Sensitive data protection

source UK Data Archive[1]

Data that contain personal or confidential information should be treated with higher levels of security than data which do not. Especially at the stage of collecting and transferring data one should be aware of the risks. Research consortia should agree on data protection procedures before the start of the data collection. Data leaks, that is personal data falling in the hands of unauthorised parties, must be reported[2]**.**

You can reduce the sensitivity of your data by :

- ✓ anonymizing or aggregating data [see our handout on anonymization]
- ✓ removing personal information, such as names and addresses, from data files and storing them separately
- ✓ encrypting data containing personal information before they are stored / transmitted

Dutch code of conduct for use of personal data in research wants you to[3] :

- ✓ Anonymize sensitive data
- ✓ Keep very sensitive data offline
- ✓ Send your data encrypted
- ✓ Have your informed consent allow new research
- ✓ Destroy personal data after the legal term (6 months after last use for research)

Transferring data

Transmitting data between locations or within research teams can be a challenge for the data management infrastructure. Surfdrive is a national file-sharing service that is especially designed for higher education and research. The files are stored in the Netherlands and the data is sent over the networks in encrypted format. SURFdrive complies with all Dutch and European privacy legislation. However, when sharing a file or folder with a user who doesn't have access to SURFdrive, extra password protection is recommended.[4] Research groups can share documents and data in Virtual Research Environments, offered by the University Libraries Leiden. Controlled access can be granted to researchers from outside Leiden University. VRE's are not suitable for high risk data (such as criminal or medical information).[5]

[1] Based on : *Managing and sharing research data : a guide to good practice* / Louise Corti, Veerle Van den Eynden, et al., Los Angeles : Sage, 2014

[2] See : http://www.students.leiden.edu/news/protecting-personal-data-and-preventing-data-leaks.html

[3] To be found here [in Dutch] : http://www.vsnu.nl/code-pers-gegevens.html

[4] More information on security issues in Surfdrive: https://www.surfdrive.nl/en/faq.html

[5] https://vre.leidenuniv.nl/SitePages/Home.aspx

Physical measures for data protection

- ☐ Controlling access
- ☐ Logging access
- ☐ Transporting no more than necessary

Network measures

- ☐ Sensitive data not on servers connected to external network
- ☐ Firewall protection

System / files measures

- ☐ Password on computer
- ☐ Password / controlled access on individual files
- ☐ Encryption (Pretty Good Privacy – PGP - standard technology)
- ☐ Non-disclosure agreements for managers / users
- ☐ Not sending via email or other file transfer means without encrypting ((GnuPg)
- ☐ Destroying data in a consistent and robust manner
- ☐ File-sharing services like Google Docs or Dropbox are not suitable for sensitive data.

Encrypting data

Encryption transforms data to make it unreadable to anyone except those with a key. Data encryption will maintain data security during transmission and should be used when sending disclosive information. It can also be used for safely storing files, such as for back-ups or storage on mobile devices. Individual files can be encrypted, as well as entire storage devices or spaces. More information and a step-by-step exercise on how to encrypt your data is on the UK DA website[6].

More about University's security policy :
http://media.leidenuniv.nl/legacy/minimale-maatregelen-informatiebeveiliging.pdf [Dutch].

[6] http://www.data-archive.ac.uk/create-manage/storage/encrypt