INSTRUCTIONS FOR WORKING WITH PERSONAL AND CONFIDENTIAL DATA

1. BEFORE RESEARCH

DO YOU WORK WITH PERSONAL DATA?

Do you gather / have any personal data that may lead to the identification of a person (e.g. name, email, VUnet ID, phone or IP-address, grade list, payment data, absence records, medical data, audio/video, zip code) or data that combined with other data becomes personal data?

WHAT TO DO?
1. REGISTER YOUR PROJECT AT SBE RESEARCH OFFICE through the pre-Privacy Impact Assessment form (see step 1, "Before Research").
2. In case you plan to outsource (part of) the data processing to a sub-contractor, conclude a Data Processing Agreement. For a template agreement please contact [researchoffice.sbe@vu.nl].

DO YOU WORK WITH CONFIDENTIAL DATA?

Do you gather / have confidential, but not personal data (e.g., competition sensitive, publication restricted, under license, socially sensitive)?

WHAT TO DO?
1. REGISTER YOUR PROJECT AT SBE RESEARCH OFFICE through the pre-Privacy Impact Assessment form (see step 1, "Before Research").
2. In case you plan to outsource (part of) the data processing to a sub-contractor, conclude a Data Processing Agreement. For a template agreement please contact [researchoffice.sbe@vu.nl].

DO YOU HANDLE PERSONAL OR CONFIDENTIAL DATA?

Do you handle any personal or confidential data? If so, take the following measures to minimize potential privacy and sensitivity issues.

WHAT TO DO?

1. Act in line with the Privacy Impact Assessment (PIA) advice (see step 1, "Before Research").
2. Notify SBE Research Office how, when and where the data are stored.
4. Install virus scanner (download from VUnet) on your working station.
5. Always lock your working station ([Windows-key] + L) and backup your data by default.
6. Secure data exchange / Synchronization / Sharing: with yourself or others:
   - VU mail = encrypted attachment
   - SURF Filesender (read more)
   - SURFdrive (only if local Surfdrive copy folder is encrypted + good access to maps arranged)
   - Do NOT use public WiFi or unsafe, unencrypted exchange.

2. DURING RESEARCH

DO YOU HANDLE PERSONAL OR CONFIDENTIAL DATA?

Do you handle any personal or confidential data? If so, take the following measures to minimize potential privacy and sensitivity issues.

WHAT TO DO?

1. Secure data exchange / Synchronization / Sharing: with yourself or others:
   - VU mail = encrypted attachment
   - SURF Filesender (read more)
   - 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 WORK WITH PERSONAL DATA?

Do you gather / have any personal data that may lead to the identification of a person (e.g. name, email, VUnet ID, phone or IP-address, grade list, payment data, absence records, medical data, audio/video, zip code) or data that combined with other data becomes personal data?

WHAT TO DO?
1. Secure data exchange / Synchronization / Sharing: with yourself or others:
   - VU mail = encrypted attachment
   - SURF Filesender (read more)
   - 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 WORK WITH CONFIDENTIAL DATA?

Do you gather / have confidential, but not personal data (e.g., competition sensitive, publication restricted, under license, socially sensitive)?

WHAT TO DO?

1. Secure data exchange / Synchronization / Sharing: with yourself or others:
   - VU mail = encrypted attachment
   - SURF Filesender (read more)
   - SURFdrive (only if local Surfdrive copy folder is encrypted + good access to maps arranged)
   - Do NOT use public WiFi or unsafe, unencrypted exchange.

USE THE FAIR PRINCIPLE FOR ANY DATA, WITH OR WITHOUT PRIVACY OR CONFIDENTIALITY ISSUES

WHAT TO DO?

1. Use the fair principle for any data, with or without privacy or confidentiality issues.

3. AFTER RESEARCH

DO YOU HANDLE PERSONAL OR CONFIDENTIAL DATA?

Do you handle any personal or confidential data? If so, take the following measures to minimize potential privacy and sensitivity issues.

WHAT TO DO?

1. Store data in a retrievable way for at least 10 years, in compliance with VUDN code of conduct for verification of research (read more).
2. Notify SBE Research Office how, when and where the data are stored.

DELETE UNNECESSARY DATA

WHAT TO DO?

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

STORE DATA AFTER RESEARCH (AT LEAST 10 YEARS) FOR VERIFICATION

WHAT TO DO?

1. Store data in a retrievable way for at least 10 years, in compliance with VUDN code of conduct for verification of research (read more).
2. Notify SBE Research Office how, when and where the data are stored.

DELETE UNNECESSARY DATA

WHAT TO DO?

