

ITSikkerhedsGruppen´s

# Cloud Storage

Europæiske muligheder

---

January 19, 2026

# Når politik truer adgangen til dine data

De fleste virksomheder og privatpersoner anvender cloud-løsninger til opbevaring af data. Men prøv at forestille dig, at du fra den ene dag til den anden mister adgangen til vigtige data.

Cloud dækker over tjenester som f.eks. Dropbox, Microsoft365, OneDrive, Google Drive og iCloud-løsninger. Vi bruger dem til at gemme, dele og samarbejde om filer online. Det er nemt og effektivt.

Men vidste du, at mange af de populære platforme er amerikanske og dermed underlagt Cloud Act og præsidentielle beslutninger?

De nuværende trusler og politiske forhold fra USA kræver, at vi genovervejer situationen. Digital afhængighed er et alvorligt pressionsmiddel. Så lad os tale lige ud af posen:

Man bør gen-overveje sit virksomhedssetup, nu!

Dette dokument er dog ikke ment som en kritik af USA. De gør, hvad de mener er bedst i forhold til deres risikobillede. Dokumentet er alene udarbejdet for, at vores kunder skal være klar over de risici og muligheder der er.

## Overvej disse spørgsmål:

- Hvem kan tilgå vores filer og data?
- Hvem kan slette eller blokere vores adgang?
- Har vi den rigtige løsning der matcher compliance-krav?
- Hvad vil det betyde, hvis vi mistede adgangen?
- Hvad vil det betyde, hvis vores data blev kopieret eller kompromitteret?

Her får du derfor nogle alternativer med europæisk forankring:

Navn	Webadresse	Land	Kryptering	Zero-knowledge	Placering af data	Overførsel til tredjelande	Typiske brugere	Særlige egenskaber
<b>Proton Drive</b>	proton.me/drive	Schweiz	E2EE	Ja	EU + CH	Nej	Privat, virksomheder	Open source-klienter, stærk privacy governance
<b>Filen.io</b>	filen.io	Tyskland	E2EE	Ja	EU (DE)	Begrænset (support/analyse)	Privat, SMB	Minimal metadata, open source, analysedata til USA
<b>Tresorit</b>	tresorit.com	Schweiz	E2EE	Ja	EU valgfrit	Nej	Enterprise, myndigheder	Granulær adgang, audit logs
<b>Nextcloud</b>	nextcloud.com	Tyskland	TLS + SSE / E2EE	Afhænger af setup	Selvvalgt	Nej (hvis EU-hostet)	Offentlig sektor	Fuld datakontrol, open source, integration med Office-pakker
<b>Internxt</b>	internxt.com	Spanien	E2EE	Ja	EU	Nej	Privat, SMB	Decentral arkitektur
<b>Jottacloud</b>	jottacloud.com	Norge	TLS + SSE	Nej	Norge / EU	Nej	Privat, erhverv	Norsk lovgivning, enkel backup
<b>Koofr</b>	koofr.eu	Slovenien	TLS + klient-	Delvist	EU	Nej	Privat, SMB	Ingen tracking, EU-only

			side (Vault)					
<b>pCloud (EU)</b>	pcloud.com	Schweiz	TLS + klient-side (Crypto)	Valgfrit	EU (LU)	Muligt (support)	Privat, erhverv	EU-region kan vælges
<b>IONOS HiDrive</b>	ionos.com/hidrive	Tyskland	TLS + SSE	Nej	EU (DE)	Nej	SMB, enterprise	Tysk hyperscaler
<b>ownCloud</b>	owncloud.com	Tyskland	TLS + SSE	Afhænger af setup	Selvvalgt	Nej (EU-host)	Enterprise	Compliance- og audit-fokus
<b>Seafile</b>	seafile.com	Tyskland	E2EE (valgfrit)	Ja	Selvvalgt	Nej (EU-host)	Organisationer	Effektiv sync
<b>CryptPad Drive</b>	cryptpad.org	Frankrig	E2EE	Ja	EU (FR)	Nej	Privacy-kritiske brugere	Open Source
<b>OVHcloud Object Storage</b>	ovhcloud.com	Frankrig	TLS + SSE	Nej	EU	Nej	Enterprise / backend	EU-hyperscaler
<b>Scaleway Object Storage</b>	scaleway.com	Frankrig	TLS + SSE	Nej	EU (FR/NL)	Nej	Tech / enterprise	S3-kompatibel EU-cloud

Listen er en blanding af egne undersøgelser og artikler fra anerkendte kilder

## Bemærkninger:

- E2EE / zero-knowledge betyder, at leverandøren ikke har adgang til indholdet.
- Server-side kryptering beskytter data teknisk, men leverandøren har fortsat adgang.
- Dataplacering "EU valgfrit" betyder, at man aktivt skal vælge korrekt region eller hostingmodel.