PROTECTING YOUR DATA PRIVACY

February 2023

https://righttoconnect.org

Protecting Your Data Privacy

Data

Activists, HRDs, and CSOs typically possess important information, and many have access to a wide range of resources that could help them achieve their goals. These assets, which are stored as data, are vulnerable to attacks from authorities and hackers.

The safe storage of data on encrypted hard drives or flash drives is an option, but doing so may make the data even more vulnerable to loss, theft, or technical issues. Moreover, hard devices only have limited storage space.

As a result, cloud storage has grown in importance. The ability to share data more easily is another benefit of using the cloud, which is essential for activists who need to spread information to further their causes.

Cloud Storage

It may be necessary for the vast majority of important cloud storage companies to grant authorities access to your data.

You must be informed that just because your cloud storage provider offers data encryption, this does not guarantee your privacy. Encryption alone won't shield against this because some providers have been known to trade data and files with authorities.

How to Secure Cloud Storage

You may secure your cloud storage by choosing a cloud storage company that encrypts your files while they are on your device before uploading to the cloud, as opposed to files that are encrypted in transit to the cloud. Remember that service providers can have access to encryption keys and could decode your files or hand them over to the authorities if required.

You should seriously consider manually encrypting your data before uploading it to a cloud provider. In this case, you will be the only person with access to your data's decryption key as long as you never submit the encryption keys along with your files.

There are numerous paid and unpaid encryption tools out there, but be sure they work with your devices and your cloud storage provider. Ensure that the program utilizes end-to-end encryption, which keeps your contents secure from the time they leave your smartphone until you can access them again.

Sharing Data

Users of the Veracrypt program (https://veracrypt.fr/) can store encrypted folders that appear to outsiders to be regular or system files on their hard drives and in online storage services like Google Drive and Dropbox. Before uploading papers for online sharing and storage, this is done to ensure their security while they are being saved on the computer. After using Veracrypt to encrypt a document like this, select delete the application to avoid the program drawing attention. This goes for the Trash Bin as well. See the following alternatives for secure end-to-end encrypted file sharing:

- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com

Resources:

- https://veracrypt.fr/
- https://www.dropbox.com
- https://www.google.com/drive/
- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com