Storage and sharing of research data

System / device to store in	**Storage of data / processing data** (without special categories of personal data[1])	**Storage of data / processing data** (with special categories of personal data[2])	**Share research data** (without special categories of personal data[1])	**Share research data** (with special categories of personal data[2])
Computer operated by the researcher[3]	**Yes**	**No**	**Yes**	**No**
A computer that the IT department has certified security on	**Yes**	**Yes**	**Yes**	**Yes**
Kau computer (Mac or PC managed centrally by the IT department)	**Yes**	**Yes**	**Yes**	**Yes**
USB hard disk / memory that is not encrypted[4]	**Yes**	**No**	**Yes**	**No**
USB hard disk / memory that is Encrypted[5]	**Yes**	**Yes**	**Yes**	**Yes**
Central storage Kau	**Yes**	**Yes**[6]	**Yes**	**Yes**[6]
Sunet Drive[7]	**Yes**	**Yes**	**Yes**	**Yes**

See also administrative decision Fb28/19, Rules of procedure for the processing of information in systems and services[8], for more information on how different types of information (including personal data) can be handled in the university's various systems and services.

[1] Personal information such as name, date of birth, contact information for work and for students, as well as the privacy-sensitive personal information: social security number, personal identity number, credit card information, information from performance appraisals, salary information and more.
[2] The special categories of personal data are: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
[3] The computer must have a password for login, necessary security updates installed, a firewall activated and the university's selected client protection installed. The hard drive should be encrypted.
[4] However, the USB device must be handled in such a way that unauthorized persons cannot access the information, e.g. stored locked up or under supervision.
[5] Get help from the IT department to achieve adequate protection, 2525@kau.se
[6] Central storage that is judged according to Fb28/19, Rules of procedure for the processing of information in systems and services, to have adequate security for special categories of personal data.
[7] https://www.kau.se/en/research/research-data/during-project/sunet-drive
[8] https://inslaget.kau.se/universitetet/informationshantering/informationssakerhet