr Unabhängigkeit von einem Anbieter
- Bessere Integration in deine Arbeitsumgebung
- Deine Daten so nutzen, wie es zu dir passt

SO GEHT'S – IN 8 SCHRITTEN



TIPP: Nimm dir Zeit, arbeite Schritt für Schritt und halte wichtige Zwischenergebnisse fest.

CHECKLISTE: SICHER UMZIEHEN

- ☒ **1. Datenbestand erfassen**
Welche Konten, Ordner, Dateien und Freigaben gibt es? Speicherplatz und Limits im Ziel prüfen.
- ☒ **2. Backup erstellen**
Vor dem Umzug ein lokales oder unabhängiges Backup anlegen.
- ☒ **3. Metadaten erhalten**
Wenn möglich: Ordnerstruktur, Dateinamen, Zeitstempel, Berechtigungen und andere Metadaten beibehalten.
- ☒ **4. Testlauf durchführen**
Eine kleine, repräsentative Auswahl an Daten übertragen und Funktionen testen (Öffnen, Freigaben, Apps).
- ☒ **5. Vollständige Übertragung**
Alle Daten in den neuen Cloud-Dienst migrieren.
- ☒ **6. Ergebnis vergleichen**
Dateianzahl und Gesamtgröße prüfen.
Bei wichtigen Daten Prüfsummen (z. B. SHA256) verwenden.
- ☒ **7. Freigaben und Verknüpfungen prüfen**
Geteilte Ordner, Berechtigungen und Verknüpfungen in Apps und Geräten wiederherstellen.
- ☒ **8. Eine Zeit lang prüfen**
Alte Daten vorerst behalten und alles in Ruhe testen.
- ☒ **9. Alte Integrationen widerrufen**
Wenn alles passt: alte Daten löschen und verbundene Apps, Zugriffe und Integrationen beim alten Anbieter entfernen.



TOOLS: HILFE BEIM UMZUG



Du kannst Dateien manuell übertragen oder offizielle Import- und Migrationsfunktionen der Anbieter nutzen. Es gibt auch Drittanbieter-Tools – wähle nur seriöse und vertrauenswürdige Lösungen.



ACHTUNG: DRITTANBIETER-TOOLS



Migrationstools von Drittanbietern können umfangreichen Zugriff auf dein Konto erhalten, z. B. auf alle Dateien, Ordner und Metadaten.

- ☒ Nur vertrauenswürdige und bekannte Anbieter nutzen
- ☒ Nur die minimal nötigen Berechtigungen gewähren
- ☒ Sichere Verbindung (HTTPS) und gute Bewertungen prüfen
- ☒ Zugriff nach dem Umzug wieder widerrufen
- ☒ Keine sensiblen Daten an unbekannte Dienste geben
- ☒ Es gibt keine Garantie für einen fehlerfreien oder vollständigen Umzug



BEST PRACTICE

- ☒ Ruhe bewahren und Schritt für Schritt vorgehen
- ☒ Wichtige Daten zusätzlich lokal sichern
- ☒ Testlauf mit realen Dateien durchführen
- ☒ Prüfsummen für wichtige Daten verwenden
- ☒ Freigaben und Berechtigungen sorgfältig prüfen
- ☒ Alte Integrationen nach dem Umzug widerrufen
- ☒ Regelmäßige Backups auch nach dem Umzug beibehalten



FAZIT: GUT GEPLANT IST HALB MIGRIERT!

Ein sorgfältiger Umzug spart Zeit, Nerven und schützt deine Daten. Mit Backup, Tests und Kontrolle gelingt der Wechsel sicher und entspannt.



Lieber einmal richtig – als später Daten verlieren!

EMPFOHLENE TOOLS IM ÜBERBLICK (AUS WAHL, KEINE GARANTIE)



rclone
Kommandozeilen-Tool für viele Cloud-Dienste. Flexibel und leistungsfähig.



MultCloud
Webbasierte Plattform zum Übertragen zwischen Cloud-Diensten.



CloudHQ
Einfache Migration zwischen Clouds – inkl. Planung und Automatisierung.



RaiDrive
Cloud-Speicher als Laufwerk einbinden und Dateien einfach verschieben.



Offizielle Tools
Import- und Migrationsfunktionen der Anbieter nutzen (z. B. Google, Microsoft, Proton).

CLOUD UND DATENSCHUTZ

DEINE DATEN. DEIN RECHT. DEINE VERANTWORTUNG.



Cloud-Dienste bieten Komfort und viele Möglichkeiten. Gleichzeitig ist der Schutz deiner Daten eine gemeinsame Aufgabe – von Anbietern, Staaten und dir.

1 WO LIEGEN DEINE DATEN?

Der Speicherort beeinflusst Datenschutz, Vertragsregeln und mögliche Behördenzugriffe. Entscheidend sind zusätzlich Anbieter, Verschlüsselung und Kontoeinstellungen.



EU/EWR DSGVO gilt



Daten unterliegen der Datenschutz-Grundverordnung (DSGVO).



Zugriffe von Behörden nur auf gesetzlicher Grundlage und nach den Regeln der EU/EWR.



Guter Schutz durch ein hohes datenschutzrechtliches Niveau.



SCHWEIZ

Schweizer DSG, bei EU-Angeboten zusätzlich DSGVO möglich



Daten unterliegen dem Schweizer Datenschutzgesetz (DSG).



Zugriffe von Behörden nur auf gesetzlicher Grundlage.



Bei Anbietern mit Sitz in der EU oder Verarbeitung in der EU kann zusätzlich die DSGVO gelten.



USA/US-ANBIETER

US-Recht kann unter gesetzlichen Voraussetzungen auch Daten im Ausland erfassen.



US-Behörden können bei US-Anbietern unter bestimmten gesetzlichen Voraussetzungen auf Daten zugreifen (z. B. nach dem CLOUD Act).



Dies kann auch Daten betreffen, die außerhalb der USA gespeichert sind, sofern sie der Kontrolle des Anbieters unterliegen.



Zusätzliche Schutzmaßnahmen (z. B. Verschlüsselung, Standort, Vertragsregeln) sind wichtig.

2 WER KANN AUF DATEN ZUGREIFEN?



Cloud-Anbieter

Kann auf deine Daten zugreifen, wenn keine kundenseitige Ende-zu-Ende-Verschlüsselung verwendet wird (z. B. zur Bereitstellung, Wartung und Missbrauchsabwehr).



Berechtigte Kontonutzer

Personen, denen du Zugriff gewährst (z. B. über gemeinsame Ordner oder geteilte Konten).



Kompromittierte Konten oder Geräte

Bei gestohlenen Zugangsdaten oder infizierten Geräten können Angreifer auf deine Daten zugreifen.



Behörden

Zugriff nur auf gesetzlicher Grundlage, z. B. durch gerichtliche Anordnung – je nach anwendbarem Recht und Zuständigkeit des Anbieters.



Insider

Mitarbeiter des Anbieters können unter Wahrung interner Kontrollen auf Daten zugreifen. Dies ist ein Restrisiko, das sich durch Verschlüsselung und geeignete Anbieterwahl reduzieren lässt.

3 CLOUD ACT – RICHTIG EINGEORDNET



Der **CLOUD Act erlaubt keinen beliebigen Zugriff**. US-Anbieter können jedoch durch rechtmäßige Anordnungen zur Herausgabe von Daten verpflichtet werden, die ihrer Kontrolle unterliegen – auch wenn sie außerhalb der USA gespeichert sind. Konflikte mit ausländischem Recht können geprüft werden.

4 WANN HilFT ENDE-ZU-ENDE-VERSCHLÜSSELUNG?



- ✓ Nur deine Geräte besitzen die Schlüssel.
- ✓ Der Anbieter kann Dateiinhalte nicht entschlüsseln.
- ✓ Metadaten, Freigaben und kompromittierte Endgeräte bleiben mögliche Risiken.

5 BEST PRACTICE – SO SCHÜTZT DU DEINE DATEN



EU/Schweizer Standort wählen

Prüfe den Speicherort deiner Daten und die Vertragsbedingungen des Anbieters.



Ende-zu-Ende-Verschlüsselung

Nutze, wenn möglich, E2EE oder ergänzend eine starke lokale Verschlüsselung.



Starke Authentifizierung

Aktiviere Zwei-Faktor-Authentifizierung (2FA) oder Passkeys.



Freigaben minimieren

Teile Daten nur mit wenigen, vertrauenswürdigen Personen und überprüfe regelmäßig Berechtigungen.



Backups erstellen

Lege regelmäßige Backups an – idealerweise getrennt vom Cloud-Anbieter (z. B. lokal oder bei einem separaten Dienst).



Rechtliches prüfen

Lies die Datenschutzerklärung und prüfe die Auftragsverarbeitung (Art. 28 DSGVO bzw. entsprechende Regelungen in der Schweiz).



SPEICHERORT IST WICHTIG. SCHLÜSSELKONTROLLE IST ENTSCHEIDEND.

Informiert entscheiden. Verantwortungsvoll handeln. Sicher in der Cloud.



DIE GRÖSSTEN CLOUD-FEHLER

Kleine Fehler. Große Folgen.

Vermeide diese typischen Fehler – und halte deine Daten sicher, privat und wiederherstellbar.



1 ALLES IN EINEM ORDNER



Unstrukturierte Ablage führt zu Chaos. Du findest wichtige Dateien schwer, verpasst den Überblick und die Wiederherstellung wird aufwendig.

Besser so:
Nutze eine klare Ordnerstruktur (z. B. Dokumente, Finanzen, Fotos, Projekte ...) und Unterordner.

WARUM RISKANT? ⚠️

Keine Übersicht, Fehler beim Löschen oder Überschreiben und schwierige Wiederherstellung.

6 PASSWORT MEHRFACH VERWENDET



Ein kompromittiertes Passwort öffnet Angreifern die Tür zu mehreren Konten – inklusive deiner Cloud.

Besser so:
Verwende für jeden Dienst ein einzigartiges, starkes Passwort mit einem Passwort-Manager.

WARUM RISKANT? ⚠️

Ein Leak bei einem Dienst gefährdet alle anderen Konten.

2 KEIN BACKUP



Cloud ist kein Backup! Löschst du etwas versehentlich oder wird dein Konto gesperrt, kann alles verloren sein.

Besser so:
Nutze die 3-2-1-Regel: 3 Kopien • 2 verschiedene Medien • 1 Kopie außer Haus (z. B. zweite Cloud).

WARUM RISKANT? ⚠️

Gelöschte Dateien, gehackte Konten oder Anbieterprobleme können zu dauerhaftem Datenverlust führen.

7 ALTE FREIGABEN VERGESSEN



Freigegebene Links und Ordner bleiben oft aktiv – auch wenn sie längst nicht mehr gebraucht werden.

Besser so:
Überprüfe regelmäßig alle Freigaben und entferne Zugriffe, die nicht mehr benötigt werden.

WARUM RISKANT? ⚠️

Unbekannte Dritte können weiterhin Zugriff auf deine Daten haben.

3 KEINE 2FA (ZWEI-FAKTOR-AUTHENTIFIZIERUNG)



Nur mit Benutzername und Passwort kann jeder, der dein Passwort kennt, auf deine Cloud zugreifen.

Besser so:
Nutze nach Möglichkeit Passkeys oder phishing-resistente Sicherheitsschlüssel. Falls nicht verfügbar, verwende eine Authenticator-App.

WARUM RISKANT? ⚠️

Passwörter können gestohlen, geraten oder durch Phishing erbeutet werden.

8 NIEMAND KENNT DEN RECOVERY-CODE



Ohne Wiederherstellungscodes oder Zweitgerät kann ein verlorener Zugang dauerhaft gesperrt sein.

Besser so:
Recovery-Codes sicher speichern (offline, z. B. in einem Passwort-Manager oder Safe).

WARUM RISKANT? ⚠️

Kein Zugang mehr zu deinen Daten – für immer.

4 ÖFFENTLICH FREIGELEGEBENE LINKS



Öffentliche Links können von jedem gefunden und weiterverbreitet werden – ohne dein Wissen.

Besser so:
Links nur gezielt teilen, Zugriffsmöglichkeiten einschränken und – je nach Anbieter – Passwort- und Ablaufoptionen nutzen. Benannte Empfänger sind oft sicherer als öffentliche Links.

WARUM RISKANT? ⚠️

Vertrauliche Daten können öffentlich zugänglich werden.

9 UNGEPÜFTE DRITTANBIETER-APPS



Verbundene Apps können weitreichenden Zugriff auf deine Cloud-Dateien erhalten.

Besser so:
Prüfe verbundene Apps regelmäßig und entferne nicht mehr benötigte Zugriffe.

WARUM RISKANT? ⚠️

Alte oder unseriöse Apps können Daten lesen, verändern oder löschen.

5 SENSIBLE DATEN OHNE EIGENE VERSCHLÜSSELUNG



Deine Daten liegen unverschlüsselt auf den Servern des Anbieters – auch wenn sie während der Übertragung und auf den Servern verschlüsselt sind.

Besser so:
Für besonders sensible Daten zusätzlich eine Ende-zu-Ende-Verschlüsselung auf deiner Seite nutzen, z. B. mit Cryptomator, VeraCrypt oder im Client integrierter E2EE.

WARUM RISKANT? ⚠️

Der Anbieter (oder gesetzliche Stellen) kann auf deine Daten zugreifen.

10 KEINE VERSIONSKONTROLLE



Ohne Versionsverlauf können gelöschte oder überschriebene Dateien nicht wiederhergestellt werden.

Besser so:
Versionsverlauf aktivieren und regelmäßig prüfen. Wichtige Dateien zusätzlich sichern (separates Backup).

WARUM RISKANT? ⚠️

Die Aufbewahrungsdauer des Versionsverlaufs ist je nach Anbieter begrenzt – und kein echtes Backup.



SO SCHÜTZT DU DEINE CLOUD RICHTIG

- ✓ Klare Struktur & Benennung
- ✓ Regelmäßige Backups
- ✓ 2FA mit starken Methoden
- ✓ Starke, einzigartige Passwörter
- ✓ Freigaben kontrollieren
- ✓ Verschlüsselung nutzen
- ✓ Recovery-Codes sicher aufbewahren
- ✓ Versionierung aktivieren



MERKE DIR:

Die Cloud ist praktisch – aber nur sicher, wenn du die richtigen Regeln beachtest!



DEINE DATEN. DEINE VERANTWORTUNG. SICHERHEIT BEGINNT BEI DIR.

CLOUD + NAS

CLOUD ODER NAS? ODER WARUM VIELE BEIDES NUTZEN.

Die Cloud ist praktisch. Ein NAS ist dein eigener Speicher – sicher wird es erst durch gute Konfiguration und Backups.



CLOUD

Speicher in Rechenzentren im Internet



- ✓ Zugriff von überall mit Internetverbindung
- ✓ Keine Hardware, keine Wartung
- ✓ Skalierbar mit wenigen Klicks
- ✓ Ideal zum Teilen und Zusammenarbeiten
- ✓ Automatische Backups (optional)

VS.

NAS (NETWORK ATTACHED STORAGE)

Dein eigener Speicher zu Hause oder im Büro



- ✓ Vollständige Kontrolle über deine Daten
- ✓ Einmalige Anschaffung, keine laufenden Kosten
- ✓ Schnelle Zugriffe im lokalen Netzwerk
- ✓ Keine Abhängigkeit vom Internet
- ✓ Erweiterbar und individuell anpassbar

VERGLEICH: CLOUD vs. NAS

KRITERIUM	CLOUD	NAS	GEWINNER
ZUGRIFF VON ÜBERALL	✓ Ja, immer und überall (mit Internet)	⚠ Nur mit Einrichtung (via DDNS / VPN)	CLOUD
DATENSICHERHEIT	✓ Professionell betrieben, aber Anbieter- und Kontorisiken.	⚠ Volle Verantwortung; Sicherheit hängt von Einrichtung, Updates und Backups ab.	KOMMT DARAUF AN
LAUFENDE KOSTEN	✗ Monatliche / jährliche Gebühren	✓ Strom, Festplatten, Ersatzteile und eventuell Zusatzdienste	NAS
EINRICHTUNG	✓ Sehr einfach (Account erstellen, loslegen)	⚠ Einrichtung & Wartung erforderlich	CLOUD
SPEICHER ERWEITERN	✓ Einfach online erweitern	⚠ Festplatten kaufen und einbauen	CLOUD
GESCHWINDIGKEIT IM LAN	⚠ Abhängig vom Internet	✓ Sehr schnell im lokalen Netzwerk	NAS
DATEN TEILEN	✓ Sehr einfach per Link	⚠ Einrichtung von Freigaben oder VPN nötig	CLOUD
UNABHÄNGIGKEIT	✗ Abhängig vom Anbieter, Preisen und Richtlinien	⚠ Abhängig von deiner Hardware und deiner Einrichtung	KOMMT DARAUF AN
AUSFALLRISIKO	⚠ Ausfälle oder Sperrungen beim Anbieter möglich	⚠ Hardware-Defekt, Diebstahl, Stromausfall möglich	UNENTSCHEIDEN

WARUM VIELE BEIDES NUTZEN (DAS BESTE AUS ZWEI WELTEN)

NAS

Zentrale Speicherung und Verwaltung aller wichtigen Daten bei dir zu Hause.



SEPARATER CLOUD-BACKUP-JOB – versioniert, geschützt und getrennt von der normalen Synchronisation.

- ✓ Schneller Zugriff im Alltag über das NAS
- ✓ Wichtige Daten zusätzlich in der Cloud sichern
- ✓ Von überall auf die wichtigen Daten zugreifen
- ✓ Schutz vor Hardware-Defekt, Brand, Diebstahl

CLOUD

Zusätzlicher, offsite Speicher für deine wichtigsten Daten als Backup.



