

Archivi cloud

Per «archivio cloud» si intende uno spazio di archiviazione accessibile via Internet. Non tutti i provider di servizi cloud ottengono buoni voti in materia di protezione e sicurezza dei dati. Alcune regole possono essere utili per proteggere i vostri dati nella cloud.

Protegetevi così:

- **Scegliete un provider cloud adatto.** I provider stranieri spesso presentano degli svantaggi per quanto riguarda la protezione dei dati.
- **Effettuate l'accesso in modo sicuro.** Utilizzate una [password sicura \(https://www.ebas.ch/it/4-proteggere-gli-accessi-online/\)](https://www.ebas.ch/it/4-proteggere-gli-accessi-online/) e, se è prevista questa possibilità, un'autenticazione a due fattori, come per l'e-banking.
- **Trasferite i vostri dati solo in modo cifrato.** Utilizzate un servizio che trasferisce i vostri dati in modo cifrato (https).
- **Archivate i vostri dati solo in modo cifrato.** La cifratura corretta dei dati da parte del provider cloud spesso non si può verificare. Quindi provvedete voi stessi a crittografare i vostri dati.
- **Conservate anche una copia locale dei vostri dati.** Create regolarmente anche dei backup locali dei vostri dati archiviati nella cloud – anche il salvataggio corretto dei dati da parte del provider cloud solitamente non si può verificare.
- **Protegete tutti i dispositivi che accedono ai dati della cloud.** Seguite a tal fine le nostre [«5 operazioni per la vostra sicurezza digitale» \(https://www.ebas.ch/it/5-operazioni-per-la-vost-ra-sicurezza-digitale/\)](https://www.ebas.ch/it/5-operazioni-per-la-vost-ra-sicurezza-digitale/).

Quando si utilizzano archivi cloud come Dropbox, iCloud, OneDrive o Google Drive, i vostri dati vengono memorizzati in nodi centrali tramite la rete Internet pubblica. Quindi i vostri dati vengono trasmessi a terzi, e ciò solleva alcune questioni in materia di sicurezza e protezione dei dati.

Sede del provider cloud

La sede del provider di servizi cloud è fondamentale: spesso i vostri dati vengono salvati all'estero e sono quindi soggetti a una legislazione diversa in materia di protezione dei dati. Inoltre, molti dati in Internet vengono sistematicamente registrati e analizzati dai servizi segreti.

Secondo la legge, anche l'archiviazione e la conservazione sono una forma di trattamento dei dati, e pertanto sono operazioni soggette alle norme sulla protezione dei dati.

L'utilizzo dei servizi cloud diventa quindi critico quando dati personali degni di particolare protezione appartenenti a terzi vengono memorizzati da un provider di servizi cloud. A seconda delle circostanze, ne può facilmente risultare una violazione della legge sulla protezione dei dati (LPD) o del più rigido regolamento europeo sulla protezione dei dati (GDPR/RGPD).

Dati personali degni di particolare protezione sono i dati concernenti:

- le opinioni o attività religiose, filosofiche, politiche o sindacali,
- la salute, la sfera intima o l'appartenenza a una razza,

- le misure d'assistenza sociale,
- i procedimenti o le sanzioni amministrativi e penali.

Per ridurre i potenziali conflitti con la legge sulla protezione dei dati, è quindi preferibile scegliere un operatore svizzero.

Accesso sicuro

Ai dati della cloud si può accedere sia attraverso il browser, aprendo ed effettuando l'accesso sul sito Internet del provider, sia utilizzando un programma installato sul vostro dispositivo o una app.

L'anello centrale di tutto quanto è l'accesso: una password debole spalanca le porte agli intrusi. È quindi indispensabile osservare le nostre [6 regole per una password sicura](https://www.ebas.ch/it/4-protecting-online-access) (<https://www.ebas.ch/it/4-protecting-online-access>). Se è prevista questa possibilità, proteggete ancora meglio l'accesso utilizzando un'autenticazione a due fattori, come quelle applicate nell'e-banking.

