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?

1. Act in line with PIA advice
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.

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.

WHAT TO DO?
1. Store data in a retrievable way and where the data are stored inform SBE Research Office [researchoffice.sbe@vu.nl]
2. Secure storage during research:
   - Act in line with PIA advice
   - In case you use encrypted data, inform SBE Research Office how and where the data are stored [researchoffice.sbe@vu.nl]
   - Do NOT use public WiFi or un-secured internet connection.

DO YOU HANDLE DATA WITH PRIVACY AND SENSITIVITY ISSUES?

WHAT TO DO?
1. Secure data exchange/synchronization/sharing:
   - Use VUnet mail and encrypted attachment
   - Use SURF Filesender
   - SURFdrive only if local SURFdrive copy folder is encrypted + good active virus scanner + restricted access to mass arranged
   - Do NOT use public WiFi or unsafe, unencrypted exchange

WHAT TO DO?
1. 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)

DO YOU HANDLE DATA WITHOUT PRIVACY AND SENSITIVITY ISSUES?

WHAT TO DO?
1. Destroy unnecessary copies of your data.
2. Delete access rights for persons who are no longer involved.

WHAT TO DO?
1. Storing data after research (for 10 years) for verification:
   - Store data in a retrievable way for at least 10 years, complying with VUnet code of conduct for verification of research. Use the Research Data Wizard on VUnet [read more]
   - Notify SBE Research Office [email] about your data's storage location and encryption keys / access restrictions if applicable.

DELETE UNNECESSARY DATA
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

DO'S
1. Budgeting and Data Management Plan for funders
   - Do you need to budget your DATA STORAGE? OR Does your FUNDER require a Data Management Plan or Plan? Fill out a data management template [read more].
2. 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].
3. Data Ownership
   - Who 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].
4. 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].
5. 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)
6. Use Virus Scanner and Do Security Updates
   - Install a virus scanner (download from VUnet) on your working station [read more]. Never miss security updates.
7. 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].
8. Data Minimalization
   - Only collect those data that are strictly necessary for the purpose of your research

DON'T'S
1. 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 laptops, USB-sticks, SD-cards, cell phone storage
   - Don't store data for verification only at a commercial publisher and waive your rights.

2. Data Backup
   - Don't work without automatic backups
   - Don't work without fallback arranged for encryption key access
   - Don't risk loss of access to the data for your research group in case one member drops out

3. 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

4. Storing Data after Research (for 10 Years) for Verification
   - Don't store personal and certain confidential data on non-EU servers (e.g. Dropbox, OneDrive, Google Drive)
   - Don't use 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.

5. 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].

6. 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)

7. Use Virus Scanner and Do Security Updates
   - Install a virus scanner (download from VUnet) on your working station [read more]. Never miss security updates.

8. 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].

9. Data Minimalization
   - Only collect those data that are strictly necessary for the purpose of your research

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

INSTRUCTIONS FOR WORKING WITH PERSONAL DATA

1. Before Research
2. During Research
3. After Research

1. Do you work with confidential data?
2. What to do?
3. During RDM Support:
   - After 3, 2, 1 access restrictions if applicable.
4. Do you gather / have confidential data of any form? (e.g., competition sensitive, publication restriction, under license, socially sensitive?)
5. What to do?
6. After RDM Support:
   - Do you handle data privacy and sensitivity issues?
7. Do you handle data with privacy and sensitivity issues?
8. What to do?
9. Storing data after research (for 10 years) for verification:
10. Delete unnecessary data:
11. Data storage:
12. Data backup:
13. Risk of data leaks:

1. Do you work with confidential data?
2. What to do?
3. During RDM Support:
   - After 3, 2, 1 access restrictions if applicable.
4. Do you gather / have confidential data of any form? (e.g., competition sensitive, publication restriction, under license, socially sensitive?)
5. What to do?
6. After RDM Support:
   - Do you handle data privacy and sensitivity issues?
7. Do you handle data with privacy and sensitivity issues?
8. What to do?
9. Storing data after research (for 10 years) for verification:
10. Delete unnecessary data:
11. Data storage:
12. Data backup:
13. Risk of data leaks: