Guidance Notes – Data Protection and Confidentiality Obligations

These guidance notes are intended to provide information on the data protection and confidentiality provisions set out in the Berlin Data Protection Act (BlnDSG) of 17 December 1990. Under Section 8 (§ 8) of the BlnDSG, you have a duty to protect data confidentiality. You would not want unauthorized individuals gaining access to your personal data (i.e. information regarding your personal or material circumstances), so please ensure that you safeguard the security and confidentiality of any personal data which you process as part of your (professional) role. This also means that you are only permitted to process personal data as part your work at Charité if you have been authorized to do so. This obligation continues even if you move into a different position at Charité or if you leave your job.

Purpose of data protection
Data protection refers to the basic right of the individual to determine which data are to be processed, used, or collected, as well as how and when they are to be processed, used, or collected, and who is authorized to do so.

Fundamental principles
The following fundamental principles should be noted:

Purpose limitation
Personal data may only be processed for the purposes specified prior to the data being obtained. Changes to the purpose of data processing are possible, but only to a limited extent. Any such changes must have a legal basis; otherwise, it is necessary to have the consent of the data subject

Transparency
The data subject must be informed as to how their personal data will be used. This includes informing them of the purpose of data collection, the identity of the institution responsible and, where necessary, the identity of any third parties with whom the data may be shared.

Data minimization
Personal data must not be held for longer than necessary, i.e. they must not be stored for future purposes, except where there is a legal basis. Personal data must be deleted in accordance with the relevant retention periods.

Accuracy/Accessibility
Personal data must be accurate when collected, must be kept up-to-date while being stored, and must be accessible.

Subsidiaries and external parties
Legally speaking, the transfer of personal data to subsidiaries constitutes a disclosure of data to a third party. Any transfer of personal data to a third party must have a legal basis; otherwise, it is necessary to have the consent of the data subject.

Personal data
The term 'personal data' refers to any details about the personal or material circumstances of an identified or identifiable individual, including their name, date of birth, education, and health status, as well as financial and family circumstances. Data are classed as personal data even when the name of the individual is not known, if the process required to identify them (for instance, using their staff number or patient number) is not excessively cumbersome. Photos, video recordings, x-rays, and audio recordings may also contain personal data.

Data processing
The term 'data processing' is comprehensive in its scope; under Section 4 of the Berlin Data Protection Act (§ 4 BlnDSG), it is defined as referring to the processing, collection, storage, modification, transfer, blocking, deletion, and use of personal data.

Unauthorized processing
'Unauthorized processing' refers to any processing of personal data for purposes other than the purpose for which they were provided. This means that you must only process personal data if this is permitted or required by the BlnDSG or by other legal provisions, or if the affected person has given their consent. Breaches of data protection and confidentiality regulations are punishable under the Berlin Data Protection Act and other legal provisions, and may result in compensatory damages, claims for compensation or injunctive relief, imprisonment, or a fine.

Please see below for a summary of the most important legal provisions pertaining to this issue. Please read these carefully. When signing your contract, you will be asked to sign a statement confirming that you will comply with all relevant data protection regulations.

If you have any questions regarding data protection and confidentiality, please contact Charité's Data Protection Officer, who will be happy to help: datenschutz@charite.de.

Excerpt from the Law to Protect Personal Data in the Berlin Administration
(Berlin Data Protection Act - BlnDSG)
as of 17 December 1990

Section 1
Purpose and Object of Data Protection

(1) The purpose of this Act is to regulate the processing of personal data by public authorities and other public agencies in order to

1. Protect the right of each individual to self-determine the disclosure and use of his or her data, unless any restrictions are permitted by this Act or by other legislation (informational self-determination),
2. To protect the constitutional order based on the principle of the separation of powers against any risk caused by automated data processing.

(2) This law protects personal data collected, stored, modified, transferred, blocked, deleted or otherwise used by public authorities or other public bodies.

