Cloud storage

The term cloud storage denotes storage space which is accessed over the Internet. Not all cloud providers score well as far as data protection and data security are concerned. A few rules will help you protect your data in the cloud.

Protect yourself by...

- **Choosing a suitable cloud provider.** Using foreign providers often has some drawbacks with regard to your data protection.
- **Securely logging in.** Use a secure password (https://www.ebas.ch/en/4-protecting-online-access/) and if possible two-factor authentication, similar to the method used with e-banking.
- **Only ever transmitting your data in encrypted form.** Use a service which transmits your data in encrypted form (https).
- **Only ever storing your data in encrypted form.** You are frequently unable to check that your cloud provider encrypts your data correctly. You should therefore encrypt your data yourself.
- **Creating an additional local back-up of your data.** Regularly create local back-ups of your data stored in the cloud - you are generally unable to check that your cloud provider backs up your data correctly either.
- **Protecting all devices accessing your cloud data.** To do so, please follow our "5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/)".

When using cloud storage such as Dropbox, iCloud, OneDrive or Google Drive, your data are stored in central locations via the public Internet. You are therefore passing on your data to a third party. This raises concerns with regard to security and data protection.

Cloud provider location

The cloud provider's location is vital: Your data are often stored abroad and are therefore subject to different data protection laws. In addition, many data on the Internet are systematically recorded and analysed by intelligence services.

According to law, storage and retention of data is also a form of data processing and hence subject to data protection.

Using cloud services therefore becomes particularly critical if third party personal data requiring special protection are stored with a cloud provider. Depending on the environment, this can quickly lead to a breach of the local data protection regulations (DSG) or the stricter European General Data Protection Regulations (GDPR).

Some instances of personal data requiring special protection are:

- Religious, ideological, political or union-related views or activities.
- Health, private life or ethnicity.
- Social benefit measures.

- Civil or criminal prosecution and sanctions.

To prevent potential conflicts with the data protection laws, you should therefore preferably opt for a Swiss provider.

Secure access

You either access your cloud data via your browser by calling up your provider website and logging yourself in there. Or you use a program or app installed on your device providing you with access to your service.

The point of access is the vulnerability here: A weak password throws the gates wide open to attackers. It is therefore an absolute must to follow our "6 rules for a secure password" (https://www.ebas.ch/en/4-protecting-online-access/) . If possible, use two-factor authentication, similar to the method used with e-banking, to better protect access.

When accessing the cloud via smartphone or tablet, your data are only as secure as the level of protection against access to your device and the cloud service in case of loss or theft. Further information can be found here (https://www.ebas.ch/en/4-protecting-online-access/) . Access via unsecured networks - i.e. Wi-Fi (https://www.ebas.ch/en/wlan/) - also poses a risk.

Secure data transmission

Use a service which transmits your data in encrypted form and prevents unauthorised access by third parties during transmission this way.

In your browser, this is the case if your address line starts with "https://", and a lock symbol (https://www.ebas.ch/en/checking-certificates/) is displayed. If you use a cloud service via software or an app installed, you must ensure that your data are transmitted via an encrypted connection via your configuration settings.

Secure data storage

With cloud storage, you entrust third parties with the storage of your data. For this reason, it is vital to pay particular attention to data back-ups and data encryption.

Most cloud providers now offer the option to file your data in encrypted form. Yet while this is generally easy and convenient to handle, it is just about impossible to check how reliable this is. The most secure method therefore is to encrypt and decrypt at least your sensitive data yourself.

Secure back-up

You are generally unable to check that your cloud provider backs up your data correctly either. For this reason, you should make absolutely sure that you create local back-ups of all your data stored in the cloud, too. Further information can be found here (https://www.ebas.ch/en/1-backing-up-data/) .

Secure devices

If your device is infected with malware, your data are not secure in the cloud either and are liable to attack. You should therefore follow our "5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) ".

Cloud provider

There are a large number of cloud providers all over the world: Some examples:

Foreign cloud providers:

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

Swiss cloud providers with data storage in Switzerland:

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

With cloud storage, data are stored in central places via the public Internet. This saves storage space and enables access to your data from any location and with different devices, even by several people at the same time.

Passing on personal data to third parties however can potentially adversely affect your data security and raises concerns with regard to data protection. It is therefore vital to make the right choice of provider.