INFORMATION ON DATA PROTECTION WITHIN THE BERLIN AGING STUDY

When using the Berlin Aging Study data
we must ask you to observe the following:

1. Data Protection Regulations

Data relating to individuals are subject to the requirements of the German Data Protection Act (BDSG, 20.12.1990) and the Berlin Data Protection Act (BlnDSG, 3.7.1995).

2. Obligations regarding Data Protection within the Berlin Aging Study

All those using Berlin Aging Study (BASE) data within the framework of a special agreement with the Chairman — irrespective of their own legal relationship to the Berlin Aging Study — are obliged to guarantee the protection of the data and to satisfy the requirements of the German Data Protection Act and the Berlin Data Protection Act when working with the data (see above). A document outlining these requirements is attached.

All those using Berlin Aging Study data are also obliged not to use, copy, publish or open the data for any purpose than the scientific project agreed with the BASE Chairman / Steering Committee, and not to transfer these data to any third party.

These obligations remain in force even after the conclusion of the proposed use of the Berlin Aging Study data.

Berlin Aging Study, Max Planck Institute for Human Development,
Lentzeallee 94, 14195 Berlin, Germany, Tel.: ++ 49 30 824 06 - 290, Fax: ++ 49 30 824 99 39

3. Violations of Data Protection Regulations

Violations of the German Data Protection Act can lead to a fine or imprisonment (according to § 43 BDSG and § 32 BlnDSG).

4. Extent of Protected Data

The German Data Protection Act and the Berlin Data Protection Act apply to all stored data relating to individuals, irrespective of the medium used. The law therefore protects data relating to individuals in all forms (for example registers, questionnaires, tapes, floppy disks, compact discs, microfilm, etc.). It also covers all processing methods for such data.

5. General Secrecy Obligations

The above mentioned obligations are not affected by, and do not affect, other statutory secrecy obligations.

Thank you for your cooperation.

Berlin Aging Study, Max Planck Institute for Human Development,
Lentzeallee 94, 14195 Berlin, Germany, Tel.: ++ 49 30 824 06 - 290, Fax: ++ 49 30 824 99 39

BERLIN DATA PROTECTION ACT (BLNDSG): INFORMATION FOR RESEARCHERS

Berlin Aging Study Data can only be transferred to external scientists on condition that these agree to guarantee the protection of the data and to satisfy the legal requirements of the Berlin Data Protection Act when working with the data. The following excerpts from the Act are relevant for scientific research. Berlin Aging Study Data are collected and processed in accordance with these requirements. External scientists are also obliged to adhere to the following requirements when processing Berlin Aging Study Data.

1. Purpose and subject of data protection

a) The purpose of data protection is to regulate the processing of personal data in order to
(1) protect the rights of the individual and
(2) ensure that constitutional laws are not endangered by automatic data processing.

b) The Act protects personal data which are compiled, stored, modified, communicated, blocked, erased or used in any other way by public authorities or other public establishments.

2. Field of Application

The Act protects the utilization of personal data in all public authorities and other public establishments in Berlin. The same is valid for physical and legal persons, companies or other private-law associations involved in public administration.

3. Definitions

a) For the purpose of the Act, personal data means details about the personal or material circumstances of an identified or identifiable physical person (the person concerned). The same is valid for deceased persons unless the interests of the person concerned can no longer be damaged.

b) Data processing is the compilation, storage, modification, communication, blocking, erasure and utilization of personal data. For the purpose of the Act
(1) *compilation* is the collection of data about the person concerned,
(2) *storage* is the acquisition, recording or retention of data on a storage medium,
(3) *modification* is the alteration of the contents of stored data, irrespective of method used,
(4) *communication* is the passing of stored data or data acquired directly by means of data processing to third parties in such a way that the data are communicated by the processing unit to the third party or are held ready for recall by the third party,
(5) *blocking* is the prevention of further processing of stored data,
(6) *erasure* is the deletion of stored data,
(7) *utilization* is any other use of personal data.

c) For the purposes of the Act
(1) a *processing unit* is any public authority or other public establishment which processes data on its own account or has data processed by others;
(2) a *third party* is any person or establishment outside the processing unit, with the exception of the person concerned;

(3) a *data file* is a collection of data which can be processed automatically (automated data file) or a collection of data which is assembled on a uniform basis and can be arranged and evaluated according to specific features (non-automated data file);
(4) a *file* is any further document for official use including pictorial and sound recordings.

4. Technical and organizational measures

Every public authority or establishment which processes personal data is obliged to take the technical and organizational measures necessary to guarantee the implementation of the provisions of the Act. The precise measures to be taken are dependent on the current state of technology.

If personal data are processed in *non-automated data files*, particular measures must be taken to prevent third party access to these files when they are processed, stored, transported or destroyed.