TYPISCHE NUTZUNG

- Fotos & Videos: Auf NAS speichern, Cloud als Backup und fürs Teilen.
- Dokumente: Lokal arbeiten, in der Cloud synchronisieren.
- Backups: NAS → Cloud (automatisiert & verschlüsselt).
- Unterwegs: Wichtige Dateien jederzeit aus der Cloud abrufen.

BELIEBTE NAS-HERSTELLER

Synology **QNAP**

- ✓ Viele Funktionen (Backups, VPN, Virtualisierung, Multimedia u. v. m.)
- ✓ Einfache Bedienung
- ✓ Große Community & Apps



WICHTIG BEI NAS

- RAID nutzen (z. B. RAID 1/5/10) – schützt vor Festplattenausfall, aber nicht vor allem!
- Regelmäßig Backups erstellen – auch in die Cloud.
- Automatische Updates aktivieren.
- Starke Admin-Zugang & 2FA nutzen.
- Bei Fernzugriff immer VPN oder sichere Dienste (z. B. Synology QuickConnect mit 2FA).

EMPFOHLENE CLOUDS (als Ergänzung)

Proton Drive pCloud Microsoft OneDrive Google Drive

- ✓ Ende-zu-Ende-Verschlüsselung (z. B. Proton Drive)
- ✓ Datenschutzfreundliche Anbieter wählen
- ✓ Tools wie Cryptomator oder VeraCrypt nutzen (siehe nächstes Kapitel!)



FAZIT: CLOUD UND NAS KÖNNEN SICH ERGÄNZEN – WENN SYNCHRONISATION UND BACKUP KLAR GETRENNT SIND.
Deine Daten. Deine Kontrolle. Deine Freiheit.



SICHERHEITSHINWEIS

Selbst ein NAS schützt deine Daten nicht vor Brand, Diebstahl oder Naturkatastrophen.
Deshalb: 3-2-1-Regel beachten → 3 Kopien, 2 verschiedene Medien, 1 Kopie außer Haus (z. B. in der Cloud).

CLOUD + SMARTPHONE

AUTOMATISCHER UPLOAD – FOTOS & VIDEOS SICHER NUTZEN.

Komfortabel, gut organisiert – und mit den richtigen Einstellungen wirklich sicher.



1 AUTOMATISCHER UPLOAD – SO FUNKTIONIERT'S



1. Aufnahme
Du machst ein Foto oder Video.



2. Verbindung
Dein Smartphone verbindet sich mit WLAN oder Mobilfunk.



3. Upload
Die Datei wird automatisch in die Cloud hochgeladen.



4. Verfügbar
Deine Fotos & Videos sind auf all deinen Geräten verfügbar.

Hinweis: Der Upload spart dir Zeit und ist bequem – ersetze aber kein zusätzliches Backup.

2 WAS WIRD HOCHGELADEN?



FOTOS

Neue Fotos werden automatisch in die Cloud gesichert (je nach Einstellung).



VIDEOS

Auch Videos werden – je nach Einstellung – automatisch hochgeladen.



3 DAS BRINGT DIR DAS



Komfort & Übersicht

Deine Fotos und Videos werden automatisch gesichert und sind auf allen Geräten verfügbar.



Schutz bei Geräteverlust

Auch wenn dein Smartphone verloren geht, sind deine Aufnahmen in der Cloud.



Bessere Organisation

Nach Datum, Ort oder Personen sortiert – so findest du deine Erinnerungen schnell.



Mehr Speicherplatz

Dein Smartphone bleibt frei, weil die Dateien in der Cloud liegen.



Einfaches Teilen

Links teilen, Alben freigeben – mit Familie und Freunden.



Automatische Highlights

Viele Dienste erstellen automatisch Rückblicke, Alben und Collagen.



4 WICHTIGE HINWEISE



Kein eigenständiges Backup

Der automatische Upload ist keine Garantie für ein Backup. Gelöschte Dateien oder ein verlorener Account können sich – je nach Dienst und Einstellungen – auch in der Cloud auswirken.



Abhängigkeit vom Konto

Kein Zugriff ohne Account. Verlust oder Sperrung kann zum Verlust deiner Daten führen.



Eingeschränkter Offline-Zugriff

Ohne Internet sind nicht alle Dateien verfügbar. Wichtige Inhalte zusätzlich offline speichern.



Verbrauch von mobilen Daten

Uploads können viel Datenvolumen kosten. Entsprechend die Einstellungen nutzen (z. B. nur WLAN, Roaming pausieren).



Datenschutz beachten

Deine Fotos sind bei einem Anbieter gespeichert. Prüfe die Datenschutzeinstellungen und teile nur, was du wirklich teilen möchtest.



5 EMPFOHLENE EINSTELLUNGEN FÜR MEHR SICHERHEIT



Bildschirm sperren

- ✓ PIN, Passwort, oder biometrisch (Fingerabdruck / Face ID)
- ✓ Automatische Sperre aktivieren



Aktuell bleiben

- ✓ Betriebssystem und Apps regelmäßig aktualisieren
- ✓ Sicherheitsupdates zeitnah installieren



Zwei-Faktor-Authentifizierung

- ✓ 2FA oder Passkeys verwenden
- ✓ Wiederherstellungscodes sicher aufbewahren



Bei Verlust

- ✓ Funktion zum Auffinden und Löschen aktivieren (z. B. „Mein Gerät finden“)
- ✓ Gerät aus der Ferne sperren oder löschen



Netzwerke bewusst nutzen

- ✓ Sensible Aktivitäten nicht in unsicheren, öffentlichen Netzwerken
- ✓ VPN nur bei Bedarf einsetzen (z. B. im Ausland oder bei untrusted networks)



Zusätzliches Backup

- ✓ Regelmäßig ein unabhängiges Backup erstellen (z. B. externe Festplatte oder NAS)
- ✓ So sind deine Fotos auch dann sicher, wenn etwas mit dem Konto passiert.



EXTRA-TIPP: OFFLINE-ZUGRIFF

Lade wichtige Fotos und Dokumente für unterwegs auf dein Gerät, damit du sie auch ohne Internet sehen kannst (z. B. Reisen, Flugmodus).



DEINE DATEN – DEINE ENTSCHEIDUNG

Prüfe regelmäßig die Datenschutzeinstellungen deines Cloud-Dienstes und entscheide bewusst, welche Inhalte gesichert und geteilt werden.



FAZIT

Automatischer Upload ist komfortabel und sicher – mit den richtigen Einstellungen, einem zusätzlichen Backup und einem bewussten Umgang mit deinen Daten.

MEHR KOMFORT. MEHR SICHERHEIT. MEHR ERINNERUNGEN FÜR IMMER.



CLOUD + WINDOWS & macOS

DEINE DATEIEN. DEINE GERÄTE. ÜBERALL SYNCHRON.

Die Cloud verbindet deine Computer, Smartphones und Tablets mit deinen Dateien – sicher, automatisch und plattformübergreifend verfügbar.



1 WIE FUNKTIONIERT DIE SYNCHRONISATION?

Du installierst einen Cloud-Sync-Client auf deinem Gerät. Dieser synchronisiert ausgewählte Ordner automatisch mit der Cloud.



DESKTOP

Zugriff auf Dateien auf all deinen Geräten.



DOKUMENTE

Texte, Tabellen, PDFs und andere wichtige Dateien synchron halten.



BILDER

Fotos, Videos und kreative Dateien überall verfügbar.



DOWNLOADS

Dateien automatisch in der Cloud synchronisieren (z. B. Installationsdateien).

2 ZUGRIFF AUF DEINE DATEIEN

Je nach Cloud-Dienst stehen dir mehrere Möglichkeiten zur Verfügung:



Sync-Client (Desktop-App)

Synchronisiert Ordner automatisch im Hintergrund auf Windows und macOS.



Dateien bei Bedarf (Files-on-Demand)

Du siehst alle Dateien im Explorer (Windows) oder Finder (macOS). Nur bei Bedarf werden sie auf das Gerät heruntergeladen.



Browser-Zugriff

Greife über den Webbrowser von jedem Gerät aus auf deine Dateien zu.



Die verfügbaren Funktionen können je nach Cloud-Anbieter, Betriebssystem und Gerät unterschiedlich sein.

3 TYPISCHE STANDARDORDNER

WINDOWS



Desktop

C:\Users\DeinName\Desktop



Dokumente

C:\Users\DeinName\Documents



Bilder

C:\Users\DeinName\Pictures



Downloads

C:\Users\DeinName\Downloads



macOS



Schreibtisch

/Users/deinname/Desktop



Dokumente

/Users/deinname/Documents



Bilder

/Users/deinname/Pictures



Downloads

/Users/deinname/Downloads



Du kannst in der Cloud auch eigene Ordner auswählen und zwischen Geräten synchronisieren.

4 DATEIEN BEI BEDARF (FILES-ON-DEMAND)



Nur online (platzsparend)



Wird bei Bedarf heruntergeladen



Lokal verfügbar

- ✓ Spart lokalen Speicherplatz auf deinem Gerät.
- ✓ Die Datei wird erst bei Bedarf heruntergeladen.
- ✓ Der Cloud-Speicherplatz (Kontingent) wird trotzdem genutzt.
- ✓ Kein Ersatz für eine separate Datensicherung (kein Backup).



Wichtig: Dateien bei Bedarf sparen nur Speicherplatz auf deinem Gerät, nicht in der Cloud. Sie sind kein eigenständiges Backup.

5 EMPFOHLENE EINSTELLUNGEN FÜR EINE SICHERE UND EFFIZIENTE NUTZUNG



NUR WICHTIGE ORDNER

Synchronisiere nur die Ordner, die du wirklich benötigst (selektive Sync einrichten).



SYNC-STATUS PRÜFEN

Kontrolliere regelmäßig, ob alle Dateien korrekt synchronisiert sind.



SEPARATES BACKUP

Nutze zusätzlich ein separates Backup (z. B. externe Festplatte) für wichtige Daten.



SYSTEM & APPS AKTUALISIEREN

Halte Windows, macOS und die Cloud-App immer auf dem neuesten Stand.



GERÄT VERSCHLÜSSELN

Verwende die integrierte Geräteverschlüsselung (z. B. BitLocker, FileVault).



SICHER ANMELDEN

Nutze ein starkes Passwort und wenn möglich die Zwei-Faktor-Authentifizierung (2FA).

6 GETEILTE ORDNER & FREIGABEN



- ✓ Gehe sorgfältig mit geteilten Ordnern um.
- ✓ Teile nur mit vertrauenswürdigen Personen.
- ✓ Überprüfe regelmäßig, wer Zugriff hat.
- ✓ Beachte, dass geteilte Dateien auf Geräten anderer Personen gespeichert werden können.

7 WICHTIGE HINWEISE



- ✓ Funktionen und Bezeichnungen unterscheiden sich je nach Cloud-Dienst und Betriebssystem.
- ✓ Kein Cloud-Dienst ist von vornherein sicherer als ein anderer – Sicherheit hängt von den Einstellungen und der Nutzung ab.
- ✓ Informiere dich über die Datenschutzrichtlinien deines Anbieters.
- ✓ Nutze die Cloud bewusst und halte sensible Daten besonders geschützt.



RICHTIG EINGERICHTET, MACHT DIE CLOUD DEINEN ALLTAG EINFACHER – AUF ALLEN DEINEN GERÄTEN.
FLEXIBEL. SICHER. PLATTFORMÜBERGREIFEND.

CLOUD + KI

SMARTER ARBEITEN. DATEN BEWUSST SCHÜTZEN.

Künstliche Intelligenz ist in vielen Cloud-Diensten integriert. Sie kann dir helfen – aber nur, wenn du weißt, welche Daten verarbeitet werden und wie du die Kontrolle behältst.



1 WO KI IN CLOUD-DIENSTEN BEGEGNET

KI-Funktionen sind heute an vielen Stellen integriert, zum Beispiel:



Suche

KI-gestützte Suche findet Informationen schneller und versteht auch natürliche Sprache.



Zusammenfassungen

Lange Inhalte werden automatisch in kurzen, verständlichen Zusammenfassungen dargestellt.



Schreibunterstützung

KI hilft beim Formulieren, Korrigieren, Übersetzen und Umformulieren von Texten.



Bildererkennung

Bilder und Grafiken können analysiert und beschrieben werden, z. B. Inhalte, Objekte oder Text in Bildern.



Dokumentenanalyse

KI kann Inhalte aus verschiedenen Dateiformaten lesen, strukturieren und relevante Informationen extrahieren.



Automatisierung

Wiederkehrende Aufgaben können mit KI-Unterstützung automatisiert werden, z. B. sortieren, kategorisieren oder Antworten vorschlagen.

2 WELCHE DATEN KÖNNEN VERARBEITET WERDEN?

Je nach Anbieter, Tarif, Funktion und deinen Einstellungen können unter anderem folgende Daten verarbeitet werden:



Eingaben und Anfragen (Prompts)

Was du in die KI eingibst.



Hochgeladene Dateien

Dokumente, Bilder, Tabellen, Präsentationen u. a.



Inhalte von Dokumenten

Texte, Tabellen, Bilder und weitere enthaltene Informationen.



Metadaten

z. B. Dateiname, Dateityp, Erstellungsdatum, Autor, Kommentare oder Tags.



Nutzungsdaten

z. B. wie Funktionen genutzt werden, Feedback oder Protokolldaten.



Der genaue Umfang der Datenverarbeitung hängt vom Anbieter, dem gewählten Tarif, der jeweiligen Funktion und deinen Einstellungen ab.

3 DREI FRAGEN VOR DER NUTZUNG

Bevor du eine KI-Funktion verwendest, kläre für dich:



Ist die KI-Funktion aktiv?

Verstehe, ob und in welchem Umfang die Funktion gerade genutzt wird.



Wo und wie lange werden Daten verarbeitet oder gespeichert?

Informiere dich, in welchen Rechenzentren deine Daten verarbeitet werden und wie lange sie gespeichert bleiben.



Werden meine Inhalte zur Verbesserung der KI-Modelle verwendet?

Prüfe, ob deine Eingaben und Dateien für das Training von Modellen genutzt werden.



Die Antworten auf diese Fragen findest du in den aktuellen Datenschutz- und Hilfeseiten des jeweiligen Anbieters. Die Informationen können sich ändern – prüfe sie daher regelmäßig.

4 SENSIBLE DATEN – LIEBER NICHT HOCHLADEN

Lade keine sensiblen oder vertraulichen Informationen in KI-Dienste hoch, insbesondere:



Passwörter und Zugangsdaten



Wiederherstellungs-codes (Recovery Codes)



Private Schlüssel (z. B. API-Keys)



Gesundheitsdaten und medizinische Unterlagen



Ausweisdokumente (z. B. Personalausweis, Reisepass)



Vertrauliche Verträge und Geschäftsunterlagen



Personenbezogene Daten von Dritten (nur mit ausdrücklicher Erlaubnis und ausreichendem Schutz)

5 EINSTELLUNGEN RICHTIG PRÜFEN

Nutze die aktuellen Datenschutz- und Hilfeseiten deines Anbieters. Menüs und Optionen können sich ändern. Achte insbesondere auf folgende Punkte:



Verlauf und Speicher

Wie lange werden deine Daten gespeichert und kannst du sie löschen?



Modell-Training

Ob und wie deine Inhalte zur Verbesserung der Modelle genutzt werden.



Verbundene Apps

Welche zusätzlichen Dienste oder Apps Zugriff haben.



Teilen und Freigaben

Mit wem Inhalte geteilt werden, z. B. im Team oder in Organisationen.



Verwende immer die aktuellen Informationen des Anbieters – diese sind zuverlässiger als allgemeine Anleitungen.

6 VERSCHLÜSSELUNG HAT EINE GRENZE

Wenn eine KI Inhalte lesen und verarbeiten soll, müssen diese in der Regel entschlüsselt werden. Während der Verarbeitung liegen die Daten in einer für die KI lesbaren Form vor.



Daten werden für die Verarbeitung entschlüsselt, damit die KI sie analysieren kann.



Dateien, die bereits clientseitig (lokal) verschlüsselt sind, können nicht analysiert werden – es sei denn, du gibst bewusst Zugang (z. B. durch Entschlüsselung oder Upload der entschlüsselten Version).

7 BEWÄHRTE PRAKTIKEN FÜR DIE NUTZUNG VON KI IN DER CLOUD



Daten minimieren

Teile nur die Daten, die wirklich nötig sind.



Anonymisieren

Entferne oder verallgemeinere personenbezogene Informationen.



Zugriff kontrollieren

Nutze getrennte Konten und verlege nur die notwendigen Rechte.



Arbeit und Privat trennen

Nutze separate Konten für berufliche und private Zwecke.



Ergebnisse prüfen

Verifiziere KI-Ergebnisse und prüfe wichtige Informationen auf Richtigkeit.



Lokale/offline Option

Nutze, wenn möglich, lokale oder Offline-Optionen für besonders sensible Inhalte.



Backups erstellen

Bewahre wichtige Daten zusätzlich auf – unabhängig vom KI-Dienst.



KI IST EIN WERKZEUG. DU ENTSCHEIDEST, WELCHE DATEN ES SEHEN DARF.

CLOUD + FAMILIENFREIGABE

GEMEINSAM NUTZEN. GEMEINSAM SPAREN. GEMEINSAM SICHER.

Apple, Google, Microsoft und Dropbox bieten Familienkonten an. Damit teilst du Speicher, Dienste und Vorteile – einfach, sicher und übersichtlich.



