Standard terms for a database for private research approved by the Danish Data Protection Agency.

AUTHORISATION to process personal data

The Data Protection Agency hereby grants authorisation for the implementation of the project, cf. section 50(1)(i) of the Danish Act on Processing of Personal Data. In this connection, the Data Protection Agency lays down the following terms:

General terms

Period of validity: The authorisation is valid until September 1, 2015

1. Hanne Vebert Olesen is responsible for compliance with these present terms.

2. The data can be used for the implementation of the project only.

3. Processing of personal data must be performed only by the controller or at the instance of the controller and at his responsibility.

4. Any person processing personal data must be cognizant of these present terms.

5. The terms must be complied with also where processing is made by a data processor.

6. Facilities used for storage and processing of the data must be organized and fitted up in order to prevent unauthorized access.

7. Data processing must be organized in such a manner that data are protected against accidental or unlawful destruction, loss or impairment. Furthermore, the necessary control should be exercised to ensure that no inaccurate or misleading data are processed. Inaccurate or misleading data or data processed in contravention of the above Act or of these terms shall be rectified or erased.

8. Data must not be kept in a form that makes it possible to identify the data subject for a longer period than is necessary for the implementation of the project.

9. If results from the project are published this must be done so that it is impossible to identify individual persons.

10. It is a condition compliance is made with related terms, if any, laid down in accordance with other legislation.

Electronic data

11. Identification data must be encrypted or replaced by a code number or the like. Alternatively, all data can be stored encrypted. Encryption keys, code keys etc. must be stored securely and separate from the personal data.

12. Access to project data can be obtained only through the use of a confidential password. A password must be replaced at least once a year and when conditions dictate it.

13. If data identifying individuals are transferred over the Internet or other external network, the necessary security measures must be taken to ensure that the data do not come to the knowledge of any unauthorized third parties. As a minimum, the data must be encrypted during transmission. Transmission of sensitive personal data requires strong encryption. When using internal networks, it must be ensured that unauthorized persons are unable to obtain access to the data.

14. Removable storage media, safety copies of data etc. must be stored securely and under lock and so that unauthorized access is prevented.

Manual data

15. Manual project material, including print-outs, failure lists and control lists etc., as well as other material which may directly or indirectly be linked with specific persons, must be stored securely under lock and so that unauthorized access is prevented.

Bio-bank and biological material

16. Samples with biological material and biological material in bio-banks must be stored securely under lock so that unauthorized access is prevented and in such a manner that it is ensured that the material is not lost, impaired or accidentally or illegally destroyed.

17. Biological material marked with civil registration number (CPR-no.) or name must be stored subject to special safety requirements.

18. The project material shall contain internal guidelines for storage of biological material and the guidelines shall be updated at least once a year.

Data to be provided to the data subject

19. Where the personal data are to be obtained from the data subject (through interviews, questionnaires, clinical or para-clinical examination, treatment, observation etc.), detailed data about the project shall be distributed/forwarded to the data subject. The data subject must be informed of the name of the controller, the purpose of the project and of the fact that it is voluntary to participate and that consent may be withdrawn at any time. Where the data are to be disclosed to be used for other scientific or statistical purposes, the data subject shall be advised also of the purpose of the disclosure and the recipient's identity.

20. The data subject shall furthermore be advised that the project is notified to the Data Protection Agency in accordance with Act on Processing of Personal Data, and that the Agency has laid down specific terms to be complied with for the project for the purpose of protecting the data subject's privacy.

Right of access to personal data

21. The data subject has no right of access to the data being processed with regard to himself.

Disclosure

22. Disclosure of data identifying individuals to a third party may take place for other statistical or scientific purposes only.

23. Disclosure may be made only subject to prior approval of the Data Protection Agency. The Data Protection Agency may lay down new terms for the disclosure as well as the recipient's data processing.

24. Disclosure of data may furthermore take place if it appears from other legislation that the data shall be disclosed.

Processing by a data processor

25. The Data Protection Agency's conditions shall apply also to processing made by a data processor.

26. When data are processed by a data processor, a written agreement shall be made between the controller and the data processor. The agreement shall stipulate that the data processor acts on behalf of the controller only and that the data must not be used for the data processor's own purposes. The controller shall furthermore request sufficient data from the data processor to ensure that the Data Protection Agency's terms can and will be complied with.

27. Where the data processor is established in another Member State it shall, furthermore, appear from the agreement that such other regulations on safety measures with regard to data processors that may be in force in the Member State in question, shall apply also to the data processor in question.

Changes of the project

28. The Data Protection Agency shall be notified of significant changes in relation to the project (in the form of a change to an existing notification). Less significant changes may be notified to the Data Protection Agency.

29. *Changes, if any, of the final date of completion of the project shall always be notified.*

Completion of the project

30. At the completion of the project at the latest the data shall be erased, be made anonymous, or be destroyed, so that subsequently it is not possible to identify individuals participating in the project.

31. Alternatively, the data may be transferred for further storage with the State's Archives (including "Dansk Dataarkiv" - Danish Data Archives)

32. The controller shall inform the Data Protection Agency promptly when the project is completed and the data have been erased, made anonymous, destroyed or transferred to the State's Archives.

33. Erasure of data from electronic media shall take place in such a manner that it is impossible to recover the data.

34. (*Special terms for tests/ trials, etc.)* After the completion of the project, data regarding the individual person may, however, if requested by an authority or if to comply with the GCP rules, be kept for the period of time required. A list of participating individuals can be kept as well for the same period of time.

Transfer of data to third countries

35. Transfer of data to third countries, including for the purpose of processing by a data processor and for internal application in the project, requires the Data Protection Agency's prior approval.

36. Transfer may, however, take place without approval of the Data Protection Agency if the data subject has given his explicit consent. The data subject can withdraw his consent.

37. Transfer of data shall take place by courier or registered mail. In case of electronic transmission the necessary security measures shall be taken to prevent unauthorized access. As a minimum, the data must be safely encrypted during the entire transmission.

The above terms shall apply until further notice. The Data Protection Agency reserves the right to take up the terms and conditions for revision at a later date, if required.