

Data storage in the FACS Core Facility

V02

Aarhus University is obligated to comply with applicable legislation on the protection of personal data (GDPR). Moreover, the university has contractual obligations relating to confidentiality. Classification of data only covers data that is not covered by the circular from the Danish Ministry of Justice regarding security (only in Danish).

It is your own responsibility to make sure your data is stored correct.

After acquisition of data, transfer your data to your server, following the procedure: “Data transfer.....”

You are allowed to leave a template/ncf.file in your folder on the instrument but be aware that other users will have access to that template.

Data storage security and back-up

Both the One drive and the common drive at Aarhus University are protected with two factor logins with access control from the root of the folder. These drives are automatically backed up.

PIs may create a group folder accessible for employees via their AU-ID. The PI will grant access or remove access to his/her group folder on the common drive.

The drives can only be accessed from AU internal network or via VPN with two factor logins.

Regarding security and storage of confidential data please see the table below and the following link:

<https://medarbejdere.au.dk/en/informationsecurity/classification-of-data#c2545080>

	Public	Internal	Confidential	Sensitive
O-drive	Yes	Yes	Yes	No
OneDrive	Yes	Yes	No*	No*
Sharepoint	Yes	Yes	No*	No*

Yes: You are ALLOWED to save/share data here

No: You are NOT ALLOWED to save/share data here

No*: Provided that data has been PSEUDONYMISED