Apple Familienfreigabe



- ✓ Familiengruppe mit bis zu 6 Personen (Organisator + 5)
- ✓ iCloud+ Speicher kann – je nach aktuellem Tarif – mit der Familie geteilt werden
- ✓ Geteilte Käufe und Abos, sofern vom Anbieter in Familienfreigabe unterstützt (Apps, Musik, Filme, TV)
- ✓ Familienalbum, geteilte Kalender, Standortfreigabe und Bildschirmsperre
- ✓ Zentrale Verwaltung mit Kindersicherung

Bis zu 6 Familienmitglieder (Organisator + 5 weitere)

Google Google Familiengruppe



- ✓ Familiengruppe mit bis zu 6 Personen (Organisator + 5)
- ✓ Google One Speicher kann geteilt werden (je nach aktuellem Tarif)
- ✓ Bestimmte Google-Dienste und berechtigte Abos können geteilt werden (z. B. YouTube Premium)
- ✓ Persönliche Dateien bleiben privat und sind nur sichtbar, wenn du sie ausdrücklich teilst
- ✓ Gemeinsame Familienfunktionen wie Family Link, Kalender und Einkäufe im Play Store

Bis zu 6 Familienmitglieder (Organisator + 5 weitere)

Microsoft Microsoft 365 Family



- ✓ Microsoft 365 Family mit bis zu 6 Personen (Organisator + 5)
- ✓ Bis zu 6 TB OneDrive-Speicher insgesamt (normalerweise je 1 TB pro Person; je nach aktuellem Tarif)
- ✓ Office-Apps für die ganze Familie auf mehreren Geräten
- ✓ Weitere Microsoft-Dienste wie Outlook, Defender und Familien-Sicherheitsfunktionen
- ✓ Bildschirmsperre, App-Limits, Inhaltsfilter, Standort & Berichte

Bis zu 6 Familienmitglieder (Organisator + 5 weitere)

Dropbox Dropbox Family



- ✓ Family-Abo mit bis zu 6 Personen (Organisator + 5)
- ✓ Gemeinsamer Speicher nach aktuellem Tarif
- ✓ Jede Person hat ein eigenes, privates Konto
- ✓ Gemeinsamer Familienbereich (Dropbox Family Room) für geteilte Fotos und Dateien
- ✓ einfache Verwaltung, Wiederherstellung von Dateien und gemeinsame Organisation

Bis zu 6 Familienmitglieder (Organisator + 5 weitere)

VERGLEICH AUF EINEN BLICK

FUNKTION	Apple	Google	Microsoft	Dropbox
GETEILTER SPEICHER	Je nach iCloud+ Tarif	Je nach Google One Tarif	Bis zu 6 TB insgesamt (je nach Tarif)	Je nach Tarif
MAX. MITGLIEDER	6 (inkl. Organisator)	6 (inkl. Organisator)	6 (inkl. Organisator)	6 (inkl. Organisator)
GETEILTE ABOS / DIENSTE	Apple-Dienste und Käufe, sofern unterstützt	Berechtigte Google-Dienste (z. B. YouTube Premium)	Microsoft 365 Apps und weitere Dienste	Je nach Tarif
PRIVATSPHÄRE	Persönliche Dateien bleiben privat (Freigabe optional)	Persönliche Dateien bleiben privat (Freigabe optional)	Persönliche Dateien bleiben privat (Freigabe optional)	Persönliche Dateien bleiben privat (Freigabe optional)
KINDERSICHERUNG	Bildschirmsperre, Kaufanfragen, Inhaltsfilter, Standort	Family Link, App-Limits, Inhaltsfilter, Standort	Microsoft Family Safety, Bildschirmsperre, Inhaltsfilter	Einfache Verwaltung und altersgerechte Einstellungen
PLATTFORM	Apple Geräte	Android, iOS, Web	Windows, macOS, iOS, Android, Web	Alle Plattformen
BESONDERHEIT	Nahtlos im Apple-Ökosystem integriert	Enge Integration mit Google-Diensten	Produktivität, Sicherheit und Organisation	Gemeinsamer Familienbereich (Dropbox Family Room)

WARUM EIN FAMILIENKONTO SINNVOLL IST



Kosten sparen

Ein Abo für alle statt für jeden einzeln.



Mehr Sicherheit

Zentrale Verwaltung, Kindersicherung und Datenschutzfunktionen.



Zeit sparen

Gemeinsame Verwaltung von Diensten, Geräten und Einstellungen.



Alles an einem Ort

Fotos, Dokumente, Kalender und Erinnerungen – für die ganze Familie.

SO RICHTEST DU EIN FAMILIENKONTO EIN

1

Dienst auswählen

Wähle den Anbieter, der am besten zu euch passt.

2

Organisator erstellen

Ein Erwachsener richtet das Familienkonto ein.

3

Mitglieder einladen

Familienmitglieder per E-Mail oder Link hinzufügen.

4

Berechtigungen festlegen

Zugriff, Inhalte, Ausgaben und Bildschirmsperre einstellen.

5

Dienste teilen

Speicher, Abos und Inhalte sofort nutzen.

6

Regelmäßig überprüfen

Einstellungen und Berechtigungen anpassen.

WICHTIGE HINWEISE



Datenschutz beachten

Nicht alles wird automatisch mit allen geteilt.



Regeln gemeinsam festlegen

Klare Absprachen schaffen Vertrauen und Sicherheit.



Einstellungen regelmäßig prüfen

Kinder werden älter – Regeln und Berechtigungen anpassen.



Preise, Speicher und enthaltene Dienste können sich ändern

Bitte die aktuellen Bedingungen der Anbieter prüfen.



EXTRA-TIPP

Kombiniere verschiedene Dienste! z. B. Google One für Android-Geräte und Microsoft 365 für Produktivität.



**GEMEINSAM BEZAHLEN.
GETRENNT SPEICHERN.
GEZIELT TEILEN.**



FAZIT

Familienkonten machen die Cloud günstiger, sicherer und einfacher. Für heute – und für morgen.



FAMILIENGROUPE IST NICHT GLEICH GEMEINSAMER DATENORDNER.

Persönliche Dateien bleiben getrennt, bis du sie ausdrücklich teilst.



CLOUD-SPEICHER FÜR PRIVATANWENDER

Welche Lösung passt zu deinen Bedürfnissen?

Ein unabhängiger Vergleich der beliebtesten Cloud-Speicher für private Nutzer

WAS IST CLOUD-SPEICHER?

Cloud-Speicher ermöglicht es dir, Dateien online zu speichern, zu synchronisieren und von überall aus darauf zuzugreifen – sicher, bequem und plattformübergreifend.

ANBIETER	 iCloud	 Google Drive	 Dropbox	 OneDrive (Microsoft)	 Proton Drive
 PASST BESONDERS ZU	Apple-Ökosystem	Google-Dienste & Zusammenarbeit	plattformübergreifende Synchronisation	Windows & Microsoft 365	Datenschutz & Ende-zu-Ende-Verschlüsselung
 KOSTENLOSER EINSTIEG	5 GB	15 GB, geteilt mit Gmail und Google Fotos	2 GB	5 GB	kostenloser Tarif Umfang kann sich ändern
 VERSCHÜSSELUNG	Transport & Speicher; E2EE abhängig von Datenart und aktiviertem erweitertem Datenschutz	Transport & Speicher; standardmäßig keine persönliche E2EE	Transport & Speicher; standardmäßig keine persönliche E2EE	Transport & Speicher; Personal Vault ist zusätzlicher Zugriffsschutz, keine allgemeine E2EE	Ende-zu-Ende-verschlüsselt; Anbieter kann Dateiinhalte nicht lesen
 STÄRKEN	• Nahtlose Integration in Apple-Geräte • Einfache Bedienung • Zuverlässige Synchronisation	• Sehr gute Zusammenarbeit • Tiefe Integration in Google-Dienste • Plattformübergreifend nutzbar	• Einfache, zuverlässige Synchronisation • Viele Plattformen • Flexible Freigabeoptionen	• Gute Integration mit Windows und Microsoft 365 • Praktisch für Office-Dateien • Plattformübergreifend	• Starker Fokus auf Datenschutz • Ende-zu-Ende-Verschlüsselung • Sitz in der Schweiz • Einfache, moderne Oberfläche
 BEACHTEN	Außerhalb des Apple-Ökosystems eingeschränkter Funktionsumfang.	Speicher mit weiteren Google-Diensten (Gmail, Google Fotos u. a.) geteilt.	Kleiner kostenloser Speicher.	Funktionsumfang abhängig von Tarif und Microsoft-Integration.	Weniger Integrationen als große Plattformanbieter.



Tarife, Preise und Funktionen ändern sich. Vor Abschluss beim Anbieter prüfen.



KEIN PAUSCHALER SIEGER

DIE RICHTIGE WAHL IST INDIVIDUELL

Es gibt nicht den einen besten Cloud-Speicher für alle. Die passende Lösung hängt von deinen Prioritäten ab:

- ✓ Welches Ökosystem nutzt du (z. B. Apple, Google, Microsoft)?
- ✓ Wie wichtig ist dir die Zusammenarbeit mit anderen?
- ✓ Wie hoch sind deine Anforderungen an Datenschutz und Verschlüsselung?
- ✓ Welches Budget ist für dich realistisch?
- ✓ Wie wichtig ist dir eine einfache Wiederherstellung gelöschter Dateien?

Prüfe deine eigenen Anforderungen und wähle den Dienst, der am besten zu dir passt.



SICHER NUTZEN

EINFACHE MASSNAHMEN, GROSSE WIRKUNG

Mit diesen Tipps erhöhst du die Sicherheit deiner Cloud-Daten:

- ✓ Nutze ein eindeutiges, langes Passwort oder noch besser einen Passkey (z. B. mit biometrischer Anmeldung).
- ✓ Aktiviere die Zwei-Faktor-Authentifizierung (2FA).
- ✓ Bewahre Wiederherstellungscodes offline und sicher auf.
- ✓ Überprüfe regelmäßig, mit wem du Dateien geteilt hast, und entferne nicht mehr benötigte Freigaben.
- ✓ Verschlüssele besonders sensible Dateien vor dem Upload zusätzlich auf deinem Gerät (client-seitig).
- ✓ Lege ein unabhängiges Backup deiner wichtigen Daten an.



SELF-HOSTING IST EINE ANDERE KATEGORIE

MEHR KONTROLLE, ABER AUCH MEHR VERANTWORTUNG

Wer mehr Kontrolle über seine Daten möchte, kann einen eigenen Server betreiben, z. B. mit Nextcloud oder einem NAS (Network Attached Storage).

- ✓ Du bestimmst, wo die Daten liegen, und kannst viele Funktionen selbst anpassen.
- ✓ Du bist selbst verantwortlich für Updates, Sicherheit und einen sicheren Fernzugriff (z. B. VPN).
- ✓ Regelmäßige Backups sind unerlässlich.
- ✓ RAID schützt vor Hardware-Ausfällen, ist aber kein Backup. Auch die Synchronisation zwischen Geräten ersetzt kein Backup.

Self-Hosting bietet viele Möglichkeiten, erfordert aber technisches Know-how und kontinuierliche Wartung.



CLOUD = KOMFORT. BACKUP = WIEDERHERSTELLBARKEIT.

FÜR WICHTIGE DATEN BRAUCHST DU BEIDES.

Cloud-Speicher macht den Alltag einfacher. Ein separates Backup stellt sicher, dass du deine Daten auch bei Fehlern, Diebstahl oder versehentlichem Löschen wiederherstellen kannst.





iCLOUD

DEINE INHALTE. ÜBERALL DABEI. EINFACH SICHER.

iCloud ist der Cloud-Dienst von Apple. Er speichert deine Fotos, Dateien, Backups und mehr sicher in der Cloud und synchronisiert sie automatisch über all deine Apple-Geräte – und auch auf Windows-PCs und im Web.

AUF EINEN BLICK

- ✓ 5 GB kostenloser Speicher (aktuell)
- ✓ Nahtlos in Apple-Geräte & -Apps integriert
- ✓ Automatische Synchronisation in Echtzeit
- ✓ Datenübertragung verschlüsselt, sichere Speicherung
- ✓ Ende-zu-Ende-Verschlüsselung je nach Datenkategorie
- ✓ Auf iPhone, iPad, Mac, Apple Watch, Apple TV, Windows und im Web nutzbar (mit Einschränkungen)
- ✓ Für Einzelpersonen und Familien



SPEICHER

5 GB kostenlos (aktuell)

Mit iCloud+ kannst du mehr Speicherplatz buchen. Preise und Verfügbarkeit können sich ändern.



iCLOUD+ TARIFE

Größere Speicherpläne mit zusätzlichen Funktionen wie Privat-Relay, E-Mail-Schutz, eigener Domain für E-Mails und HomeKit Secure Video. Preise können sich ändern.



DATEITYPEN

Fotos, Videos, Dateien, Backups, Nachrichten, Kontakte, Kalender, Notizen und mehr. Einzelne Dateien bis 50 GB (über iCloud Drive). Unterstützte Formate können variieren.



GERÄTE & ZUGRIFF

iPhone, iPad, Mac, Apple Watch, Apple TV.

Auch auf Windows (iCloud für Windows) und im Web unter icloud.com – mit eingeschränktem Funktionsumfang.



SICHERHEIT

Datenübertragung mit TLS verschlüsselt. Daten auf Apple-Servern verschlüsselt gespeichert. Ende-zu-Ende-Verschlüsselung je nach Datenkategorie und ob „Erweiterter Datenschutz“ aktiviert und verfügbar ist.



FAMILIE

Speicher kann mit bis zu 5 Familienmitgliedern gemeinsam genutzt werden.

Geteilter Speicher macht die Dateien der anderen nicht automatisch sichtbar – jede Person behält ihre eigenen privaten Daten.

WICHTIGSTE FUNKTIONEN



Fotos in iCloud

Speichert deine Fotos und Videos in voller Qualität und macht sie auf allen Geräten verfügbar.



iCloud Drive

Speichere Dateien in der Cloud, greife von überall darauf zu und arbeite geräteübergreifend an denselben Dateien.



Backups in iCloud

Automatische Backups deines iPhone oder iPad, wenn es geladen und mit WLAN verbunden ist.



iCloud-Schlüsselbund

Speichert Passwörter, Kreditkarten und WLAN-Zugänge sicher und synchronisiert sie auf deinen Geräten.



Familienfreigabe

Teile Speicher, Käufe, Abos, Standorte und mehr mit bis zu 5 Familienmitgliedern.



iCloud Mail

Eigene @icloud.com E-Mail-Adresse mit Spam-Schutz.

SO FUNKTIONIERT iCLOUD



1 ANMELDEN

Melde dich mit deiner Apple-ID auf deinem Gerät an und aktiviere iCloud in den Einstellungen.



2 AUTOMATISCH SYNCEN

Deine Daten werden automatisch in iCloud geladen und auf all deinen Geräten synchronisiert.



3 ÜBERALL ZUGREIFEN

Greife jederzeit auf deine Inhalte zu – auf jedem Apple-Gerät, in Windows oder im Web (mit Einschränkungen).



4 TEILEN & ZUSAMMENARBEITEN

Teile Dateien, Ordner, Fotos, Kalender und mehr mit anderen – einfach und sicher.



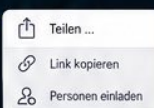
5 SICHER AUFBEWAHREN

Deine Daten sind in der Cloud sicher gespeichert und aktuell, auch wenn dein Gerät verloren geht oder kaputt ist.

DATEIEN & DATEN TEILEN – SO GEHT'S

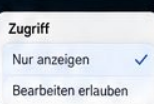
1 Datei oder Ordner auswählen

Tippe oder klicke auf „Teilen“ und wähle z. B. „Link kopieren“ oder lade Personen ein.



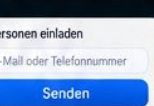
2 Berechtigungen festlegen

Bestimme, ob andere anzeigen oder bearbeiten dürfen.



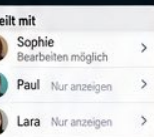
3 Personen einladen

Gib E-Mail-Adresse oder Telefonnummer ein oder teile den Link.



4 Geteilte Inhalte verwalten

Du kannst geteilte Dateien und Ordner jederzeit in der Teilen-Übersicht anpassen oder den Zugriff beenden.



iCLOUD NUTZEN – KURZANLEITUNG



Auf dem iPhone / iPad

1. Einstellungen öffnen.
2. Oben auf deinen Namen tippen.
3. „iCloud“ auswählen.
4. Wunschoptionen aktivieren.



Auf dem Mac

1. Systemeinstellungen öffnen.
2. Auf deinen Namen > „iCloud“ klicken.
3. Funktionen auswählen.



Auf Windows

1. iCloud für Windows laden und installieren.
2. Mit deiner Apple-ID anmelden.
3. Gewünschte Inhalte synchronisieren (z. B. Fotos, iCloud Drive, Passwörter).



Im Web

1. Auf icloud.com anmelden.
2. Fotos, Dateien, Kontakte, Kalender u. v. m. nutzen. (Funktionsumfang kann eingeschränkt sein.)

PRAKTISCHE TIPPS



Speicher optimieren

„iPhone-Speicher optimieren“ aktivieren und große Dateien in iCloud speichern.



Ordnung halten

Ordner in iCloud Drive nutzen und aussagekräftige Namen vergeben.



Große Anhänge

Große Dateien über iCloud Drive teilen und nicht per E-Mail versenden.



Geteilte Alben

Erstelle geteilte Alben für Familie und Freunde.



Zwei-Faktor-Authentifizierung

Aktiviere die Zwei-Faktor-Authentifizierung für deine Apple-ID.



Speicher verwalten

Unter „Einstellungen“ > [dein Name] > „iCloud“ siehst du, was wie viel Speicher belegt. Nicht benötigte Daten kannst du löschen.

WAS KANN iCLOUD ALLES SPEICHERN?



