VU VRIJE UNIVERSITEIT AMSTERDAM

School of Business and Economics

RESEARCH DATA MANAGEMENT ROUTE MAP (SBE.VU.NL/RDM)

INSTRUCTIONS FOR WORKING WITH PERSONAL DATA

1 BEFORE RESEARCH

DO YOU WORK WITH PERSONAL DATA?

Do you gather / have PERSONAL DATA of any form? (e.g., name, email, VUnet ID, phone, (IP-)address, grade list, payment data, absence records, medical data, audio or video, granular zip codes) OR data that COMBINED with other data BECOME PERSONAL DATA?

WHAT TO DO?

1. Fill out a Privacy Impact Assessment (PIA) before gathering data and if so advised, contact Information Security Officer VU [read more].

2. Register your data set at SBE Research Office by filling out the data registration form [read more], so that the School is aware which data is used by its researchers.

DO YOU WORK WITH CONFIDENTIAL DATA?

Do you gather / have CONFIDENTIAL DATA (e.g., competition sensitive, publication restriction, under license, societally sensitive)?

WHAT TO DO?

1. Register your data set at SBE Research Office by filling out the data registration form [read more], so that the School is aware which data is used by its researchers.

2 DURING RESEARCH

DO YOU HANDLE DATA WITH PRIVACY AND SENSITIVITY ISSUES?

WHAT TO DO?

SECURE STORAGE DURING RESEARCH:

1. Act in line with PIA advice

2. In case you use encrypted data, inform SBE Research Office how and where the data are stored [researchoffice.sbe@vu.nl].

WHAT TO DO?

SECURE DATA EXCHANGE/ SYNCHRONIZE/ SHARING:

(with yourself or others)
- VU mail + encrypted attachment
- SURF Filesender
- SURFdrive (only if local Surfdrive copy folder is encrypted + good active virus scanner + restricted access to maps arranged)
- Do NOT use public WIFI or unsafe, unencrypted exchange

DO YOU HANDLE DATA WITHOUT PRIVACY AND SENSITIVITY ISSUES?

WHAT TO DO?

FAST AND EASY STORING DATA DURING RESEARCH:

- Own data: H/G-drive, cloud
- Group data: G-drive
- Large data: Scistor
- Cloud-storage: SURFdriveVirtual servers: SciCloud
- Local drive: only with up-to-date virus scanner + remote backup
- Cloud (Dropbox, SURFdrive, Google Drive)

3 AFTER RESEARCH

STORING DATA AFTER RESEARCH (FOR 10 YEARS) FOR VERIFICATION

WHAT TO DO?

1. Store data in a retrievable way for at least 10 years, complying with VSNU code of conduct for verification of research. Use the Research Data Wizard on VUnet [read more]

2. Notify SBE Research Office [email] about your data's storage location (and encryption keys / access restrictions if applicable.

DELETE UNNECESSARY DATA

WHAT TO DO?

1. Destroy unnecessary copies of your data.

2. Delete access rights for persons who are no longer involved.

BEST PRACTICES FOR WORKING WITH PERSONAL DATA

GOOD TO KNOW BEFORE STARTING YOUR RESEARCH

BUDGETING AND DATA MANAGEMENT PLAN FOR FUNDERS

Do you need to BUDGET your DATA STORAGE? OR Does your FUNDER require a Data Management Paragraph or Plan? f so, fill out a data management template [read more].

ETHICS REVIEW

Does your research need approval by the School's Research Ethics Review Board?
If so, fill out the Research Ethics checklist online [read more].

DATA OWNERSHIP

Will the data collected by others or are you part of a research consortium? If so, Find out what who owns the data, and what your exploitation possibilities are. Find out more at IXA [read more].

DO'S

ALWAYS DETERMINE PRIVACY IMPACT

Before gathering data, always conduct a Privacy Impact Assessment (PIA) to identify and minimize potential privacy risks of your project [read more].

REDUCE OBVIOUS RISKS

Reduce obvious risks (e.g. anonymize and split data into a sensitive and insensitive part, encrypt your laptop or PC, always lock your working station ([Windows-key] + L) and backup your data by default).

USE VIRUS SCANNER AND DO SECURITY UPDATES

Install a virus scanner (download from VUnet) on your working station [read more],never miss security updates

ORGANIZE AND COMMERCIALIZE DATA AFTER RESEARCH

- Organizing data / making data reproducible: use different folders data and code/syntax, use systematic file names, keep a log / codebook [read more]
- Commercializing your data: showcase your data, but restrict access on your conditions. Find out what the possibilities and conditions are for re-using data at IXA [read more]

DATA MINIMALIZATION

Only collect those data that are strictly necessary for the purpose of your research

DONT'S

DATA STORAGE

- Don't store personal and certain confidential data on non-EU servers (e.g. Dropbox, OneDrive,Google Drive)
- Don't use non-encrypted local (C: or D:) or cloud storage (e.g. Amazon EU) of personal / confidential data
- Don't work with non-encrypted laptops, USB-sticks, SD-cards, cell-phone storage
- Don't store data for verification only at a commercial publisher and waive your rights.

DATA BACKUP

- Don't work without automated backups
- Don't work without fallback arranged for encryption key access
- Don't risk lossof access to the data for your research group in case one member drops out

RISK OF DATA LEAKS

- Don't fail to report data leaks immediately to the SBE Research Office (researchoffice.sbe@vu.nl)
- Don't use Public WiFi (e.g. train, café) for working with personal / confidential data; NB admissible with secure (Edu)VPN
- don't share/mail personal/sensitive data without encryption

RDM SUPPORT: WWW.SBE.VU.NL/RDM - RESEARCHOFFICE.SBE@VU.NL - 020-5985667