If personal data are processed *automatically*, adequate measures must be taken to
(1) prevent third party admittance to the data processing equipment (admittance control),
(2) prevent the unauthorized reading, copying, modification or removal of storage media (storage medium control),
(3) prevent unauthorized entries in the database memory and the unauthorized reading, modification or erasure of personal data (memory control),
(4) prevent the unauthorized use of data processing systems via data communications equipment (user control),
(5) guarantee that the users of the data processing systems only have access to the data for which they have been granted authorization (access control),
(6) record the communication of data — what was transmitted to whom, and when? (communication control),
(7) guarantee that it is later possible to check and establish which personal data were input by whom into which data processing system (input control),
(8) guarantee that personal data processed on behalf of third parties are processed according to the instructions of the client (third party control),
(9) prevent unauthorized reading, copying, modification or erasure of data which is communicated or transported by data carrier (transport control),
(10) ensure that the internal organization of the public authority or establishment is such that data protection regulations can be observed (organization control).

5. Admissibility of data processing

a) The processing of personal data is only admissible if
(1) a legal provision permits it or
(2) the person concerned has given his / her consent.
Sentence (1) is only valid if the regulation guarantees data protection analogous to that set out in the Berlin Data Protection Act.

b) If the data processing relies on the consent of the subject, he / she must be adequately informed of the consequences of this consent, and about how the data will be put to use. If communication of the data is planned, the subject must be informed of the recipient and the purpose of the data communication. The subject must be informed that he or she has the right to refuses to give consent.

c) Consent must be given in writing unless special circumstances prevent this. Where consent

is given in writing together with other declarations, the person concerned must be informed of this in writing.

d) Consent is null and void if it was given due to threats or lack of information.

6. Data secrecy

a) Persons engaged in data processing for public authorities and other public establishments, either on their own account or for others, must not process personal data without authorization.
b) On taking up their duties, such persons must be required to undertake to abide by these regulations. This undertaking continues to be valid after termination of their activity.

7. Necessity

a) The processing of personal data is only admissible if it is necessary for the legitimate accomplishment of the assigned task.
b) If personal data are compiled in files such that the separation of necessary and unnecessary data is not possible or a disproportionate amount of work is involved in separating them, then communication of these unnecessary data within the processing unit is admissible, but their utilization is forbidden.

8. Data compilation

a) Personal data must be compiled from the person concerned with his / her consent.
b) When personal data are compiled with the consent of the person concerned, he / she must be adequately informed of the aim of the investigation and of the recipient of the data.
c) Public authorities and other public establishments may compile data without the consent of the person concerned when
(1) a legal provision permits it,
(2) the person concerned has consented to this form of infomation compilation or
(3) the person concerned cannot be informed in time and there is no reason to believe that his / her interests will be damaged.

9. Predetermination of purpose

a) Personal data may only be processed for the purpose for which they were originally compiled or stored.
b) Personal data may only be processed for purposes other than those for which they were originally compiled or stored if
(1) a legal provision permits it or
(2) the person concerned has given his / her consent.
c) If personal data are compiled in files such that the separation according to purpose is not possible or a disproportionate amount of work is involved in separating them, then they do not have to be separated, but the utilization of those data not necessary for the relevant purpose is forbidden.

10. Communication of data within the public sector

The communication of personal data to public authorities and other public establishments is admissible if

(1) a legal provision permits it or
(2) the person concerned has given his / her consent.
The communication of personal data to public authorities and other public establishments is also admissible if the recipient requires the data in order to accomplish the task for which the data were gathered and if it is necessary for the legitimate accomplishment of the tasks for which the communicating unit or the recipient is competent.

11. Data processing for scientific purposes

a) For the purpose of scientific research, data processing units are only able to communicate personal data *without consent* of the person concerned for certain research projects
(1) if, due to the type of data or the tye of use, the interests of the person concerned are not damaged, or
(2) if the public interest in the accomplishment of the research project considerably outweighs the interests of the person concerned and the research project cannot be accomplished in any other way. The communication of data under this provision must be approved by the Berlin state authorities.

b) As far as the research project allows, features which would allow the identification of the person concerned must be stored separately, and must be erased as soon as the project is completed.

c) The processing of data for any other than authorized research purposes is not admissible. The data may only be communicated to third parties with the written consent of the persons concerned.

d) If these regulations do not apply to the recipient, he or she may only receive personal data if he or she guarantees to satisfy the requirements of the Berlin Data Protection Representative.

e) Public establishments may only publish personal data if
a) the person concerned has given his / her consent or
b) this is imperative for the portrayal of research results on contemporary themes.

f) The processing unit itself may process personal data for research purposes without the consent of the person concerned
(1) if, due to the type of data or the tye of use, the interests of the person concerned are not damaged, or
(2) if the public interest in the accomplishment of the research project considerably outweighs the interests of the person concerned and the research project cannot be accomplished in any other way.

12. Offences

a) Any unauthorized person who
(1) communicates or modifies personal data or
(2) retrieves or procures personal data from data banks in sealed containers is liable to a term of imprisonment not exceeding one year, or to a fine.

b) If the offender commits the offence in exchange for payment or with the intention of enriching himself / herself or another person or of harming another person, he / she is liable to a term of imprisonment not exceeding two years, or to a fine.

c) Such offences are prosecuted only if a complaint is filed. The data protection representative is also entitled to file a complaint, even against the will of the person concerned.