Fotos & Videos



Dateien & Ordner (iCloud Drive)



Nachrichten (iMessage)



Kontakte



Kalender



Notizen



Passwörter (iCloud-Schlüsselbund)



Gesundheitsdaten (Health)



Käufe & Abos



Home-Daten (HomeKit)



Sprachmemos



und vieles mehr ...



SICHERHEIT & DATENSCHUTZ

- ✓ Verschlüsselung bei der Übertragung (TLS)
- ✓ Verschlüsselte Speicherung auf Apple-Servern
- ✓ Ende-zu-Ende-Verschlüsselung je nach Datenkategorie und Einstellungen
- ✓ Erweiterter Datenschutz (optional, je nach Region)
- ✓ Apple kann ohne deinen Gerätecode nicht auf Ende-zu-Ende-verschlüsselte Daten zugreifen.



VORTEILE

- ✓ Stark in Apple-Geräte & -Apps integriert
- ✓ Einfache Einrichtung & automatische Synchronisation
- ✓ Flexibel auf vielen Geräten nutzbar
- ✓ Hilft, deine Daten zu schützen und verfügbar zu halten
- ✓ Praktische Zusatzfunktionen über iCloud+
- ✓ Gut für Privatpersonen und Familien



WAS IST ZU BEACHTEN?

- ✗ Nur 5 GB kostenlos (aktuell)
- ✗ Preise und Funktionen von iCloud+ können sich ändern.
- ✗ Windows- und Web-Nutzung mit Einschränkungen.
- ✗ Ende-zu-Ende-Verschlüsselung hängt von der Datenkategorie und den Einstellungen (Erweiterter Datenschutz) ab.
- ✗ Wiederherstellungsoptionen einrichten – besonders bei aktiviertem Erweiterter Datenschutz.



IDEAL FÜR

- ✓ iPhone, iPad & Mac Nutzer
- ✓ Familien & gemeinsam genutzte Geräte
- ✓ Alle, die ihre Daten sicher und bequem in der Cloud haben möchten
- ✓ Nutzer, die von überall auf ihre Inhalte zugreifen möchten
- ✓ Alle, die Apple-Dienste nahtlos miteinander nutzen wollen



EINFACH. SICHER. ÜBERALL DABEI.



Mehr Infos: support.apple.com/de-de/icloud und icloud.com



GOOGLE DRIVE

SICHER SPEICHERN. EINFACH TEILEN. BESSER SZAMMENARBEITEN.

Google Drive ist der Cloud-Speicher von Google. Speichere deine Dateien sicher online, greife von überall darauf zu und arbeite gemeinsam mit anderen.

AUF EINEN BLICK

- ✓ 15 GB kostenlos (geteilt mit Gmail & Fotos)
- ✓ Sicherer Zugriff von allen Geräten
- ✓ Nahtlose Zusammenarbeit mit Google-Apps
- ✓ Starke Sicherheitsfunktionen
- ✓ Flexible Speicher-Optionen mit Google One



KOSTENLOSER SPEICHER

15 GB Speicherplatz gratis – gemeinsam für Google Drive, Gmail und Google Fotos.



GOOGLE ONE FÜR MEHR SPEICHER

Größere Speicherpakete über Google One verfügbar. Preise und Optionen können sich ändern.



DATEITYPEN

Nahezu alle gängigen Dateitypen – z. B. Bilder, Videos, Dokumente, Archive und mehr.



ZUGRIFF AUF ALLEN GERÄTEN

Im Web, unter Windows, macOS, Linux, Android und iOS. Dateien sind überall aktuell verfügbar.



ZUSAMMENARBEITEN

Direkt in Google Docs, Sheets und Slides gemeinsam in Echtzeit erstellen und bearbeiten.



SICHERHEIT

Verschlüsselte Übertragung, verschlüsselte Speicherung, 2-Faktor-Authentifizierung und weitere Schutzfunktionen.

DIE WICHTIGSTEN FUNKTIONEN



Dateien speichern & sichern

Bewahre deine Dateien sicher in der Cloud auf und greife jederzeit darauf zu.



Einfach teilen

Teile Dateien oder Ordner mit anderen und lege Berechtigungen fest.



Gemeinsam bearbeiten

Arbeite in Google Docs, Sheets und Slides in Echtzeit zusammen – mit Kommentaren und Änderungsverlauf.



Schnell finden

Mit der leistungsstarken Google-Suche findest du Dateien, Inhalte in Bildern (OCR) und mehr – schnell und zuverlässig.



Offline verfügbar

Wichtige Dateien offline nutzen und Änderungen werden automatisch synchronisiert, sobald du wieder online bist.



Versionen & Papierkorb

Frühere Versionen wiederherstellen und gelöschte Dateien im Papierkorb finden (zeitlich begrenzt).

SO FUNKTIONIERT GOOGLE DRIVE



1 HOCHLADEN

Dateien oder Ordner per Drag & Drop im Browser hochladen oder über die Drive-App auf deinen Geräten.



2 SPEICHERN & SYNCHRONISIEREN

Deine Dateien werden sicher in der Cloud gespeichert und mit all deinen Geräten synchronisiert.



3 ORGANISIEREN

Ordner erstellen, Dateien umbenennen, farbig kennzeichnen und mit Sternen markieren.



4 TEILEN & ZUSAMMENARBEITEN

Berechtigungen festlegen und gemeinsam in Echtzeit bearbeiten.



5 ZUGREIFEN

Auf deine Dateien zugreifen – jederzeit und auf all deinen Geräten, online oder offline.

DATEIEN TEILEN – SO GEHT'S



1 Datei oder Ordner auswählen

Klicke mit der rechten Maustaste auf die gewünschte Datei oder den Ordner und wähle „Teilen“.



2 Berechtigungen festlegen

Lege fest, wer die Datei sehen, kommentieren oder bearbeiten darf (z. B. bestimmte Personen oder alle mit dem Link).



3 Link teilen

Kopiere den Link und sende ihn an die gewünschten Personen.



Tipp: Bewusst teilen

Teile Links nur mit vertrauenswürdigen Personen und prüfe die Berechtigungen regelmäßig. Vermeide die Einstellung „Jeder mit dem Link“, wenn die Inhalte sensibel sind.

GOOGLE DRIVE AUF ALL DEINEN GERÄTEN



Im Browser nutzen

Einfach auf drive.google.com anmelden – keine Installation erforderlich.



Drive für Desktop (Windows, macOS, Linux)

Dateien im Datei-Explorer oder Finder synchronisieren und bequem vom Computer aus nutzen.



Auf Smartphone & Tablet

Die Google Drive App für Android oder iOS nutzen – direkt aus der App heraus hochladen, ansehen und teilen.



Auch offline arbeiten

Wichtige Dateien offline verfügbar machen – Änderungen werden später automatisch synchronisiert.

SICHERHEIT & DATENSCHUTZ



Verschlüsselung auf dem Weg und im Ruhezustand

Deine Daten werden bei der Übertragung (TLS) und auf den Google-Servern (at rest) verschlüsselt. Google schützt deine Daten mit modernen Sicherheitsmaßnahmen.



Dein Konto zusätzlich schützen

Aktiviere die 2-Faktor-Authentifizierung und nutze möglichst Passkeys.



Für sehr sensible Daten

Wenn du besonders vertrauliche Dateien speichern möchtest, verwende eine Ende-zu-Ende-Verschlüsselung auf deinem Gerät (Client-side), bevor du sie hochlädst (z. B. mit einer vertrauenswürdigen Verschlüsselungssoftware).

GOOGLE ONE – MEHR SPEICHER



Mit Google One kannst du deinen Speicherplatz erweitern und erhältst je nach Tarif zusätzliche Vorteile.



Größere Speicherpakete verfügbar



Preise und Inhalte können sich ändern



In der Google One App verwalten



Gut zu wissen

Die 15 GB des kostenlosen Google-Kontos werden gemeinsam von Google Drive, Gmail und Google Fotos genutzt.



VORTEILE

- ✓ Einfach zu bedienen
- ✓ Überall verfügbar
- ✓ Starke Zusammenarbeit
- ✓ Zuverlässig und sicher
- ✓ Nahtlose Integration mit Google-Apps



MÖGLICHE NACHTEILE

- ✗ Geteilter Speicher mit Gmail & Fotos
- ✗ Für sehr große Datenmengen kann ein kostenpflichtiger Tarif nötig sein
- ✗ Internetverbindung erforderlich
- ✗ Keine Ende-zu-Ende-Verschlüsselung für normale Drive-Dateien



IDEAL FÜR

- ✓ Privatpersonen & Familien
- ✓ Schüler*innen, Studierende & Bildung
- ✓ Teams in Unternehmen
- ✓ Freelancer & Kreative
- ✓ Vereine & Organisationen



UNSER FAZIT

Google Drive ist ein sicherer, leistungsstarker und benutzerfreundlicher Cloud-Speicher mit hervorragenden Möglichkeiten zur Zusammenarbeit. Mit den richtigen Einstellungen und ergänzenden Sicherheitsmaßnahmen eine ausgezeichnete Wahl für den Alltag.



DEINE DATEIEN. ÜBERALL. IMMER DABEI.

Sicher speichern. Einfach teilen. Mehr erreichen – mit Google Drive.



Auf allen Geräten.
Für alles, was wichtig ist.



Dropbox

Deine Dateien. Einfach. Sicher. Überall.

Dropbox ist ein bewährter Cloud-Speicher, mit dem du Dateien sicher speichern, synchronisieren und teilen kannst – auf all deinen Geräten, privat und beruflich.

AUF EINEN BLICK

- ✓ Einfach zu bedienen
- ✓ Zuverlässige Synchronisation
- ✓ Starkes Teilen & Zusammenarbeit
- ✓ Versionierung und Wiederherstellung
- ✓ Für Privatpersonen, Teams & Unternehmen



SPEICHER

Dropbox Basic bietet einen begrenzten kostenlosen Speicher. Kostenpflichtige Tarife bieten mehr Speicher und Funktionen.

TARIFE & FUNKTIONEN

Funktionen und Speicherplatz variieren je nach Tarif und können sich ändern. Aktuelle Informationen findest du auf der offiziellen Website.

DATEIGRÖSSE

Große Dateien lassen sich bequem hochladen und teilen. Grenzen abhängig von deinem Tarif.

PLATTFORMEN & APPS

Windows, macOS, Linux, iOS, Android und Web-App. Deine Dateien sind auf all deinen Geräten verfügbar.

SICHERHEIT

Verschlüsselung bei Übertragung (TLS) und im Ruhezustand (AES-256). Keine standardmäßige, vom Nutzer kontrollierte Ende-zu-Ende-Verschlüsselung für reguläre Dateien.

INTEGRATIONEN

Zusammenarbeit mit zahlreichen Tools, z. B. Microsoft 365, Google Workspace, Slack, Zoom, Trello und vielen mehr.

DIE WICHTIGSTEN FUNKTIONEN



Dateien speichern & synchronisieren
Deine Dateien sind sicher in der Cloud gespeichert und auf all deinen Geräten synchronisiert.



Einfaches Teilen & Zusammenarbeit
Teile Dateien oder Ordner per Link, lege Berechtigungen fest und arbeite gemeinsam in Projekten.



Versionverlauf & Wiederherstellung
Stelle frühere Versionen wieder her. Die Aufbewahrungsdauer von Versionen hängt von deinem Tarif ab.



Automatisches Foto-Backup
Sichere deine Fotos und Videos bequem von Smartphone oder Kamera in Dropbox.



Schnelle Suche
Finde Dateien, Inhalte und sogar Text in Bildern mit leistungsstarker Suche.



Ordnerstruktur & Organisation
Halte deine Dateien mit Ordnern, Favoriten und übersichtlichen Ansichten organisiert.



Selective Synchronisation
Wähle, welche Ordner auf deinem Gerät gespeichert werden. Online-nur-Dateien sparen Platz auf deinem Gerät, aber nicht deinen Dropbox-Speicherplatz.

SO FUNKTIONIERT DROPBOX



1 KONTO ERSTELLEN

Registriere dich auf dropbox.com und erstelle dein Konto.



2 APP INSTALLIEREN

Lade die Dropbox-App für dein Betriebssystem herunter und melde dich an.



3 ORDNER EINRICHTEN

Dropbox erstellt einen Dropbox-Ordner auf deinem Gerät.



4 DATEIEN HINZUFÜGEN

Ziehe Dateien in den Ordner oder lade sie manuell hoch.



5 AUTOMATISCH SYNCHRONISIERT

Deine Dateien werden sicher in der Cloud gespeichert und mit all deinen Geräten synchronisiert.



6 TEILEN & ZUSAMMENARBEITEN

Teile Dateien oder Ordner per Link und lege Berechtigungen fest.

DATEIEN & ORDNER TEILEN – SO GEHT'S

1 Datei oder Ordner auswählen

Klicke mit der rechten Maustaste auf die Datei oder den Ordner, den du teilen möchtest.



2 Freigabeoptionen festlegen

Wähle, ob andere die Datei nur ansehen oder bearbeiten dürfen, und setze ggf. ein Passwort oder ein Ablaufdatum.

3 Link kopieren und teilen

Kopiere den Link und sende ihn per E-Mail, Messenger oder füge ihn in ein Dokument ein.

SICHERHEIT & DATENSCHUTZ



Verschlüsselung

Deine Dateien sind bei der Übertragung (TLS) und im Ruhezustand (AES-256) verschlüsselt.



Kein standardmäßiges Ende-zu-Ende

Normalerweise werden die Verschlüsselungsschlüssel von Dropbox verwaltet. Für besonders sensible Daten kann eine zusätzliche, clientseitige Verschlüsselung sinnvoll sein (z. B. mit entsprechender Software).



Kontoschutz

Aktiviere die Zwei-Faktor-Authentifizierung (2FA) oder Passkeys, verwende ein starkes, einzigartiges Passwort und überprüfe regelmäßig die zugeordneten Geräte und Apps.



Datenschutz

Dropbox verarbeitet deine Daten gemäß der DSGVO. Weitere Informationen findest du in der Datenschutzerklärung von Dropbox.

DROPBOX NUTZEN – SCHRITT FÜR SCHRITT



1. Konto erstellen und App installieren

Erstelle ein Konto, lade die App herunter und melde dich an.



2. Einstellungen anpassen

Wähle, welche Ordner synchronisiert werden (synchronisiert oder nur online).



3. Dateien hinzufügen

Ziehe Dateien in den Dropbox-Ordner oder lade sie hoch.



4. Teilen und zusammenarbeiten

Erstelle einen Link oder lade andere ein.



5. Versionen wiederherstellen

Greife bei Bedarf auf frühere Versionen zu (je nach Tarif).



6. Noch mehr Möglichkeiten entdecken

Nutze Integrationen, automatische Backups und smarte Funktionen für deinen Alltag.

PRAKTISCHE TIPPS



Geräteplatz sparen

Nutze selektive Synchronisation bzw. Online-nur-Dateien, um Speicherplatz auf deinem Gerät zu sparen (das reduziert nicht deinen Cloud-Speicherplatz).



Zugriff regelmäßig prüfen

Überprüfe, welche Geräte und Apps Zugriff auf dein Konto haben, und entferne nicht mehr benötigte Zugriffe.



Wichtige Daten zusätzlich sichern

Dropbox ist kein Ersatz für ein vollständiges Backup. Bewahre besonders wichtige Daten zusätzlich an einem zweiten Ort auf.



Sinnvolle Integrationen

Verbinde Dropbox mit deinen bevorzugten Tools, um deine Produktivität zu steigern.



Benachrichtigungen nutzen

Lass dich über Änderungen, geteilte Dateien und Aktivitäten informieren.



Aufgeräumt bleiben

Nutze Ordner, aussagekräftige Namen und Favoriten für einen schnellen Zugriff.

WOFÜR IST DROPBOX IDEAL?

- ✓ Sicherer Zugriff auf deine Dateien – überall
- ✓ Zuverlässige Synchronisation auf all deinen Geräten
- ✓ Einfaches Teilen mit Freunden, Familie und Kollegen
- ✓ Effektive Zusammenarbeit in Projekten
- ✓ Schnelle Wiederherstellung früherer Versionen (je nach Tarif)
- ✓ Geeignet für Privatpersonen, Teams und Unternehmen
- ✓ Eine ausgereifte, vertrauenswürdige Lösung

DATEITYPEN, DIE DU SPEICHERN KANNST

- 📄 Dokumente (PDF, Word, Excel, PowerPoint)
- 🖼️ Bilder und Fotos (JPG, PNG, RAW)
- 🎥 Videos (MP4, MOV, AVI u. v. m.)
- 🎵 Musik und Audio (MP3, WAV, FLAC)
- 📁 Archive (ZIP, RAR)
- 💻 Code & Design-Dateien
- + Und viele weitere Dateitypen ...



VORTEILE

- ✓ Einfach zu bedienen
- ✓ Zuverlässige Synchronisation
- ✓ Starkes Teilen & Zusammenarbeit
- ✓ Umfangreiche Integrationen
- ✓ Hohe Sicherheit und Datenschutzstandards



NACHTEILE

- ✗ Kostenloser Speicherplatz ist begrenzt
- ✗ Erweiterte Funktionen nur in kostenpflichtigen Tarifen
- ✗ Keine standardmäßige, nutzerkontrollierte Ende-zu-Ende-Verschlüsselung
- ✗ Keine vollständige Backup-Lösung



IDEAL FÜR

- 👤 Privatpersonen, die ihre Dateien sicher speichern wollen
- 👨‍👩‍👧 Familien zum Teilen von Fotos und Dokumenten
- 👨‍💻 Freelancer und Teams für Projekte & Zusammenarbeit
- 🏢 Unternehmen jeder Größe
- 🌐 Alle, die ortsunabhängig produktiv arbeiten möchten



SICHERHEIT AUF EINEN BLICK

- ✓ TLS-Verschlüsselung bei der Übertragung
- ✓ AES-256-Verschlüsselung im Ruhezustand
- ✓ Zwei-Faktor-Authentifizierung (2FA) / Passkeys
- ✓ Regelmäßige Überprüfung von Gerätezugriffen
- ✓ DSGVO-konform

MEHR ERREICHEN – MIT DROPBOX
SICHER. FLEXIBEL. ZUSAMMEN.