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

CHECKLIST FOR WORKING WITH PERSONAL DATA

BEFORE STARTING YOUR RESEARCH (OPTIONAL)

1. Budgeting and data management plan for funding agencies
   - Do you need to budget your data storage costs? Or does the funder of your research (e.g. NWMO, EC; a panel) require a Data Management Paragraph or Plan? If so, fill out a data management template.

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.

3. Intellectual property rights
   - Will the data be collected by others or are you part of a research consortium? If so, get advice regarding intellectual property rights and exploitation possibilities at Innovation Exchange Amsterdam (IXA).

DO'S (ALWAYS COMPLY WITH THE FOLLOWING)

1. Determine privacy impact
   - Before gathering data, always conduct a Privacy Impact Assessment (PIA) to identify and minimize potential privacy risks of your project (see step 1, "Before Research").

2. 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).

3. Use virus scanner and do security updates
   - Install virus scanner (download from VUnet) on your working station.

4. Organize and commercialize data after research
   - Organizing data / making data reproducible: use different folders data and code/syntax, use systematic file naming, keep a log / codebook.
   - 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 Open Science.

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

6. Data backup
   - Make automated backups.
   - Arrange fallback for encryption key access.
   - Prevent loss of access to the data for your research group in case one member drops out.

DON'TS (ALWAYS COMPLY WITH THE FOLLOWING)

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 local C: or D: or cloud storage (e.g. Amazon EU) of personal / confidential data.
   - Don't store 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.

2. Risk of data leaks
   - Don't fail to report data leaks immediately to the IT Servicedesk.
   - Don't use Public WiFi (e.g. train, cafe) for working with personal / confidential data. NB: admissible with security (EDJNP).
   - Don't share personal / sensitive data without encryption and use passwords with 8+ characters.

INSTRUCTIONS FOR WORKING WITH PERSONAL AND CONFIDENTIAL DATA

1. Do you gather / have any personal data that may lead to the identification of a person (e.g. name, email, VUnet ID, phone or IP-address, grade list, payment data, absence records, medical data, audio/video, zip code) or data that combined with other data becomes personal data?

WHAT TO DO?
1. Register your project at SBE Research Office through the pre-privacy impact assessment form.
2. In case you plan to outsource (part of) the data processing to a sub-contractor, conclude a Data Processing Agreement. For a template agreement please contact [researchoffice.sbe@vu.nl].

2. Do you gather / have confidential, but not personal data (e.g. competition sensitive, publication restricted, under license, socially sensitive)?

WHAT TO DO?
1. Register your project at SBE Research Office through the pre-privacy impact assessment form.
2. In case you plan to outsource (part of) the data processing to a sub-contractor, conclude a Data Processing Agreement. For a template agreement please contact [researchoffice.sbe@vu.nl].

3. Do you handle any personal or confidential data? If so, take the following measures to minimize potential privacy and sensitivity issues.

WHAT TO DO?

1. Act in line with the Privacy Impact Assessment (PIA) advice (see step 1, "Before Research").
2. Notify SBE Research Office how, when and where the data are stored.
4. Install virus scanner (download from VUnet) on your working station.
5. Always lock your working station ([Windows-key] + L) and backup your data by default.
6. Secure data exchange / Synchronization / Sharing: with yourself or others:
   - VU mail = encrypted attachment
   - SURF Filesender (read more)
   - SURFdrive (only if local Surfdrive copy folder is encrypted + good access to maps arranged)
   - Do NOT use public WiFi or unsafe, unencrypted exchange.

DO'S (ALWAYS COMPLY WITH THE FOLLOWING)

1. Determine privacy impact
   - Before gathering data, always conduct a Privacy Impact Assessment (PIA) to identify and minimize potential privacy risks of your project (see step 1, "Before Research").

2. 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).

3. Use virus scanner and do security updates
   - Install virus scanner (download from VUnet) on your working station.

4. Organize and commercialize data after research
   - Organizing data / making data reproducible: use different folders data and code/syntax, use systematic file naming, keep a log / codebook.
   - 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 Open Science.

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

6. Data backup
   - Make automated backups.
   - Arrange fallback for encryption key access.
   - Prevent loss of access to the data for your research group in case one member drops out.

DON'TS (ALWAYS COMPLY WITH THE FOLLOWING)

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 local C: or D: or cloud storage (e.g. Amazon EU) of personal / confidential data.
   - Don’t store 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.

2. Risk of data leaks
   - Don’t fail to report data leaks immediately to the IT Servicedesk.
   - Don’t use Public WiFi (e.g. train, cafe) for working with personal / confidential data. NB: admissible with security (EDJNP).
   - Don’t share personal / sensitive data without encryption and use passwords with 8+ characters.