Guidelines for analyses of EuroSIDA data by external experts

Introduction

Some statistical analyses of EuroSIDA data may be performed by external experts outside the core group of EuroSIDA statisticians. The purpose of this document is to describe the process, requirements and operating procedure for such analyses.

The project is defined as a set of data constituting content to address a defined research question typically leading to the formation of one original research article and/or abstract. The project must be approved by the EuroSIDA steering committee (SC) overall and for external analyses by the named person and the approval process should be archived appropriately. A proforma for project proposals can be found at http://www.cphiv.dk/Studies/EuroSIDA/Study-documents.

The PI, project statistician and a central statistician should all sign a copy of this SOP to indicate they have read and understand the guidelines, and a copy should be archived.

Procedure and requirements for external analyses

1. The project proposal should clearly identify the person leading the project (PI) and also a named statistician for the project. A change in these persons responsible should be notified to the EuroSIDA SC.
2. The PI is responsible for generating an explicit statistical analysis plan (SAP), including the list of variables required for analyses from the dataset. Central ES statisticians are responsible for checking the feasibility of the project, that it is adequately powered, as well as providing input into the proposed analyses.
3. The project team, including the PI, statistician and central statistician should agree the analyses plan, via TC if necessary, and the agreement should be archived via email agreement. During this time, the PI, project statistician and central statistician should work together to ensure a thorough understanding of the dataset and how key variables have been defined and derived. Merging of the different components of the data is the responsibility of the project statistician.
4. A request for data for analyses should be made after agreement of the statistical analysis plan, via the EuroSIDA IT team, including complete specification of the data items required. Each project will require a data transfer agreement which will be initiated by EuroSIDA IT when a project has been approved by the EuroSIDA SC and the SAP approved. The data transfer agreement will need to be signed by the PI and person performing the analysis and may take 3-6 months to action depending on whether the request for data is from a EU or non-EU country.
5. The PI and statistician must adhere to requirements for data protection and processing, as detailed in the data security appendix below. The PI must ensure that data is destroyed once the data has been analyzed and the paper published and we will require a signed declaration that this has been done. Once the project is finalized and published, a copy of all

final scripts used to analyse the data and for the published paper should be sent to EuroSIDA IT for central storage and archive.

6. The data should be analysed according to the statistical analyses plan. Additional analyses should only be taken with the prior approval of the EuroSIDA steering committee and central statistical group.
7. Results generated from analyses, including abstracts, publications, etc, should be shared with the EuroSIDA steering committee and central statisticians according to the timelines shown below.

		Core group	Co-Authors/SC	Total
		Working days needed for review		
Abstracts	Abstract deadline	6	4	10
Posters	Production deadline	6	2	8
Orals	Conference start date	6	4	10
Manuscript	Submission		10	10

8. Requests for review and approval that do not allow sufficient time for comments may not be approved. The EuroSIDA policy for co-authorships should be followed, or if not, the proposed changes approved by the EuroSIDA SC, and can be found here http://www.chip.dk/Portals/0/files/Eurosida/EuroSIDA/SOP%20coauthorship.pdf?timestamp=1464082845266

Signatures

Project PI _____ Date _____

Print name

Project statistician _____ Date _____

Print Name

EuroSIDA statistician _____ Date _____

Print Name

Appendix : Data security and Processing

Definitions:

Personal data, is data for which the Danish Act on the Processing of Personal Data applies. This is all data which can lead back to an individual person. This means that even though pseudonymised data does not contain personal identifiers, this type of data still must adhere to the Act, because the key file linking between pseudoIDs and personal IDs exists.

Data Processor, your organisation (i.e. you)

Controller, The Capital Region of Denmark – our organisation (i.e. us)

ISO 27001, ISMS – Management system for information security, standard

Data Processing Agreement, the agreement entered between you and The Capital Region of Denmark for projects that involve statistical analysis by your personnel.

Ad Hoc Workplaces, remote workplaces or home offices

Sub-Data Processors, 3rd party/organisation

From the Data processing agreement:

Below are the most relevant issues regarding data security.