OneDrive

Dein Cloud-Speicher. Sicher. Integriert. Überall dabei.

OneDrive ist der Cloud-Speicher von Microsoft. Er ist nahtlos in Windows und Microsoft 365 integriert und hilft dir, deine Dateien sicher zu speichern, zu synchronisieren und auf allen Geräten produktiv zu arbeiten.

ÜBERALL ZUGRIFF – AUF ALL DEINEN GERÄTEN

- ✓ Nahtlos in Windows und Microsoft 365
- ✓ Auf PC, Mac, iOS, Android und im Web
- ✓ Deine Dateien immer aktuell synchronisiert
- ✓ Sicherer Zugriff von überall
- ✓ Ideal für Privatpersonen, Familien, Schule und Beruf



SPEICHER

Ein kleiner kostenloser Speicher ist enthalten. Zusätzlicher Speicher ist oft in Microsoft 365 enthalten.



TARIFE

Mehr Speicher und Funktionen sind in Microsoft 365 Abos erhältlich. Details und Verfügbarkeit können sich ändern.



DATEIGRÖSSE

Unterstützt sehr große Dateien. Praktisch keine relevanten Limits für typische Nutzung.



ZUGRIFF & APPS

Windows, macOS, iOS, Android, Web sowie Office-Apps (Word, Excel, PowerPoint) und viele weitere.



SICHERHEIT

Verschlüsselte Übertragung (TLS) und verschlüsselte Speicherung im Ruhezustand. Zusätzliche Schutzfunktionen wie Zwei-Faktor-Authentifizierung und Ransomware-Erkennung.



INTEGRATION

Perfekte Zusammenarbeit mit Windows, Microsoft 365, Teams, Outlook und vielen weiteren Diensten und Apps.

DIE WICHTIGSTEN FUNKTIONEN



Dateien speichern & synchronisieren

Bewahre deine Dateien sicher in der Cloud auf und halte sie auf allen Geräten automatisch aktuell.



Einfach teilen & zusammenarbeiten

Teile Dateien und Ordner per Link oder E-Mail und arbeite gleichzeitig in Office-Apps zusammen.



Versionen wiederherstellen

Stelle frühere Versionen deiner Dateien wieder her, falls etwas versehentlich geändert oder gelöscht wurde.



Persönlicher Tresor (Personal Vault)

Ein besonders geschützter Bereich für sensible Dateien. Verfügbar je nach Plan, mit zusätzlicher Anmeldung.



Dateien bei Bedarf (Files On-Demand)

Spare Speicherplatz auf deinem Gerät. Dateien werden nur bei Bedarf heruntergeladen. Das spart lokalen Speicherplatz, aber nicht deinen Cloud-Speicher.



Automatische Backups

Sichere wichtige Ordner wie Desktop, Dokumente und Bilder automatisch in OneDrive (unter Windows).



Nachhaltigkeit

Microsoft betreibt seine Rechenzentren erneuerbar und arbeitet kontinuierlich an mehr Energieeffizienz.

SO FUNKTIONIERT ONEDRIVE



1 ANMELDEN

Melde dich mit deinem Microsoft-Konto an (z. B. Outlook, Hotmail oder live.com) – in der OneDrive-App, in Windows oder im Web.



2 HOCHLADEN & SYNCHRONISIEREN

Lege Dateien im OneDrive-Ordner ab. Sie werden automatisch sicher in der Cloud gespeichert und auf deinen Geräten synchronisiert.



3 ÜBERALL VERFÜGBAR

Greife von PC, Mac, Smartphone, Tablet oder im Web auf deine aktuellen Dateien zu.



4 TEILEN & ZUSAMMENARBEITEN

Teile Dateien oder Ordner, lege Berechtigungen fest und arbeite gemeinsam in Echtzeit an Dokumenten.



5 IN MICROSOFT 365 ARBEITEN

Öffne und bearbeite Dateien direkt in Web, Windows oder Office-Apps – allein oder gemeinsam mit anderen.



6 SICHER AUFBEWAHRT

Deine Dateien sind verschlüsselt übertragen und gespeichert. Zusätzliche Schutzfunktionen helfen, deine Daten vor Verlust und Bedrohungen zu schützen.

DATEIEN & ORDNER TEILEN – SO GEHT'S

1 Datei oder Ordner auswählen

Klicke mit der rechten Maustaste auf die Datei oder den Ordner und wähle „Teilen“.



2 Freigabe einstellen

Wähle, wer den Link verwenden darf (z. B. bestimmte Personen oder Personen in deiner Organisation).

3 Berechtigungen festlegen

Lege fest, ob andere nur anzeigen oder auch bearbeiten dürfen.

Linkeinstellungen

- ☒ Jede Person mit dem Link
☐ Personen in meiner Organisation
☐ Bestimmte Personen

☒ Bearbeiten zulassen

Übernehmen

4 Link kopieren oder senden

Kopiere den Link und teile ihn per E-Mail, Chat oder in Teams.

Link kopieren

5 Zugriffe verwalten

Du kannst geteilte Links jederzeit ändern oder widerrufen.

ONEDRIVE NUTZEN – KURZANLEITUNG



Im Web (onedrive.live.com)

1. Mit deinem Microsoft-Konto anmelden
2. Dateien hochladen, verwalten und teilen
3. Office-Dateien direkt im Browser bearbeiten



Unter Windows

1. OneDrive ist meist vorinstalliert
2. Mit dem Microsoft-Konto anmelden
3. Ordner wie Desktop, Dokumente, Bilder sichern
4. Mit Dateien im Explorer arbeiten



Unter macOS

1. OneDrive-App aus dem App Store installieren
2. Mit dem Microsoft-Konto anmelden
3. Ordner auswählen und synchronisieren



Auf dem Smartphone oder Tablet (iOS/Android)

1. OneDrive-App aus dem App Store oder Google Play
2. Mit dem Microsoft-Konto anmelden
3. Fotos automatisch sichern (optional)

PRAKTISCHE TIPPS



Wichtige Ordner sichern

Aktiviere die Sicherung von Desktop, Dokumenten und Bildern.



Offline verfügbar machen

Dateien lassen sich bei Bedarf lokal verfügbar machen. Das spart Gerätespeicher, ändert aber nicht deinen Cloud-Speicher.



Einstellungen prüfen

Lege fest, welche Ordner synchronisiert werden und nutze die Einstellungen in der OneDrive-App.



Versionen und Papierkorb

Gelöschte Dateien und frühere Versionen können je nach Plan und Einstellungen für eine bestimmte Zeit wiederhergestellt werden.



Unabhängige Backups

OneDrive ist kein Ersatz für ein vollständiges Backup. Sichere zusätzlich wichtige Daten auf einem zweiten Medium.

WAS KANN ICH IN ONEDRIVE SPEICHERN?



Dokumente (Word, Excel, PowerPoint, PDF u. v.m.)



Fotos & Videos (inkl. automatischem Upload)



Musik & Audio-Dateien



E-Mails & Anhänge (aus Outlook)



Notizen (OneNote)



Scans & Belege



Projekte & Präsentationen



Und vieles mehr ...



DEINE VORTEILE

- ✓ Nahtlose Integration in Windows & Microsoft 365
- ✓ Einfach zu bedienen
- ✓ Auf allen Geräten verfügbar
- ✓ Sicher und zuverlässig
- ✓ Ideal für Zusammenarbeit



WORAUF DU ACHTEN SOLLTEST

- ⚠ Kein vollständiger Ersatz für ein Backup
- ⚠ Freigabelinks sorgfältig prüfen
- ⚠ Versionierungs- und Papierkorbzeiten hängen vom Plan ab
- ⚠ Kein vom Nutzer steuerbares Ende-zu-Ende-Chiffrieren
- ⚠ Verfügbarkeit von Funktionen kann sich ändern



IDEAL GEEIGNET FÜR

- ✓ Privatpersonen & Familien
- ✓ Schüler, Studierende & Lehrkräfte
- ✓ Berufstätige & Teams
- ✓ Vereine, Organisationen & Unternehmen



SICHERHEIT & DATENSCHUTZ

- ✓ Verschlüsselte Übertragung (TLS)
- ✓ Verschlüsselte Speicherung im Ruhezustand
- ✓ Zwei-Faktor-Authentifizierung (2FA) oder Passkeys
- ✓ Ransomware-Erkennung und Dateiwiederherstellung
- ✓ Du behältst die Kontrolle über deine Daten



SICHER NUTZEN – UNSERE EMPFEHLUNG

- Aktiviere Zwei-Faktor-Authentifizierung (2FA) oder Passkeys.
- Verwende ein starkes, einzigartiges Passwort.
- Sei vorsichtig beim Teilen und überprüfe Berechtigungen.



MEHR INFOS & SUPPORT

- Website: onedrive.live.com
- Hilfe: support.microsoft.com
- Datenschutz: privacy.microsoft.com

DEINE DATEIEN.
DEINE WELT.
AUF ALLEN GERÄTEN.



NAS DEIN ZENTRALER SPEICHER

SICHER. FLEXIBEL. UNABHÄNGIG.

Ein NAS (Network Attached Storage) ist dein privater Dateiserver im Netzwerk. Alle Geräte greifen darauf zu – sicher, schnell und jederzeit verfügbar.



DIE VORTEILE EINES NAS



DEINE DATEN BLEIBEN DEINE

Speicherung bei dir zu Hause – nicht in fremden Rechenzentren.



MEHR SICHERHEIT

RAID erhöht die Verfügbarkeit. Backups schützen vor Datenverlust. Verschlüsselung schützt vor unbefugtem Zugriff.



ÜBERALL ZUGRIFF

Von unterwegs auf deine Dateien zugreifen – sicher und bequem.



KOSTEN SPAREN

Laufende Kosten für Strom, Festplatten, Ersatzteile und gegebenenfalls Zusatzdienste.



VIELSEITIG EINSETZBAR

Dateien, Backups, Medien, Überwachung, Hosting und vieles mehr.

WAS KANN EIN NAS?

- ✓ Dateien zentral speichern & teilen
- ✓ Automatische Backups für PC, Mac, Smartphones
- ✓ Fotos & Videos sicher sichern
- ✓ Medien streamen (z. B. Filme, Musik)
- ✓ Überwachungskameras aufzeichnen
- ✓ Cloud-Speicher als Alternative oder Ergänzung
- ✓ Eigene Dienste betreiben (z. B. Webserver, Mail, VPN)



SO FUNKTIONIERT EIN NAS

- NAS mit Router verbinden**
Über LAN-Kabel für maximale Stabilität und Geschwindigkeit.
- Festplatten einsetzen**
Je nach Modell 1 bis 24+ Laufwerke möglich.
- RAID auswählen**
Für Sicherheit und Performance (z. B. RAID 1, 5, 6, 10).
- Einrichten & loslegen**
Über Weboberfläche oder App einfach konfigurieren.



RAID – DEIN DATEN. DEINE WAHL.

- RAID 0** Maximale Geschwindigkeit, keine Redundanz. Ausfall einer Platte gefährdet alle Daten.
- RAID 1** Spiegelung: Eine Festplatte darf ausfallen. RAID IST KEIN BACKUP.
- RAID 5** Eine Festplatte darf ausfallen; Wiederaufbau belastet das System.
- RAID 6** Zwei Festplatten dürfen ausfallen.
- RAID 10** Hohe Leistung und Redundanz; etwa 50 % nutzbare Kapazität.

RAID NACH BEDARF WÄHLEN – ZUSÄTZLICH IMMER EIN GETRENNTES BACKUP.

TYPISCHE EINSATZGEBIETE

- DATEIEN & DOKUMENTE**
Zentral speichern und teilen.
- FOTOS & VIDEOS**
Automatisch sichern, Erinnerungen bewahren.
- MEDIEN-CENTER**
Filme, Serien, Musik streamen.
- ÜBERWACHUNG**
Kameraaufnahmen aufzeichnen & sichern.
- BACKUP-ZENTRALE**
Für PC, Mac, Smartphones und andere Geräte.
- EIGENE DIENSTE**
Webserver, Mail, VPN, Datenbanken u. v. m.

BELIEBTE NAS-HERSTELLER

- Synology** Benutzerfreundlich, viele Apps, starkes Betriebssystem (DSM).
- QNAP** Leistungsstark, viele Funktionen, ideal für Power-User.
- asustor** Gute Preis-Leistung, einfach zu bedienen.
- TERRAMASTER** Viel Leistung für wenig Geld, gute Hardware.
- UGREEN** Neue Modelle mit starkem Preis-Leistungs-Verhältnis.

Tipp: Achte auf Updates und eine aktive Community.

WICHTIGE FUNKTIONEN, AUF DIE DU ACHTEN SOLLTEST

- LEISTUNGSSTARKE HARDWARE**
CPU, RAM und Ethernet beeinflussen Performance.
- ERWEITERBARKEIT**
Mehr Festplatten oder Erweiterungsgehäuse möglich?
- FERNZUGRIFF**
Sicherer Zugriff über Internet (z. B. über QuickConnect, VPN).
- SICHERHEIT**
Verschlüsselung, 2FA, Benutzerrechte & Firewall.
- BACKUP & SNAPSHOTS**
Regelmäßige Backups und Snapshots schützen vor Datenverlust.
- APPS & ERWEITERUNGEN**
Apps für Cloud, Medien, Überwachung, Office und mehr.

NAS STARTEN – SO GEHT'S

- 1 NAS auswählen & Festplatten einbauen
- 2 Mit Router verbinden (LAN-Kabel!)
- 3 NAS-System einrichten (Weboberfläche)
- 4 Benutzerkonten & Ordnerstruktur anlegen
- 5 Backups einrichten (regelmäßig!)
- 6 Geräte verbinden & Daten sichern

Tipp: Nur ein funktionierendes und getestetes Backup ist ein gutes Backup.

NAS vs. CLOUD

- | NAS | VS. | CLOUD |
|---------------------------------|-----|---|
| ✓ Daten bleiben bei dir | | ✓ Überall verfügbar (Internet nötig) |
| ✓ Einmalige Kosten | | ✓ Keine Hardware zuhause nötig |
| ✓ Volle Kontrolle | | ✓ Laufende Kosten |
| ✓ Kein Abo notwendig | | ✓ Anbieter hat Kontrolle über deine Daten |
| ✓ Auch offline im LAN verfügbar | | ✓ Geschwindigkeit abhängig von Internet |

NAS + SEPARATER, VERSIONIERTER CLOUD-BACKUP-JOB

- ✓ **Backup:** Zusätzliche, unabhängige Kopie deiner NAS-Daten in der Cloud (versioniert).
- ✓ **Synchronisation:** Halte Daten auf mehreren Geräten oder in der Cloud aktuell.
- ✓ **Beides sinnvoll:** Synchronisation ≠ Backup! Gelöschte oder beschädigte Dateien werden sonst mit synchronisiert.

Ein NAS ist eine Investition in deine Daten, Sicherheit und Freiheit.



DEINE DATEN. DEIN ZUHAUSE. DEIN NAS.

Unabhängig von großen Anbietern. Sicher. Flexibel. Zukunftssicher.



KOMBINIERE NAS & CLOUD

Für maximale Sicherheit und Verfügbarkeit: Lokales Backup + Cloud-Backup = Perfekt!

SELF-HOSTED CLOUD

MEHR KONTROLLE. MEHR VERANTWORTUNG.

Dein eigener Cloud-Dienst auf einem NAS oder Server zu Hause, einem gemieteten Server oder bei einem vertrauenswürdigen Host.



DIE VORTEILE



VOLLE KONTROLLE

Du bestimmst selbst Konfiguration, Funktionen und Zugriffsrechte.



INDIVIDUELL ANPASSBAR

Erweiterbar durch Apps, Integrationen und eigene Anforderungen.



AUCH LOKAL NUTZBAR

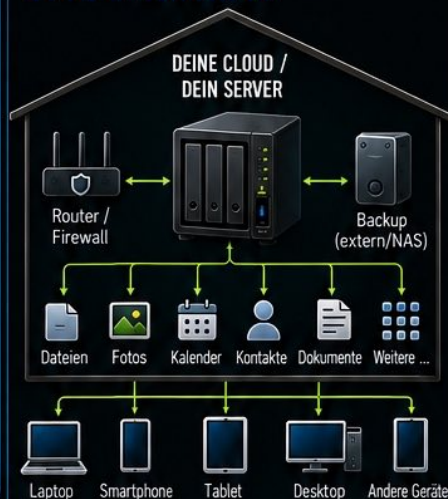
Zugriff im Heimnetz auch ohne Internet möglich.



FREIE ANBIETERWAHL

Bei dir zu Hause, auf einem gemieteten Server oder bei einem vertrauenswürdigen Host.

SO FUNKTIONIERT ES



BEISPIEL-SOFTWARE



Nextcloud

Umfangreiche Kollaborationsplattform für Dateien, Kalender, Kontakte, Notizen u. v. m.



ownCloud

Bewährte Lösung für Dateisynchronisation und gemeinsame Nutzung.



Seafile

Schnelle und effiziente Dateisynchronisation, ideal für Teams.



Pydio Cells

Modulare Plattform mit Fokus auf Sicherheit und Enterprise-Umgebungen.



Filebrowser

Leichter Web-Dateimanager für einen einfachen Zugriff auf deine Dateien.



Cloudron

Verwaltungsplattform für Apps inkl. eigener Cloud. Hat ein eigenes Lizenzmodell; keine reine Open-Source-Lösung.

