FAQ Tresorit

What is Tresorit?

Tresorit is a file storage and sharing service. It is a specific service for sensitive data: it offers enhanced security through advanced access control and data encryption. More details on the [Tresorit description page](#).

What is sensitive data?

In everyday language, data is sometimes described as sensitive in a vague way. However, Swiss law gives a very precise definition ([Art. 4, paras. 1 and 2 of the LPrD](#)) that applies to the Vaud cantonal administrations, including UNIL:
"Any personal data [any information relating to an identified or identifiable person] concerning :

- religious, philosophical, political or trade union opinions or activities, or ethnic origin ;
- the private sphere of the individual, in particular his or her psychological, mental or physical state;
- individual measures and assistance arising from social legislation;
- criminal or administrative proceedings or sanctions".

Note that there is also a marginally different definition in the federal law ([LPD art. 5](#)). Federal law applies to private individuals and federal organizations.

Research into human diseases and into the structure and function of the human body is covered by a specific law ([LRH](#)).

Who should I contact to request access to Tresorit?

If you think your research data is sensitive ([LPrD art. 4](#) or [LRH art. 2](#)), please contact your faculty data steward, who will help you make a request to the Computing and Research Support Division ([DCSR](#)). See "Aide et renseignements" on the [Data Protection page](#). Following this request, you will be offered a face-to-face appointment to install and configure Tresorit and to encrypt your computer.

Who is Tresorit for?

Tresorit is intended exclusively for UNIL researchers and their scientific collaborators (internal or external). The request to use this service must be made by a project leader affiliated to UNIL. See [directive 4.5 art. 4](#) for the definition of the designation of Principal Investigator.

Where is my data stored?

UNIL has a specific contract with Tresorit AG which guarantees that the data is stored in Switzerland. Tresorit uses online storage on the Microsoft Azure platform (see below, How is my data protected?).

How is my data protected?

Data uploaded by researchers from their computer to online storage is done using the Tresorit software or web interface. Both encrypt the data before it is sent to online storage. They require verification of your identity using a password and a code on your mobile phone.

If the data is stolen directly from online storage, the encryption applied to the data makes it impossible to read it in clear text without the decryption key.

If your computer is lost or stolen, it will be impossible to access the data on Tresorit from your computer without your password and your mobile phone. Sensitive data synchronized on your computer will also be inaccessible as it will be encrypted during the meeting with the DCSR.

What does "encryption" mean?

Encryption is an algorithmic process used to make a document impossible to understand for anyone who does not have access to the decryption key.

Why use Tresorit?

UNIL researchers working with sensitive data ([LPrD art. 4](#)) or LRH-sensitive data ([LRH art. 2](#)) submit their research project to the cantonal human research ethics committee (CER-VD). Technical and organisational measures must be put in place to ensure that projects are accepted by the CER facultaire, CER UNIL or CER-VD:

- Access to data must be restricted to the researchers concerned ([Guide du PFPDT 2015 p11](#)).
- Data must be stored in encrypted form ([Guide du PFPDT 2015 p20](#)).
- Data access and modification must be traceable ([ORH art. 5c](#)).

The aim of all these measures is to protect individuals against the misuse of data concerning them ([LPrD art. 1](#)). Tresorit is a service offering these three functions.

Who can access my data?

A group of four people are Tresorit administrators at UNIL. All these Tresorit administrators are employees of the IT Centre. Tresorit administrators can change a user's password if they forget it (protection against loss/destruction of data, LPrD art. 10). When the password is changed, which is subject to traceability and is done at the request of the **project leader** (Principal Investigator as designated in directive 4.5 art. 4), access to the files by the Tresorit administrator is temporarily possible. The Tresorit solution is designed so that neither the Tresorit company nor the storage provider can access the decrypted data.

What volume is available?

UNIL offers up to 2 To per Principal Investigator (PI), regardless of the number of projects under his/her supervision.

Can I collaborate with people outside UNIL?

Yes, the UNIL IT Centre covers the cost of all Tresorit licences for UNIL members (free of charge). If a research project needs to give access to people outside UNIL, three free licences are made available to the **project leader** (Principal Investigator, PI). If more than three external persons are required, a fee of CHF 150 per year and per person will be charged to the PI.

If a person from outside UNIL already has a Tresorit account that is not affiliated to UNIL, it is currently impossible to use this account to access UNIL research data.

What is Tresorit's backup strategy?

As the online storage uses the Microsoft Azure platform, there are three physical copies of the data.