1. The Responsibility of the Data Processor

The Data Processor undertakes at any time to meet the Danish statutory requirements as well as the Data Processor's national statutory requirements regarding data processing and data security as well as the Controller's information security policy with the associated guidelines in connection with the data processing carried out on behalf of the Controller.

2. Technical and Organisational Security Measures

The Data Processor shall make the necessary technical and organisational security measures against accidental or illegal destruction, loss or deterioration of personal data and against disclosure thereof to unauthorised people, abuse or other types of use contrary to legislation.
The Data Processor undertakes to observe the statutory requirements in force at any time regarding the processing of personal data. Consequently, data processing shall be carried out in accordance with the rules in force at any time about the processing of personal data, including in particular the Danish Act on the Processing of Personal Data and associated executive orders[1] and instructions.

[1] See for example Executive Order no 528 of 15 June 2000 on security measures to protect personal data processed on behalf of the public administration with subsequent amendments.

The Data Processor shall process information on behalf of the Controller and shall only act on instructions from the Controller. Minimum requirements regarding the necessary technical and organisational security measures shall appear from the instructions.

Furthermore, the Data Processor undertakes to process personal data in accordance with the information security policy covering the Controller, cf. Instructions regarding data processor (see below)

The principles and recommendations in ISO 27001 with subsequent amendments will thus have to be observed in all relevant areas as a framework to the extent that nothing else appears from the present data processor agreement.

3. Ad hoc Workplaces

If the Data Processor carries out data processing from ad hoc workplaces, the Data Processor shall ensure that such workplaces observe the security requirements in the present Data Processing Agreement with Appendices and the relevant IT security texts issued by the Danish Data Protection Agency.

The Data Processor shall among other things observe and document the following:

- Description of the encrypted connection used between the ad hoc workplace and the network of the Data Processor/the Controller
- Use of two-factor authentication
- The Data Processor's internal instructions to his own employees regarding ad hoc workplaces.

At the request of the Controller, the Data Processor shall provide the Controller with sufficient information to enable him to check that the technical and organisational security measures mentioned above have been established. Furthermore, the Data Processor must be able to document that identified vulnerabilities are met through a risk-based assessment.

4. Obligation to Inform and Assist

The Data Processor undertakes to inform the Controller immediately and in writing about any deviation from the requirements in the Data Processing Agreement, for example:

- any deviation from instructions provided
- any deviation from the agreement regarding accessibility
- planned releases, upgrades, tests, etc.
- any suspicion of breach of confidentiality
- any suspicion of abuse, loss and deterioration of data
- any accidental or unauthorised disclosure of or access to the personal data processed according to the present Data Processing Agreement.

The Data Processor and his possible Sub-Data Processors shall immediately assist the Controller in connection with the handling of any application from a registered person, including request for

insight, correction, blocking or deletion of information if the relevant personal data is processed by the Data Processor.

5. Handling of Data after Expiry of the Agreement

The Data Processor and his possible Sub-Data Processors undertake to return and/or delete personal data when the data processing terminates according to agreement with the Controller. The Controller shall inform the Data Processor when the data processing is to stop. The Data Processor shall then be obliged to return and/or delete the personal data on the date stated.

The data shall not be deleted until the Controller has in writing approved the intended procedure for deleting data.

If the Controller does not consider the method sufficiently safe and in accordance with the rules in force on the processing of personal data, the Controller shall inform the Data Processor of the method to be used instead. Reference is made to the IT security text ST3 from 2014 issued by the Danish Data Protection Agency with any updates.

When data has been deleted, the Data Processor shall forward a written statement to the effect that data has been deleted as agreed, including a description of the method used.

Other requirements

E-mail

You must

• use secure and encrypted e-mail if you send personal data

• ensure recipients of personal data can receive secure and encrypted e-mails

Remember that e-mail containing personal data must be erased from the mailbox within 30 days.

Screen saver

You must

• activate the screen saver as it is locked with password / PIN when you leave your computer even for a short period.