DIE KOSTEN



Strom, Domain, Hardware, Backups sowie Wartung oder Hosting können fortlaufende Kosten verursachen. Plane diese regelmäßig ein.



SICHERER FERNZUGRIFF

Nutze ein VPN oder einen sicher konfigurierten Reverse Proxy (z. B. mit HTTPS).

- ✓ MFA/Passkeys verwenden
- ✓ Nur notwendige Dienste veröffentlichen
- ✓ Unnötige Portweiterleitungen vermeiden



OPEN SOURCE ERHÖHT TRANSPARENZ – SICHERHEIT ENTSTEHT DURCH UPDATES, KONFIGURATION UND KONTROLLE.

DATENSCHUTZ & PRIVATSPHÄRE



Wie privat deine Daten sind, hängt ab von:

- ✓ der eingesetzten Software
- ✓ deiner Konfiguration
- ✓ dem Host (falls nicht selbst betrieben)
- ✓ verwendeten Plugins und Integrationen
- ✓ Log-Dateien und Protokollierung
- ✓ angebundenen Diensten von Drittanbietern

Ein Self-Hosted Setup kann deine Privatsphäre stärken – erfordert aber bewusste Entscheidungen und regelmäßige Prüfung.

EMPFOHLENE HARDWARE



Wähle CPU, RAM und Speicherplatz entsprechend der Anzahl der Nutzer, der gewünschten Apps und der zu erwartenden Auslastung.

- ✓ Für Einsteiger reichen oft NAS-Geräte oder kleine Server.
- ✓ Für mehr Nutzer und Apps sind leistungsstärkere Systeme sinnvoll.
- ✓ Nutze bei Bedarf eine unterbrechungsfreie Stromversorgung (USV), um Ausfälle zu vermeiden.
- ✓ Achte auf zuverlässige und energieeffiziente Hardware.

DEINE VERANTWORTUNG



- ✓ Regelmäßige Updates und Sicherheitspatches einspielen
- ✓ Benutzerkonten und Zugriffsrechte verwalten
- ✓ Zertifikate (z. B. TLS/HTTPS) einrichten und erneuern
- ✓ System und Dienste überwachen (z. B. Logs, Benachrichtigungen)
- ✓ Regelmäßige Backups durchführen
- ✓ Wiederherstellung regelmäßig testen
- ✓ Dokumentation und Notfallpläne pflegen

BACKUPS – UNVERZICHTBAR



Daten können durch Hardware-Defekte, Fehler, Ransomware oder menschliche Irrtümer verloren gehen.



RAID IST KEIN BACKUP.

Nutze eine 3-2-1-Strategie und teste die Wiederherstellung.



TYPISCHE ANWENDUNGSFÄLLE

- ✓ Dateien sicher speichern und teilen
- ✓ Fotos und Videos verwalten
- ✓ Kalender, Kontakte und Aufgaben nutzen
- ✓ Notizen und Dokumente bearbeiten
- ✓ Zusammenarbeit im Team ermöglichen
- ✓ Medien streamen (Musik, Filme)
- ✓ Eigene Apps und Erweiterungen installieren
- ✓ Unabhängiger von großen Anbietern sein



WICHTIGE HINWEISE

- ✓ Sicherheit erfordert kontinuierliche Pflege.
- ✓ Du bist selbst für Updates, Konfiguration und Datensicherheit verantwortlich.
- ✓ Internetverbindung für Fernzugriff nötig (bei lokalem Zugriff nicht erforderlich).
- ✓ Hardware kann ausfallen – Backups sind wichtig.
- ✓ Ein besseres Verständnis der Technik ist hilfreich.
- ✓ Je nach Einsatz können gesetzliche Anforderungen gelten (z. B. DSGVO).



MEHR KONTROLLE BEDEUTET MEHR VERANTWORTUNG.



CLOUD vs. NAS

WAS IST BESSER FÜR DICH?



Zwei Wege, deine Daten sicher zu speichern – welcher passt zu dir?
Es gibt nicht die eine richtige Lösung – es kommt auf deine Bedürfnisse an.



CLOUD

Online-Speicher bei einem Anbieter



ÜBERALL VERFÜGBAR

Greife von überall über das Internet auf deine Daten zu.



AUTOMATISCHE SYNCHRONISATION

Deine Dateien werden automatisch auf allen Geräten synchronisiert.



EINFACH ZU NUTZEN

Schnelle Einrichtung, ideal zum Teilen und für die Zusammenarbeit.



KEINE EIGENE HARDWARE

Du brauchst keine eigene Hardware und keinen Wartungsaufwand.



LAUFENDE KOSTEN

Meist monatliche oder jährliche Gebühren – abhängig vom Speicherbedarf.

BEISPIELE



DIREKTER VERGLEICH

ZUGRIFF



Überall über das Internet



Lokal im Heimnetz, optional auch von unterwegs (mit Einrichtung)

KONTROLLE



Daten liegen beim Anbieter



Lokale Kontrolle über deine Daten

KOSTEN



Laufende Abo-Kosten



Einmalige Anschaffung, Strom und Wartung

SPEICHERPLATZ



Flexibel erweiterbar



Nach Bedarf erweiterbar (Hardware)

WARTUNG



Wird vom Anbieter übernommen



Du bist für Wartung, Updates und Betrieb verantwortlich

SICHERHEIT



Konto absichern (z. B. 2FA)



Konto absichern (z. B. 2FA) und System aktuell halten

BACKUPS



Zusätzliche Backups empfehlenswert



Zusätzliche Backups empfehlenswert (RAID ist kein Backup)



NAS

Netzwerkspeicher bei dir zu Hause (oder im eigenen Umfeld)



LOKALE KONTROLLE

Deine Daten liegen bei dir und du bestimmst, wer Zugriff hat.



FLEXIBLER ZUGRIFF

Primär im Heimnetz, bei Bedarf auch von unterwegs (z. B. VPN oder Anbieter-Relay).



EINMALIGE ANSCHAFFUNG

Du kaufst die Hardware. Laufende Kosten sind meist gering (Strom, evtl. Dienste).



VIELSEITIG NUTZBAR

Dateien, Backups, Medienserver, Fotos und mehr – ganz nach deinen Bedürfnissen.



AUFWAND UND VERANTWORTUNG

Du bist für Einrichtung, Updates und Sicherheit verantwortlich.



ERWEITERBAR

Speicher und Funktionen lassen sich flexibel anpassen.

BEISPIELE



UND VIELE MEHR

WAS PASST ZU DIR?

DIE CLOUD IST IDEAL FÜR DICH, WENN ...

- ✓ du deine Daten bequem von überall nutzen möchtest.
- ✓ du keine eigene Hardware betreiben willst.
- ✓ du einfach Dateien synchronisieren und teilen möchtest.
- ✓ du flexibel Speicher nach Bedarf nutzen möchtest.
- ✓ du bereit bist, laufende Gebühren zu zahlen.



EIN NAS IST IDEAL FÜR DICH, WENN ...

- ✓ du deine Daten vor allem lokal unter eigener Kontrolle speichern möchtest.
- ✓ du bereit bist, dich um Einrichtung und Wartung zu kümmern.
- ✓ du große Datenmengen langfristig speichern willst.
- ✓ du deine Daten auch ohne Internetzugang nutzen möchtest.
- ✓ du höhere Privatsphäre und Unabhängigkeit schätzt.



HYBRID? DAS BESTE AUS BEIDEN WELTEN!

- ✓ NAS für lokale Speicherung und schnellen Zugriff.
- ✓ Cloud als zusätzliche Sicherung (Offsite-Backup).
- ✓ Praktisch für wichtige Daten, Fotos und Dokumente.
- ✓ Mehr Sicherheit – aber auch mehr Komplexität.



WORAUF ES WIRKLICH ANKOMMT

Die beste Lösung hängt von deinen Fähigkeiten, deinem Budget, der gewünschten Verfügbarkeit und deinen Datenschutz-Anforderungen ab.

SICHERHEITSTIPPS FÜR BEIDE



Starke Passwörter und 2FA



Regelmäßige Updates



Eigene Backups erstellen



DEINE DATEN. DEINE ENTSCHEIDUNG.
VERSTEHEN – VERGLEICHEN – PASSEND NUTZEN.



CLOUD ODER NAS – HAUPTSACHE, DEINE DATEN SIND SICHER.

CLOUD-SICHERHEIT

SO SCHÜTZT DU DEINE DATEN

Deine Daten sind wertvoll – egal wo sie liegen.
Mit diesen Maßnahmen nutzt du die Cloud sicher und sorgenfrei.



WARUM IST CLOUD-SICHERHEIT WICHTIG?

- Deine Daten sind überall zugreifbar – und damit auch für Angreifer interessant.
- Unsichere Konten, schwache Passwörter oder unverschlüsselte Daten können zu Datenverlust führen.
- Einmal in falsche Hände geraten, sind Daten oft schwer wiederherzustellen.
- Der Schutz deiner Daten liegt nicht nur beim Anbieter – sondern auch bei dir!

DAS GETEILTE VERANTWORTUNGSMODELL

Sicherheit ist Teamarbeit.



DIE GRÖSSTEN RISIKEN

- Schwache oder wiederverwendete Passwörter
- Kein oder fehlender Zwei-Faktor-Schutz (2FA)
- Phishing-Angriffe und betrügerische Webseiten
- Unsichere Geräte und Netzwerke
- Unverschlüsselte oder öffentlich freigegebene Daten
- Fehlende Backups

10 WICHTIGE TIPPS FÜR MEHR CLOUD-SICHERHEIT

1 LANGE, EINZIGARTIGE PASSWÖRTER ODER PASSKEYS



Wenn ein Passwort allein schützt, möglichst mindestens 15 Zeichen. Ein Passwortmanager erzeugt und speichert zufällige Passwörter.

2 ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA) AKTIVIEREN



Nutze nach Möglichkeit Passkeys oder phishing-resistente Sicherheitsschlüssel. Authenticator-Apps sind besser als SMS.

3 PHISHING ERKENNEN UND VERMEIDEN



Klicke nicht auf verdächtige Links und gebe niemals deine Zugangsdaten weiter.

4 GERÄTE UND SOFTWARE AKTUELL HALTEN



Updates schließen Sicherheitslücken und schützen vor bekannten Bedrohungen.

5 SICHERE VERBINDUNGEN NUTZEN



HTTPS prüfen, automatische Verbindungen vermeiden und sensible Zugriffe nur über vertrauenswürdige Netze ausführen. Ein seriöses VPN kann zusätzlichen Schutz im lokalen Netz bieten, ersetzt aber weder HTTPS noch Kontosicherheit.

6 DATEN VERSCHLÜSSELN



Der Anbieter verschlüsselt deine Daten in der Regel bei der Übertragung und auf seinen Systemen. Für maximalen Schutz nutze Ende-zu-Ende-Verschlüsselung mit selbst verwalteten Schlüsseln (z. B. mit Cryptomator oder VeraCrypt).

7 FREIGABEN BEWUSST EINSETZEN



Teile nur, was notwendig ist. Nutze starke Berechtigungen und überprüfe sie regelmäßig.

8 BACKUPS NICHT VERGESSEN



Verlasse dich nicht nur auf die Cloud. Regelmäßige Backups schützen vor Datenverlust.

9 AKTIVITÄTEN UND GERÄTE IM BLICK BEHALTEN



Überprüfe regelmäßig Anmeldeaktivitäten und entferne unbekannte Geräte.

10 SENSIBLE DATEN BESONDERS SCHÜTZEN



Finanzdaten, Ausweise oder Gesundheitsdaten gehören nicht unverschlüsselt in die Cloud.

VERSCHLÜSSELUNG – DEINE EXTRA-SCHICHT

Verschlüsselung sorgt dafür, dass nur du auf deine Daten zugreifen kannst – nicht einmal der Anbieter.



Deine Datei



Verschlüsselt



In der Cloud gespeichert

Empfohlene Tools:



Cryptomator



VeraCrypt

SICHERE GERÄTE – SICHERE CLOUD

Dein Gerät ist der Schlüssel zu deiner Cloud.

- Bildschirm sperren (PIN, Passwort, biometrisch)
- Festplattenverschlüsselung aktivieren
- Firewall und Virenschutz nutzen
- Nur vertrauenswürdige Apps installieren
- Verlorene Geräte können aus der Ferne gesperrt oder gelöscht werden

CLOUD-SICHERHEIT CHECKLISTE

- Starkes Passwort verwendet
- Zwei-Faktor-Authentifizierung aktiv
- Phishing-Mails erkannt und gemieden
- Geräte und Software aktuell
- Daten verschlüsselt (sofern sensibel)
- Freigaben überprüft
- Backups vorhanden
- Aktivitäten regelmäßig geprüft



WICHTIG ZU WISSEN



100 % Sicherheit gibt es nicht. Aber mit den richtigen Maßnahmen reduzierst du Risiken erheblich.



Cloud-Anbieter investieren massiv in Sicherheit – dennoch bleibt deine Eigenverantwortung entscheidend.



Ein sicherer Umgang macht die Cloud zu einem der besten Werkzeuge unserer Zeit.

MERKE DIR:

„Die Cloud ist sicher – wenn du sicher handelst.“



SICHERE GEWOHNHEITEN. STARKE PASSWÖRTER. REGELMÄSSIGE BACKUPS.
SO NUTZT DU DIE CLOUD MIT GUTEM GEFÜHL.





CRYPTOMATOR

DEINE DATEN. NUR FÜR DICH.

Cryptomator ist eine Open-Source-Software, die deine Dateien mit Ende-zu-Ende-Verschlüsselung auf deinem Gerät schützt, bevor sie in die Cloud hochgeladen werden. So bleiben deine Daten privat – egal, welchem Anbieter du vertraust.

AUF EINEN BLICK

- ✓ Open-Source & transparent
- ✓ Ende-zu-Ende-Verschlüsselung (auf deinem Gerät)
- ✓ Für Windows, macOS, Linux, Android, iOS
- ✓ Einfache Bedienung
- ✓ Funktioniert mit vielen Cloud-Anbietern
- ✓ Ideal für die sichere Speicherung sensibler Daten

WIE FUNKTIONIERT CRYPTOMATOR?

DEINE DATEIEN AUF DEM GERÄT



Du wählst Dateien oder Ordner, die du schützen möchtest.

CRYPTOMATOR ERSTELLT EINEN VAULT



Deine Daten werden lokal in einem verschlüsselten Vault (Dateistruktur) vorbereitet – mit deinem Passwort.

HOCHLADEN IN DIE CLOUD



Der verschlüsselte Vault wird in deiner Cloud gespeichert. Die Dateien liegen dort nur eingeschlüsselt vor und sind ohne dein Passwort nutzlos.

ZUGRIFF NUR MIT DEINEM PASSWORT



Nur mit deinem Passwort kann der Vault auf deinem Gerät entschlüsselt und genutzt werden.

WAS DEIN ANBIETER SEHEN KANN



Die Existenz deines Vaults und verschlüsselter Dateien.



Zeitpunkte von Uploads, Downloads und Änderungen.



Ungefähre Datenmengen (Dateigrößen).



Keine Einsicht in den Inhalt deiner Dateien (ohne Passwort).

INSTALLATION – SO GEHT'S



Windows

1. Cryptomator von cryptomator.org herunterladen.
2. Installation starten.
3. App öffnen und einrichten.



macOS

1. Cryptomator für macOS herunterladen.
2. Installationsdatei öffnen und Cryptomator in den Programme-Ordner ziehen.
3. App starten und einrichten.



Linux

1. Passende Version (AppImage, .deb oder .rpm) herunterladen.
2. Datei ausführbar machen.
3. App starten und einrichten.



Android

1. App im Google Play Store herunterladen.
2. App installieren und einrichten.



iOS (iPhone/iPad)

1. App im App Store herunterladen.
2. App installieren und einrichten.

UNTERSTÜTZTE CLOUDS



Dropbox



Google Drive



Microsoft OneDrive



Apple iCloud Drive



Box



WebDAV, Nextcloud u. v. m.

Funktioniert mit nahezu jedem Cloud-Speicher oder Server, der Standardprotokolle unterstützt.

VAULT EINRICHTEN UND SICHER NUTZEN – IN 6 SCHRITTEN

1

VAULT ERSTELLEN

Neuen Tresor erstellen

Tresor-Name
MeineDaten

Abbrechen Weiter

- Wähle einen aussagekräftigen Namen.
- Lege den Speicherort in deiner Cloud fest (z. B. Dropbox, Google Drive).

2

STARKES PASSWORT WÄHLEN

Passwort festlegen

.....

Weiter

- Verwende ein langes, einzigartiges Passwort oder eine Passphrase.
- Keine erzwungenen Sonderzeichen nötig – entscheidend ist die Länge und Einzigartigkeit.

3

DATEIEN HINZUFÜGEN



- Öffne den Vault wie einen normalen Ordner.
- Lege Dateien ab, bearbeite sie oder lösche sie – sie werden automatisch verschlüsselt.

4

VAULT VERWENDEN



- Deine Daten werden synchronisiert und bleiben in der Cloud verschlüsselt.
- Auf anderen Geräten öffnest du den Vault einfach mit demselben Passwort.

5

AUF ANDEREN GERÄTEN



- Cryptomator auf weiteren Geräten installieren.
- Vault verbinden und dein Passwort eingeben.
- Greife sicher auf deine Dateien zu – überall.

6

FERTIG – UND WAS NOCH?



- Wenn du fertig bist, sperre den Vault.
- Der Vault wird dann nicht mehr im Klartext angezeigt.
- Schließe die App bei Nichtgebrauch.

BEST PRACTICES FÜR MAXIMALE SICHERHEIT



LANGES, EINZIGARTIGES PASSWORT

Nutze eine lange Passphrase. Verwende für jeden Vault ein eigenes Passwort.