Se l'accesso avviene tramite smartphone o tablet, in caso di smarrimento o furto i vostri dati restano al sicuro soltanto nella misura in cui è protetto l'accesso al dispositivo e al servizio cloud. Ulteriori informazioni a riguardo sono disponibili [qui](https://www.ebas.ch/it/4-protecting-online-access) (<https://www.ebas.ch/it/4-protecting-online-access>). Anche l'accesso tramite reti non sicure – come le reti [WLAN](https://www.ebas.ch/it/wlan/) (<https://www.ebas.ch/it/wlan/>) – costituisce un rischio.

Trasmissione sicura dei dati

Utilizzate un servizio che trasferisce i vostri dati in modo cifrato e quindi impedisce eventuali accessi non autorizzati di terzi durante la trasmissione.

Nel browser si può riconoscere che la trasmissione è cifrata se all'inizio della barra degli indirizzi compaiono i caratteri «https://» e un'[icona a forma di lucchetto](https://www.ebas.ch/it/verifica-del-certificato/) (<https://www.ebas.ch/it/verifica-del-certificato/>). Se utilizzate il servizio cloud per mezzo di un programma installato o di una app, dovete assicurarvi nelle impostazioni di configurazione che i dati vengano trasmessi mediante una connessione cifrata.

Salvataggio dei dati sicuro

Con gli archivi cloud affidate i vostri dati a una terza parte perché ve li conservi. Per questo motivo occorre prestare particolare attenzione agli aspetti della sicurezza e della cifratura dei dati.

La maggior parte dei provider cloud offre la possibilità di archiviare i dati in modo cifrato. Anche se solitamente i sistemi sono facili e comodi da usare, la loro affidabilità è difficilmente controllabile. La cosa più sicura è quindi provvedere voi stessi a crittografare e decrittografare i dati, per lo meno quelli sensibili.

Backup sicuro

Solitamente nemmeno il salvataggio corretto dei dati da parte del provider cloud si può verificare. Pertanto dovete assicurarvi di avere anche dei backup locali periodici dei vostri dati archiviati nella cloud. Ulteriori informazioni sono disponibili [qui](https://www.ebas.ch/fr/1-sauvegarder-les-donnees/) (<https://www.ebas.ch/fr/1-sauvegarder-les-donnees/>).

Dispositivi sicuri

Se il vostro dispositivo presenta un'infezione da malware, anche i vostri dati nella cloud non sono protetti e quindi vulnerabili. Seguite quindi le nostre [«5 operazioni per la vostra sicurezza digitale»](https://www.ebas.ch/it/5-secure-digital-operations) (<https://www.ebas.ch/it/5-secure-digital-operations>).

[operazioni-per-la-vostra-sicurezza-digitale/](#) .

Provider cloud

Al mondo esistono moltissimi provider cloud. Alcuni esempi:

Provider cloud esteri:

- [Dropbox \(https://www.dropbox.com\)](https://www.dropbox.com)
- [Google Drive \(https://www.google.com/drive\)](https://www.google.com/drive)
- [Apple iCloud \(https://www.apple.com/chde/icloud\)](https://www.apple.com/chde/icloud)
- [Microsoft OneDrive \(https://onedrive.live.com\)](https://onedrive.live.com)

Provider cloud svizzeri con salvataggio dei dati in Svizzera:

- [MyDrive \(https://www.mydrive.ch\)](https://www.mydrive.ch)
- [Securesafe \(https://www.securesafe.com\)](https://www.securesafe.com)
- [Speicherbox \(https://www.speicherbox.ch\)](https://www.speicherbox.ch)

Con gli archivi cloud, i dati vengono memorizzati in nodi centrali tramite la rete Internet pubblica. In questo modo si risparmia spazio di archiviazione e i dati sono accessibili da qualsiasi luogo e con dispositivi diversi, anche da più persone contemporaneamente.

Tuttavia, il trasferimento di dati personali a terzi può in alcuni casi comprometterne la sicurezza e sollevare problemi di protezione degli stessi. La scelta del provider è quindi fondamentale.