Re 2. Technical and organisational security measures

Authorisation and Access Control

In particular, the Data Processor shall observe the following regarding authorisation and access control:

1. Authorisations shall state the extent to which the user may enquire, enter or delete personal data.
2. The Data Processor shall ensure that an appropriate background check according to the circumstances is carried out for any staff members who will in connection with their employment have access to personal data covered by the Data Processing Agreement, regardless of the format in which personal data may be available.
3. Only authorised individuals shall have access to personal data which is processed.
4. Only individuals working with the objectives for which the personal data is processed shall be authorised. Individual users must not be authorised for any use for which they have no need.
5. Furthermore individuals shall be authorised for whom access to personal data is necessary with a view to auditing or operational and system technical tasks.
6. The authorised user shall be provided with user identification and a password to be used for each logon to the system. In principle, two-factor authentication is used for access to systems with sensitive personal data via the Internet or other unsafe networks[2]. The method of authentication may for example be SMS-token, Rfid or similar methods.
7. The Data Processor shall ensure that the Data Processor's employees receive sufficient training and instructions, including but not limited to training aiming at increasing the employee's general security awareness, introduction of relevant security policies and procedures, and access to and training in documented processes and work descriptions, in particular regarding the processing of personal data. Training and instructions shall include the subjects which are relevant in order to ensure that personal data is processed according to legislation as well as the relevant policies and procedures of the Data Processor and the Controller.
8. Authorisation is granted to the Controller's systems by the Controller according to recommendation by the Controller.
9. Measures shall be taken to ensure that only authorised users can get access to personal data and that the user can only get access to the personal data and uses (processing) for which the user in question is authorised.

All employees of the Data Processor employed in electronic data processing shall be provided with user identification and a password with a view to access to the Data Processor's network. User identification and password must be used whenever the user obtains internal access to data processing. External access shall be established by means of two-factor authentication.

[2] This refers to remote access when using ad hoc workplaces

The Data Processor shall have reasonable restrictions regarding physical access. Areas where personal data is processed must by means of the above access control measures be effectively separated from areas to which there is general access.

The Data Processor shall have formal procedures for the resetting of access codes and other situations where the normal logical access control becomes inoperative.

At least every six months it shall be checked that the users have only been granted access according to their needs. This may for example mean that the systems create statistics showing the individual user's use of the system so that it can be established whether authorisations have been issued which are not used and should therefore possibly be revoked. In connection with such statistic follow-up, there will still be a need for a specific assessment of whether the employee still needs access

Without undue delay, the Data Processor shall revoke authorisations (including access) for users who no longer need such authorisation in connection with the user's work.

Checking rejected access attempts and logging

The Data Processor shall observe the following regarding checks of rejected access attempts and logging:

1. All rejected access attempts shall be registered. If within a fixed period a maximum of five consecutive access attempts with the same user identification have been rejected, additional attempts shall be banned. Access shall only be reopened when the reason for the rejected access attempts has been clarified.
2. Machine registration (logging) must be made of all use of personal data covered by section 7 and 8 of the Danish Act on the Processing of Personal Data and section 19 of the Executive Order on Security[3]. The log shall as a minimum contain information about time, user, type of use and statement of the individual to whom the data in question related, or the search criterion used. The log shall be maintained for six months after which it shall be deleted unless a longer period is fixed in accordance with the aim of the log, however, for a maximum of five years, with a view to using it as a tool in the investigation.
3. The stipulation in item 2 shall not be used for personal data included in word processing documents, etc., which are not available in their final form. This also applies to such documents which are available in their final form if the documents are deleted within 30 days. The logging requirement shall continue to be effective in case of routine administration in the form of an EDP register.
4. The stipulation in item 2 shall not apply if the processing of personal data is carried out through software which provides a pre-defined mass processing of personal data or if the data is processed with a view to statistical or research surveys and the identification data has been either encrypted or replaced by code number, etc. In both cases, the user and the time for processing must be logged, cf. item 2.

[3] Act 2000-05-31 no 429 on the processing of personal data and Executive Order 2000-06-15 no 528 on security measures for the protection of personal data processed on behalf of public administration.