RECOVERY-KEY SICHER AUFBEWAHREN

Falls du einen Recovery-Key verwendest, bewahre ihn offline und sicher auf (z. B. Passwort-Manager oder ausgedruckt).



SOFTWARE AKTUELL HALTEN

Installiere regelmäßig Updates, um von Fehlerbehebungen und Sicherheitsverbesserungen zu profitieren.



WIEDERHERSTELLUNG TESTEN

Überprüfe regelmäßig, ob du deinen Vault mit Passwort (und ggf. Recovery-Key) öffnen kannst.



ZUSÄTZLICHE BACKUPS ERSTELLEN

Cryptomator ist kein Backup. Lege unabhängige Backups deiner wichtigen Daten an (z. B. zusätzlich auf einer anderen Cloud oder externen Festplatte).

WICHTIGE HINWEISE



KEIN BACKUP

Cryptomator schützt deine Daten vor unbefugtem Zugriff, ist aber kein Backup. Gelöschte oder verlorene Dateien können nicht wiederhergestellt werden.



KEIN SCHUTZ VOR MALWARE

Ein geöffneter Vault ist auf deinem Gerät im Klartext verfügbar. Malware, ein kompromittiertes Gerät oder ein anderer unbefugter Zugriff können deine Daten lesen oder verändern.



METADATEN BLEIBEN SICHTBAR

Dein Cloud-Anbieter kann u. a. die Existenz, Zeitpunkte von Zugriffen und ungefähre Dateigrößen sehen, aber nicht den Inhalt deiner Dateien.



SENSIBLE DATEN BEWAHRT SCHÜTZEN

Behandle Passwörter, Recovery-Keys und deine Geräte sorgfältig.

ZUSÄTZLICHE TIPPS



VAULT AN GESCHÜTZTEM ORT

Speichere deinen Vault in einem vertrauenswürdigen Cloud-Konto.



GERÄTESICHERHEIT

Nutze Geräte-Sperre (z. B. PIN, biometrisch) und halte dein System aktuell.



PASSWORT-MANAGER

Ein Passwort-Manager hilft dir, sichere und einzigartige Passwörter zu verwalten.



MEHRERE CLOUDS KOMBINIEREN

Nutze z. B. eine zweite Cloud als Backup oder für zusätzliche Redundanz.



OPEN SOURCE

Der Quellcode ist öffentlich einsehbar – für unabhängige Prüfung und mehr Sicherheit.

KURZ ZUSAMMENGEFASST



Cryptomator installieren



Vault erstellen und Passwort wählen



Verschlüsseln und hochladen



Auf allen Geräten nutzen



Zusätzliches Backup erstellen



FAZIT

Cryptomator macht deine Cloud sicher – mit starker Verschlüsselung, einfacher Bedienung und transparentem Code. Es schützt deine Privatsphäre, ist aber kein Backup und kann dich nicht vor einem kompromittierten Gerät schützen.

DEINE DATEN. NUR FÜR DICH.



VERACRYPT

DEINE DATEN. DEIN SCHUTZ.

VeraCrypt ist eine kostenlose Open-Source-Software zur starken Verschlüsselung von Dateien, Laufwerken und Partitionen. Sie schützt vertrauliche Daten vor neugierigen Blicken – selbst wenn dein Gerät verloren geht oder in falsche Hände gerät.

Starke Verschlüsselung Open Source & geprüft Plattformübergreifend Einfache Bedienung

AUF EINEN BLICK

- ✓ Verschlüsselt Dateien, Container, Laufwerke und gesamte Systeme (unterstützte Windows-Systeme)
- ✓ Starke und bewährte Algorithmen (AES, Serpent, Twofish u.a.)
- ✓ Open Source, sicher und frei nutzbar
- ✓ Schützt ruhende Daten vor unbefugtem Zugriff
- ✓ Ideal für Privatpersonen, Profis und Unternehmen
- ✓ Regelmäßig geprüft und aktiv weiterentwickelt

WAS IST VERACRYPT?

VeraCrypt ist der Nachfolger von TrueCrypt und wird aktiv weiterentwickelt. Es ermöglicht dir, sensible Daten in einem verschlüsselten Container zu speichern oder gesamte Laufwerke/Partitionen zu verschlüsseln.



WARUM VERACRYPT NUTZEN?

- ✓ Schützt deine Daten im Ruhezustand (at rest)
- ✓ Bewahrt deine Daten bei Verlust oder Diebstahl deines Geräts vor unbefugtem Zugriff
- ✓ Ohne den richtigen Schlüssel (Passwort, PIM, Keyfiles) sind die Daten offline praktisch nicht zugänglich
- ⚠ **SCHÜTZT NICHT VOR MALWARE BEI GEÖFFNETEM VOLUME.**
Sobald ein Volume eingebunden ist, können Programme mit deinen Benutzerrechten auf die Dateien zugreifen.

WAS KANN VERACRYPT VERSCHLÜSSELN?

- Datei-Container**
Verschlüsselte Dateien, die wie normale Dateien funktionieren (z. B. für Dokumente, Fotos)
- Laufwerke & Partitionen**
Verschlüsselt ganze Partitionen oder externe Laufwerke/USB-Sticks
- Systemverschlüsselung**
Verschlüsselt das komplette Systemlaufwerk – für unterstützte Windows-Systeme (nicht für macOS oder Linux)

VERACRYPT PERFEKT NUTZEN – IN 7 SCHRITTEN

1 VERACRYPT HERUNTERLADEN



Lade VeraCrypt nur von der offiziellen Website herunter: veracrypt.fr

Wähle die passende Version für dein Betriebssystem.

2 CONTAINER ODER LAUFWERK WÄHLEN



Entscheide, ob du einen Datei-Container erstellen oder ein Laufwerk/Partition/Systemlaufwerk (Windows) verschlüsseln möchtest.

3 VOLUME ERSTELLEN UND SPEICHERORT



- Speicherort wählen
- Dateinamen vergeben
- Größe festlegen (z. B. 10 GB)
- Weitere Optionen bei Bedarf

4 VERSCHLÜSSELUNGSOPTIONEN FESTLEGEN



- Einen starken Algorithmus wählen (z. B. AES)
- Hash-Algorithmus (z. B. SHA-512)
- Standard-Einstellungen sind in der Regel sinnvoll

5 STARKES PASSWORT FESTLEGEN



- Verwende eine lange, außergewöhnliche Passphrase
- Optional: PIM oder Keyfiles für zusätzliche Sicherheit

6 FORMATIEREN (VOLUME ERSTELLEN)



- Bewege die Maus im Fenster, um die Zufallsdaten zu erhöhen
- Nach Abschluss ist das Volume einsatzbereit

7 VOLUME EINBINDEN UND NUTZEN



- Container auswählen
- Passwort eingeben
- Auf „Mount“ klicken
- Im Datei-Explorer wie ein normales Laufwerk nutzen

VERSTECKTE VOLUMES – PLAUSIBLE ABSTREITBARKEIT

Mit VeraCrypt kannst du versteckte Volumes erstellen. Dabei befindet sich ein zusätzliches, verstecktes Volume innerhalb eines äußeren Volumes. So kannst du bei Zwang oder Kontrolle plausibel bestreiten, dass weitere Daten existieren. Das bietet keinen absoluten Schutz vor forensischer Analyse, allen Szenarien staatlicher Ermittlungen oder Zwangsmaßnahmen, erhöht aber die Privatsphäre in vielen Situationen.



WICHTIG: Verliere niemals das Passwort des versteckten Volumes! Es kann nicht wiederhergestellt werden.

BEST PRACTICES

- ✓ Verwende eine lange, einzigartige Passphrase (mehrere zufällige Wörter).
- ✓ Nutze bei Bedarf PIM oder Keyfiles.
- ✓ Bewahre Backup-Keyfiles sicher und getrennt auf.
- ✓ Sichere wichtige Volume-Header (z. B. auf einem separaten Medium).
- ✓ Erstelle einen Wiederherstellungsplan für den Verlust von Passwörtern oder Keyfiles.
- ✓ Halte VeraCrypt und dein System aktuell.
- ✓ Nutze nur vertrauenswürdige Computer und sichere Umgebungen.

WANN VERACRYPT NUTZEN?

- Für private Dokumente, Finanzen, Verträge oder persönliche Daten
- Wenn du Daten auf externen Datenträgern speicherst oder Geräte mitführst
- Für sichere USB-Sticks und externe Festplatten
- Für Unternehmen: Schutz vertraulicher Daten und Compliance-Anforderungen
- Für Journalistinnen, Whistleblower und alle, die ihre Privatsphäre schützen wollen

UNTERSTÜTZTE BETRIEBSSYSTEME



Aktuelle unterstützte Windows-, macOS- und Linux-Versionen laut VeraCrypt-Dokumentation prüfen.

STARKE VERSCHLÜSSELUNGsalgorithmen

AES (Advanced Encryption Standard) Sehr sicher und weit verbreitet	Serpent Sehr sicher und flexibel	Twofish Schnell und effizient	Kombinationen Für maximale Sicherheit kombinierbar
Hash-Algorithmen: SHA-512, Whirlpool, SHA-256, Streebog u. a.			

WICHTIGE FEATURES

- Echtzeit-verschlüsselung
- Versteckte Volumes
- Sichere Algorithmen
- Open Source & transparent



FAZIT

VeraCrypt ist ein mächtiges, zuverlässiges und kostenloses Tool, um deine Daten wirksam zu schützen. Ob Dateien, Laufwerke oder ganze Systeme – mit VeraCrypt bleiben deine Daten in deinen Händen. Open Source. Sicher. Zuverlässig.



MEHR INFOS & DOWNLOAD

veracrypt.fr

Open Source. Sicher. Zuverlässig.



GUT ZU WISSEN

STARKE VERSCHLÜSSELUNG SCHÜTZT RUHENDE DATEN – NICHT EIN BEREITS ENTSCHLÜSSELTES SYSTEM.



CYBERDUCK

DER DATEI-TRANSFER CLIENT.

Cyberduck ist ein kostenloser und quelloffener Client, mit dem du einfach und sicher auf Server und Cloud-Speicher zugreifen kannst. Du kannst Dateien hochladen, herunterladen, bearbeiten, löschen und verwalten – flexibel über verschiedene Protokolle und Dienste.

Sicherer Zugriff Zeit sparen Dateien einfach verwalten Überall arbeiten

AUF EINEN BLICK

- ✓ Kostenlos & Open Source
- ✓ Unterstützt viele Protokolle & Clouds
- ✓ Für Windows und macOS
- ✓ Einfache & intuitive Bedienung
- ✓ Sichere Verbindungen (TLS/SSL, SSH)
- ✓ Cryptomator-Integration (wo unterstützt)
- ✓ Regelmäßige Updates durch Community



Deine Dateien.
Deine Kontrolle.

WAS IST CYBERDUCK?

Cyberduck ist in erster Linie ein Open-Source-Datei-Transfer- und Browser-Client. Er verbindet deinen Computer mit Servern und Cloud-Speichern über verschiedene Protokolle, damit du Dateien bequem verwalten kannst. **Cyberduck ist kein automatisches Synchronisations- oder Backup-Tool.**



WOFÜR KANNST DU CYBERDUCK NUTZEN?

- ✓ Auf Webserver und Cloud-Speicher zugreifen (FTP, SFTP, WebDAV u. v. m.)
- ✓ Dateien sicher übertragen (hoch- und herunterladen)
- ✓ Dateien direkt im Remote-Speicher bearbeiten
- ✓ Mehrere Verbindungen, Lesezeichen und Konten verwalten
- ✓ Mit Cryptomator-Tresoren arbeiten (sofern vom jeweiligen Dienst unterstützt)

Cyberduck synchronisiert deine Dateien nicht automatisch. Für automatische Sync- oder Backup-Funktionen nutze bitte spezielle Tools.

UNTERSTÜTZTE PROTOKOLLE & DIENSTE (Auswahl)

SFTP (SSH) FTP / FTPS WebDAV
S3 (Amazon S3) Google Drive Dropbox
Microsoft OneDrive Box Backblaze B2
OpenStack Swift und viele mehr ...

Die Liste der Dienste wird regelmäßig erweitert und kann sich mit neuen Versionen ändern.

S3 Google Drive Dropbox OneDrive Backblaze B2

IN 6 SCHRITTEN EINFACH EINRICHTEN UND NUTZEN

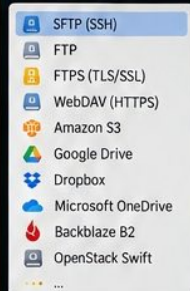
1 CYBERDUCK HERUNTERLADEN



Lade Cyberduck von der offiziellen Website herunter:
<https://cyberduck.io>

- ✓ Für Windows und macOS
- ✓ Kostenlos und Open Source
- ✓ Keine Zusatzsoftware nötig

2 VERBINDUNG ERSTELLEN



Protokoll oder Cloud-Dienst auswählen und Verbindungsinformationen eingeben.

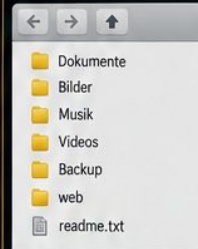
3 VERBINDUNG KONFIGURIEREN

Server:
Port:
Benutzername:
Passwort:
☐ Anonyme Anmeldung
☒ Im Schlüsselbund speichern

Verbinden

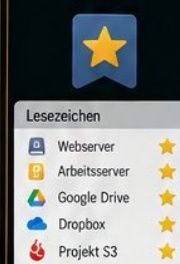
Serveradresse, Port und Zugangsdaten eingeben. Beispiel: SFTP verwendet standardmäßig Port 22.

4 DATEIEN VERWALTEN



- ✓ Dateien hoch- und herunterladen
- ✓ Ordner erstellen, umbenennen, löschen
- ✓ Dateien direkt bearbeiten
- ✓ Drag & Drop verwenden

5 LESEZEICHEN SPEICHERN



- ✓ Verbindungen als Lesezeichen speichern
- ✓ Schnell wieder verbinden
- ✓ Übersichtlich organisieren

6 CRYPTOMATOR NUTZEN (OPTIONAL)



Cyberduck kann – wo unterstützt – mit Cryptomator-Tresoren arbeiten. So kannst du verschlüsselte Ordner wie normale Speicherorte einbinden.

Die Ende-zu-Ende-Verschlüsselung erfolgt durch Cryptomator und nicht durch Cyberduck. Die Unterstützung kann je nach Dienst variieren.

SICHERHEITSTIPPS

- Nur von der offiziellen Website laden
Verwende <https://cyberduck.io>
- Host-Schlüssel und Zertifikate prüfen
Beim ersten Verbinden den SSH-Host-Key bzw. das TLS-Zertifikat kontrollieren.
- Zugangsdaten sicher speichern
Nutze den macOS-Schlüsselbund bzw. den Windows-Anmeldeinformationsspeicher.
- Immer aktuell halten
Regelmäßig Updates installieren.
- Starke Passwörter oder Schlüssel verwenden
Nach Möglichkeit SSH-Schlüssel und Zwei-Faktor-Authentifizierung beim Dienst nutzen.

PRAKTISCHE TIPPS FÜR DEN ALLTAG

- Parallele Verbindungen
Öffne mehrere Fenster oder Tabs, um verschiedene Server gleichzeitig zu nutzen.
- Integrierte Suche
Dateien schnell finden und filtern.
- Remotebearbeitung
Dateien direkt bearbeiten (sofern der Dienst dies erlaubt).
- Große Dateien zuverlässig übertragen
Unterbrochene Transfers können automatisch fortgesetzt werden.
- Individuelle Einstellungen
Speichere Verbindungsprofile, wähle passende Übertragungsmodi und passe die Oberfläche an deine Bedürfnisse an.

SEPARATE BACKUPS EMPFOHLEN

Cyberduck ist **kein** Backup-Tool. Er erstellt keine automatischen Sicherungen und keine Versionshistorie deiner Dateien. Nutze ein separates Backup-Konzept, um deine wichtigen Daten zusätzlich zu sichern (z. B. lokale Backups, Cloud-Backups oder Versionierung beim Anbieter).

SYSTEMVORAUSSETZUNGEN

macOS 10.14 oder neuer Windows 10/11 (64-Bit)

Die genauen Anforderungen können je nach Version variieren. Aktuelle Informationen findest du auf der Cyberduck-Website.



FAZIT

Cyberduck ist ein leistungsfähiger, quelloffener Datei-Transfer-Client für Protokolle und Cloud-Dienste. Er ist einfach zu bedienen, sicher und flexibel – ideal, um deine Dateien überall zu verwalten. Für automatische Synchronisation oder Backups nutze bitte separate Lösungen.



MEHR INFOS & DOWNLOAD
<https://cyberduck.io>
Open Source. Für alle.





MOUNTAIN DUCK

DEINE CLOUDS. ALS LAUFWERK.

Mountain Duck ist eine kommerzielle Desktop-Anwendung von iterate GmbH. Sie bindet Server und Cloud-Speicher als Laufwerk im Finder oder Datei-Explorer ein. Basierend auf den bewährten Cyberduck-Technologien, aber ein separates, kostenpflichtiges Produkt.

AUF EINEN BLICK

- ✓ Server und Cloud-Speicher als Laufwerk
- ✓ Dateien direkt mit deinen Apps öffnen
- ✓ Unterstützt viele Protokolle und Anbieter
- ✓ Optionale Synchronisation & Offline-Caching
- ✓ Sicher und flexibel einsetzbar
- ✓ Kostenpflichtige Lizenz; aktuelle Preise und Bedingungen beim Hersteller prüfen.



WAS IST MOUNTAIN DUCK?

Mountain Duck bindet Server und Cloud-Speicher als Laufwerk in den Finder (macOS) oder Datei-Explorer (Windows) ein. Du arbeitest mit den Dateien wie auf einer lokalen Festplatte – öffnen, bearbeiten, speichern und verschieben – mit deinen gewohnten Anwendungen.



WOFÜR KANNST DU ES NUTZEN?

- ✓ SFTP, FTP/FTPS, WebDAV und zahlreiche Cloud- und Objektspeicher einbinden
- ✓ Dateien direkt mit normalen Anwendungen öffnen und bearbeiten
- ✓ Nahtlose Integration in Finder und Datei-Explorer
- ✓ Optionale Smart Synchronisation und Offline-Caching (je nach Konfiguration)
- ✓ Mehrere Konten und Verbindungen gleichzeitig
- ✓ Ideal für Remote-Arbeit, Teams und Projekte

UNTERSTÜTZTE PROTOKOLLE & DIENSTE

Protokolle

SFTP

FTP / FTPS

WebDAV

Ausgewählte Cloud- und Objektspeicher



Amazon S3



Microsoft Azure



Google Cloud



Dropbox



OneDrive



Backblaze B2



OpenStack Swift

... und viele weitere Anbieter

IN 6 SCHRITTEN DEINE CLOUD ALS LAUFWERK EINBINDEN

1 MOUNTAIN DUCK HERUNTERLADEN & INSTALLIEREN



- Lade Mountain Duck von der offiziellen Website herunter: mountain-duck.io
- Für Windows und macOS
- Einfach installieren und starten

2 VERBINDUNG ERSTELLEN

- ✓ SFTP
- ✓ FTP / FTPS
- ✓ WebDAV
- ✓ Amazon S3
- ✓ Microsoft Azure
- ✓ Google Cloud
- ✓ Dropbox
- ✓ OneDrive
- ✓ Backblaze B2
- ✓ OpenStack Swift
- ... und weitere

- Wähle das gewünschte Protokoll oder den Dienst
- Verbindungsdaten eingeben

3 SICHER VERBINDEN

Server:
Port:
Benutzername:
Passwort:
☒ Zertifikate / Host Keys prüfen
☒ Anmeldung im Schlüsselbund speichern

- Bevorzuge SFTP oder HTTPS
- MFA/OAuth nutzen, wenn unterstützt

4 LAUFWERK EINBINDEN



- Erscheint als normales Laufwerk im Explorer oder Finder
- Sofort mit deinen Anwendungen arbeiten

5 DATEIEN NUTZEN



- Dateien öffnen, bearbeiten, speichern und verschieben
- Änderungen werden auf den Server/Cloud übertragen (je nach Synchronisation)

6 VERBINDUNGEN VERWALTEN



- Nicht benötigte Verbindungen trennen
- Lokalen Cache verwalten
- Synchronisationsoptionen anpassen

VORTEILE

- ✓ Bequeme Integration in Finder und Datei-Explorer
- ✓ Direktes Arbeiten mit Dateien in vertrauten Anwendungen
- ✓ Unterstützung vieler Protokolle und Cloud-Anbieter
- ✓ Optionale Synchronisation und Offline-Caching
- ✓ Mehrere Konten gleichzeitig
- ✓ Ideal für Zusammenarbeit, Remote-Arbeit und gemischte Umgebungen

SICHERHEITSTIPPS

- ✓ Bevorzuge SFTP oder HTTPS.
- ✓ Zertifikate und Host Keys überprüfen.
- ✓ Zugangsdaten im Betriebssystem-Schlüsselbund oder einem Passwort-Manager speichern.
- ✓ MFA/OAuth nutzen, wenn vom Anbieter unterstützt.
- ✓ Nicht benötigte Verbindungen trennen.
- ✓ Geräte und Anwendungen aktuell halten.

WICHTIGE HINWEISE

- ⚠ **Kein automatisches Backup**
Ein eingebundener Cloud-Speicher ist kein Backup. Gelöschte oder verschlüsselte Dateien (z. B. durch Ransomware) können über die Synchronisation auch in der Cloud entfernt oder verändert werden.
- ⓘ **Separate, versionierte Backups**
Nutze zusätzliche, versionierte Backups, um dich vor Datenverlust zu schützen.
- ⓘ **Abhängigkeiten beachten**
Die Verfügbarkeit und Geschwindigkeit hängen von Netzwerk, Anbieter und lokalem Cache ab.
- 📄 **Kostenpflichtige Lizenz**
Mountain Duck ist ein kommerzielles Produkt. Aktuelle Preise und Bedingungen beim Hersteller prüfen.

SYSTEMVORAUSSETZUNGEN



Aktuelle Anforderungen für Windows und macOS unter mountain-duck.io

TYPISCHE EINSATZBEREICHE



Remote-Arbeit



Teams & Projekte



Unternehmen & Bildung



Cloud-Migration & Datenzugriff

GUT ZU WISSEN



Mountain Duck basiert auf den Cyberduck-Technologien, ist aber ein separates, eigenständiges und kostenpflichtiges Produkt der iterate GmbH.



CLOUD ALS LAUFWERK – KOMFORTABEL, ABER KEIN BACKUP.



DIE PERFEKTE CLOUD FÜR ZUHAUSE

MEIN SICHERES, FLEXIBLES SETUP

PRAKTISCH. SICHER. SELBSTBESTIMMT.

Eine bewährte Kombination aus Komfort, Schutz und Kontrolle über deine Daten.



DEINE DATEN.
DEIN ZUHAUSE.
DEINE ENTSCHEIDUNG.

MEIN PERSÖNLICHES CLOUD-SETUP (BEISPIEL)

- 1 GEEIGNETEN CLOUD-ANBIETER WÄHLEN**
Z. B. Microsoft OneDrive, Google Drive, Dropbox oder ein europäischer Anbieter. Achte auf Datenschutz, Zuverlässigkeit und Funktionen, die zu dir passen.
- 2 EINZIGARTIGES PASSWORT & 2FA**
Nutze ein starkes, einzigartiges Passwort und aktiviere Passkeys oder Zwei-Faktor-Authentifizierung (2FA), z. B. mit einer Authenticator-App oder einem Sicherheitsschlüssel.
- 3 BEWUSST TEILEN**
Teile nur mit vertrauten Personen. Nutze Berechtigungen (nur ansehen/ bearbeiten) und entferne geteilte Links, wenn sie nicht mehr benötigt werden.
- 4 SENSIBLE DATEN ZUSÄTZLICH LOKAL VERSCHLÜSSELN**
Für besonders vertrauliche Dateien nutze eine Ende-zu-Ende-Verschlüsselung auf deinem Gerät (z. B. mit VeraCrypt oder Cryptomator), bevor du sie in die Cloud lädst.
- 5 AUTOMATISCH SYNCHRONISIEREN**
Installiere die Cloud-Apps auf allen Geräten. Deine Daten werden automatisch synchronisiert und sind überall aktuell verfügbar.
- 6 UNABHÄNGIGES BACKUP NACH 3-2-1**
Bewahre zusätzlich mindestens 3 Kopien auf: 1x auf deinem Gerät, 1x lokal (externe Festplatte oder NAS) und 1x an einem anderen Ort (z. B. Cloud-Speicher oder zweite Festplatte).
- 7 WIEDERHERSTELLUNG TESTEN**
Überprüfe regelmäßig, ob sich deine Daten wirklich wiederherstellen lassen – nur so ist dein Backup im Ernstfall verlässlich.

WARUM DIESES SETUP?

- | | | | |
|--|---|---|--|
|
SICHERHEIT
Mehr Schutz durch 2FA, Verschlüsselung und unabhängige Backups. |
FLEXIBILITÄT
Zugriff auf deine Daten überall – auf allen Geräten. |
KOMFORT
Automatische Synchronisation im Alltag. |
KONTROLLE
Du entscheidest, was du teilst und wie deine Daten gesichert sind. |
|--|---|---|--|

ZUSÄTZLICHE TIPPS

- ✓ Nutze einen Passwort-Manager.
- ✓ Aktiviere Benachrichtigungen für Kontoaktivitäten.
- ✓ Achte auf Phishing-Mails und verdächtige Links.
- ✓ Ordne und überprüfe deine Freigaben regelmäßig.
- ✓ Entrümpel alte Dateien und behalte den Überblick.



EMPFOHLENE TOOLS (BEISPIELE)

- Cloud-Anbieter:** OneDrive, Google Drive, Dropbox, oder europäische Anbieter wie z. B. IONOS, pCloud
- Verschlüsselung:** Cryptomator, VeraCrypt
- 2FA/Passkeys:** Authenticator-Apps, YubiKey
- Lokaler Speicher:** Externe Festplatte oder NAS

FAZIT

Keine einzelne Maßnahme macht deine Daten unverwundbar. Aber die richtige Kombination bietet einen sehr guten Schutz – für ein sicheres, entspanntes und selbstbestimmtes digitales Leben.



DEINE DATEN. DEINE ENTSCHEIDUNG. DEINE VERANTWORTUNG.



DIE 10 GOLDENEN REGELN FÜR CLOUD-NUTZER

- 1 BEWUSSTEN ANBIETER WÄHLEN**
Setze auf einen seriösen Anbieter mit starken Sicherheitsstandards und klaren Datenschutzrichtlinien. Ein europäischer Anbieter kann zusätzliche Vorteile bieten.
- 2 EINZIGARTIGES PASSWORT & PASSKEY/2FA**
Verwende für dein Cloud-Konto ein starkes, einmaliges Passwort und aktiviere Passkeys oder 2FA.
- 3 NUR BEWUSST TEILEN**
Teile Dateien nur mit vertrauten Personen, nutze Berechtigungen und entferne alte Freigaben regelmäßig.
- 4 SENSIBLE DATEN VERSCHLÜSSELN**
Verschlüssele besonders vertrauliche Dateien bereits auf deinem Gerät, bevor du sie hochlädst (Client-Side-Verschlüsselung, z. B. Cryptomator oder VeraCrypt).
- 5 SYNCHRONISATION FÜR KOMFORT**
Nutze die automatische Synchronisation auf allen Geräten – das macht den Alltag einfach und bequem.
- 6 UNABHÄNGIGES BACKUP (3-2-1)**
Mindestens 3 Kopien, auf 2 verschiedenen Medien, 1 Kopie an einem anderen Ort (z. B. Cloud oder externer Speicher).
- 7 BACKUPS TESTEN**
Stelle regelmäßig stichprobenartig Daten wieder her, um die Funktionsfähigkeit deiner Backups zu überprüfen.
- 8 UPDATES & WIEDERHERSTELLUNGS-CODES**
Halte Betriebssystem, Cloud-Apps und Sicherheits-Apps aktuell. Bewahre Wiederherstellungscodes (z. B. 2FA-Backup-Codes) an einem sicheren Ort auf.
- 9 ÖFFENTLICHE WLANS MIT AUGENMASS**
HTTPS schützt deine Daten bei der Übertragung. Unbekannte Netzwerke sind dennoch nicht vollständig vertrauenswürdig. Ein VPN kann in einigen Situationen sinnvoll sein – z. B. in fremden WLANS oder auf Reisen – ist aber nicht für alle Nutzer zwingend erforderlich.
- 10 WICHTIG: SYNC, RAID & VERSIONEN SIND KEIN VOLLWERTIGES BACKUP**
Synchronisation schützt nicht vor versehentlichem Löschen, Schadsoftware oder Account-Problemen. Auch RAID ersetzt kein Backup. Versionierungsfunktionen sind nützlich, aber keine Garantie. Nutze immer ein unabhängiges Backup nach dem 3-2-1-Prinzip.



DIE 10 GRÖSSTEN CLOUD-IRRtüMER



Fakten statt Mythen – besser verstehen, sicherer nutzen!

1



“Cloud ist ein Backup.”



Falsch! Die Cloud synchronisiert deine Daten – sie ersetzt kein Backup. Versionierung und Papierkorb können helfen, versehentliche Löschungen oder frühere Versionen wiederherzustellen, ersetzen aber kein separates Backup.

2



„Meine Daten liegen irgendwo im Internet.”



Nicht ganz. Speicherorte, Redundanz und Verfügbarkeit unterscheiden sich je nach Anbieter und Tarif. Deine Daten können in einem oder mehreren Rechenzentren und Ländern liegen – das ist nicht bei allen Anbietern gleich.

3



“Cloud ist unsicher.”



Falsch! Die Cloud kann sicher betrieben werden, aber Konto, Freigaben, Geräte, Anbieter und Verschlüsselung entscheiden über die Sicherheit. Mit starken Passwörtern, Mehrfaktor-Authentifizierung und sinnvollen Einstellungen lässt sich das Risiko deutlich reduzieren.

4



“Ich brauche Internet, sonst komme ich nie mehr an meine Daten.”



Nicht ganz. Viele Dienste bieten offline verfügbaren Zugriff, wenn die Dateien vorher heruntergeladen oder für die Offline-Nutzung markiert wurden. Ohne vorherige Synchronisation ist kein Offline-Zugriff möglich.

5



“Wenn ich eine Datei lösche, ist sie für immer weg.”



Nicht unbedingt! Die meisten Cloud-Dienste bieten einen Papierkorb und oft eine Versionierung. Wie lange gelöschte Dateien aufbewahrt werden und wie viele Versionen verfügbar sind, hängt vom Anbieter und dem gewählten Tarif ab.

6



“Synchronisation schützt vor Datenverlust.”



Falsch! Synchronisation sorgt nur dafür, dass überall der gleiche Stand ist – auch versehentliche Löschungen, Fehler oder Malware werden synchronisiert. Ein separates Backup ist weiterhin wichtig.

7



“Mehrere Clouds machen alles komplizierter.”



Sie können Ausfallsicherheit und Trennung verbessern, erhöhen aber auch Komplexität und Angriffsfläche. Mehrere Clouds sind kein automatischer Sicherheitsgewinn und erfordern eine gute Organisation, klare Prozesse und durchdachte Verwaltung.

8



“Ein NAS ersetzt jede Cloud.”



Nicht ganz! Ein NAS kann Fernzugriff, Synchronisation und Freigabelinks bieten. Sicherheit und Bedienkomfort hängen von Einrichtung, Updates und Dienst ab. Es ersetzt ohne getrennte Kopie ebenfalls kein Backup.

9



“Verschlüsselung ist nur etwas für Firmen.”



Falsch! Verschlüsselung ist auch für Privatpersonen sinnvoll. Viele Anbieter verschlüsseln Daten bei der Übertragung (Transportverschlüsselung) und im Speicher (Verschlüsselung im Ruhezustand). Ende-zu-Ende-Verschlüsselung (E2EE), bei der nur du die Schlüssel hast, ist nicht immer standardmäßig aktiv, aber oft verfügbar.

10



“Kostenlose Clouds reichen immer aus.”



Nicht immer! Kostenlose Tarife können für kleine, private Anforderungen ausreichend sein, Speicherplatz, Funktionen und Limits unterscheiden sich jedoch je nach Anbieter und Tarif. Prüfe, ob dein Bedarf langfristig gedeckt ist und welche Einschränkungen gelten (z. B. Speicher, Freigaben, Support).



FAZIT

Die Cloud ist ein mächtiges Werkzeug – wenn man sie richtig versteht und nutzt.

MYTHEN PRÜFEN. FUNKTIONEN UND TARIFE VERGLEICHEN. BACKUPS GETRENNT PLANEN.



Fazit

Die Cloud ist weder gut noch schlecht. Sie ist ein Werkzeug. Richtig eingesetzt erleichtert sie den Alltag, schützt wichtige Daten und macht den Zugriff von überall möglich. Falsch eingesetzt ersetzt sie jedoch kein Backup und keine durchdachte Datensicherung.

Dieses Buch sollte zeigen, dass Cloud-Technik kein Hexenwerk ist. Mit etwas Grundwissen lassen sich die meisten Fehler vermeiden und die Vorteile sicher nutzen.

Ob Sie sich für iCloud, OneDrive, Google Drive, Dropbox oder eine eigene NAS-Lösung entscheiden, hängt von Ihren persönlichen Anforderungen ab. Eine universell beste Cloud gibt es nicht – wohl aber die Lösung, die am besten zu Ihnen passt.

Wenn Sie nach der Lektüre Ihre Daten bewusster organisieren, regelmäßige Backups erstellen und Ihre Cloud sicher nutzen, dann hat dieses Buch sein Ziel erreicht.

Denn digitale Sicherheit beginnt nicht mit Software – sondern mit Wissen.

Herausgeberangaben



Dieses Booklet dient der allgemeinen Information und Bildung. Trotz sorgfältiger Erstellung kann keine Gewähr für Vollständigkeit und Fehlerfreiheit übernommen werden. Genannte externe Angebote können sich ändern oder eingestellt werden.

Herausgeber

Ralf Schäfer
c/o Autorenglück #87012
Albert-Einstein-Straße 47
02977 Hoyerswerda

booklet@rsausffm.de
<https://rsausffm.de>

Verantwortlich für den Inhalt: Ralf Schäfer
Stand: September 2026



DIGITAL

einfach erklärt

DIE CLOUD VERSTEHEN. SICHER NUTZEN.

Die Cloud ist längst Teil unseres digitalen Alltags. Doch was wird eigentlich gespeichert, wie funktioniert die Synchronisation – und wie bleiben persönliche Daten geschützt?

Dieses Booklet erklärt die wichtigsten Grundlagen verständlich, praxisnah und ohne unnötigen Fachjargon. Es hilft dir, Angebote einzuordnen, typische Fehler zu vermeiden und die passende Lösung für deine eigenen Bedürfnisse zu finden.



DAS ERWARTET DICH

- verständliche Erklärungen
- praktische Sicherheitsregeln
- neutrale Vergleiche
- konkrete Tipps für den Alltag

CLOUD = KOMFORT.
BACKUP = WIEDERHERSTELLBARKEIT.

Für wichtige Daten brauchst du beides.

Verstehen macht sicher.