Input data material containing personal data

The Data Processor shall observe the following regarding input data material containing personal data:

1. Input data material which is not part of a manual case or a manual register shall only be used by individuals who enter such data. Input data material covered by the stipulation regarding reporting in chapter 12 of the Danish Act on the Processing of Personal Data (i.e. input data material including confidential personal data) shall be stored so that unauthorised individuals cannot get access to the personal data included therein when it is not used.
2. Input data material mentioned in item 1 shall be deleted or destroyed when it is no longer necessary to maintain it considering the purposes covered by the processing or to check the personal data entered.
3. The stipulation in item 2 shall not apply if the material is covered by stipulations about storing/discarding according to other legislation. Input data material filed according to current filing stipulations shall be processed according to the general stipulations on maintenance, including the handing over of files to the State Archives.

When input data material is destroyed, the necessary security measures shall be taken to avoid abuse of the material or disclosure to unauthorised people.

Mobile storage media

The Data Processor shall observe the following regarding mobile storage media, like USBs, NOT LAPTOPS:

1. Mobile storage media with personal data shall be marked and stored encrypted under supervision or locked up when they are not used.
2. Mobile storage media with personal data shall only be handed over to employees and authorised individuals who have access to the personal data with a view to auditing or operational and system technical tasks.
3. A register shall be kept of the mobile storage media used in connection with the data processing.
4. Written instructions shall be prepared for the use and storing of removable mobile storage media.

In connection with repair and service on data equipment containing personal data and in connection with sale and discarding of data media used, the necessary measures shall be taken to ensure that the personal data is not accidentally or deliberately destroyed, lost or deteriorated or that the personal data is disclosed to unauthorised people, is abused or otherwise processed in violation of the Danish Act on the Processing of Personal Data.

Backup copies

The Data Processor shall ensure that backup copies of systems and personal data are made regularly. The backup copies shall be stored safely and so that the backup copies are not lost as a consequence of events leading to loss of original personal data.

The Data Processor shall regularly check that backup copies are legible.

Updates and changes

The Data Processor shall have formal procedures to ensure that updates of operating systems, databases, applications, and other software are assessed and implemented within a reasonable period of time.

The Data Processor shall have formal procedures for the handling of changes with a view to ensuring that any change is appropriately authorised, tested and approved prior to implementation. The procedure shall be supported by an effective separation of functions or management follow-up with a view to ensuring that no individuals can implement a change on their own.

Disruption of operations

The Data Processor shall have documented emergency procedures which will ensure re-establishment of services within a reasonable period of time in case of disruption of operations.

Disposal of equipment

The Data Processor shall have formal procedures in order to ensure an effective deletion of personal data prior to disposal of electronic equipment in accordance with the requirements of the Controller.

Supervision

The Data Processor shall carry out and document supervision to ensure that the Data Processor's organisation observes statutory requirements, policies and procedures.

Re 3. Ad hoc Workplaces

The Data Processor shall not carry out data processing from ad hoc workplaces (remote workplaces or home offices) unless item 15 of the Data Processor Agreement contains a description thereof.

In that case, the Data Processor shall observe the following requirements regarding external communication lines:

1. The Controller shall accept the use of ad hoc workplaces.
2. Two-factor authentication shall be used.
3. External IT communication lines shall only be established if measures are taken according to approval and special agreement to ensure that unauthorised people cannot get access to personal data through such connections.
4. Measures shall be taken to ensure that personal data transmitted via open networks such as the Internet is not lost, changed or is disclosed to unauthorised people during transmission.

5. The Controller shall establish guidelines for the above, stating the special measures to be taken to comply with such requirements.

Re 4. Duty to inform and assist

The Data Processor shall be obliged to inform the Controller without undue delay if a security event has occurred. Such information shall be given immediately after a security event has occurred or has been discovered by the Data Processor.

Such information will therefore typically be divided into two parts.

- Information that an event has occurred

- Information about the detailed circumstances, including but not limited to:

- a situation report
- the personal data which has been compromised
- initiatives which the Data Processor has initiated/intends to initiate