Excerpt Section 4
Definitions

(1) For the purposes of this Act, personal data shall mean details about personal or material circumstances of an identified or identifiable natural person (data subject). The same applies to data on deceased persons, unless the legitimate concerns of the data subject can no more be affected.

(2) Data processing shall mean the processing, collection, storage, modification, transfer, blocking, deletion and use of personal data. For the purposes of the following provisions

1. Data collection shall mean the acquisition of data about the data subject
2. Data storage shall mean capturing, recording or storing data on a data storage medium,
3. Modification shall mean changing the contents of stored data, regardless of the method used to do so,
4. Transfer shall mean the disclosure to third parties of data stored or obtained by processing of obtained data in such a way that the controller submits the data to such third party or that the third party retrieves the data prepared for retrieval,
5. Blocking shall mean preventing further processing of stored data,
6. Deletion shall mean to eliminate stored data,
7. Use shall mean any other use of personal data.

Section 8
Data Confidentiality

(1) The personnel of authorities and other public bodies who process data for these bodies or on behalf of others, is not allowed to process any personal data without authorization. For the staff of private contractors of public bodies who have official access to personal data that requirement shall be ensured by contract.

(2) The personnel shall be subjected to the requirements of paragraph 1 upon starting their job. Their obligations shall persist after the termination of their job.

Section 18
Indemnification and Injunctive Relief

(1) If the data subject's legitimate interests have been affected by any data processing that is unlawful under this Act or under any other data protection legislation, the authority or other public body which processed or had processed the data according to section 3 paragraph 1 shall compensate the financial losses incurred. If there are more infringements of the law to be apprehended, the data subject may claim an injunction. In severe cases the data subject may also claim reasonable pecuniary compensation for immaterial damage.

(2) Where several institutions are involved in automated processing and the institution which stored the data cannot be identified, each of those institutions shall be liable.

(3) Claims for indemnification and injunctive relief on the basis of other regulations shall remain unaffected.

§ 30
Data Processing for Scientific Purposes

(1) For scientific research purposes and exclusively for specific research works data-processing bodies may transfer personal data without the consent of the data subject,

1. Provided that because of the nature of the data, their notoriety or the type of the use his legitimate interests are not affected, or
2. if the public interest in carrying out the research project considerably outweighs the legitimate concerns of the data subject and provided that the purpose of research may not be achieved otherwise.

Such transfer shall require the prior consent of the supreme state authority or a body assigned by it; which not apply to public bodies according to section 2 paragraph 3. Such consent shall specify the recipient, the type of personal data to be transferred, the group of data subjects and the research project and shall be communicated to the Berlin Commissioner for Data Protection and Freedom of Information..

(2) As soon as the research purpose so allows, the characteristics required to relate the data to the data subject shall be stored separately and such characteristics shall be erased, as soon as the research purpose is achieved.

(3) Any processing of the data submitted under paragraph 1 for purposes other than research purposes shall be forbidden. The data transferred according to paragraph 1 sentence 2 must not be transferred further, unless with the consent of the data subject

(4) To the extent the provisions of this Act do not apply to the recipient, personal data may be transferred only if the recipient undertakes to comply with the provisions of paragraphs 2 and 3 and submits to the control of the Berlin Commissioner for Data Protection and Freedom of Information.

(5) The public bodies performing scientific research may publish personal data only provided that

a) the data subject has consented, or
b) this is essential for the presentation of research findings on events of contemporary history.

(6) Under the provisions of paragraph 1 the data-processing institution may process personal data for the purpose of scientific research without the consent of the data subject himself.

§32
Criminal Offences

(1) He who
1. Transfers or changes or
2. Retrieves non-obvious personal data or obtains files from locked containers without authorization

shall be punished with imprisonment of up to one year or a fine.

(2) If the offender acts for remuneration or with the intention to enrich himself or another person or to harm another person, the punishment shall be imprisonment for up to two years or a fine.

(3) The offence shall be prosecuted only upon request. The person eligible to demand prosecution shall be the data subject. Prosecution may also be demanded by the Berlin Commissioner for Data Protection and Freedom of Information. The Berlin Commissioner for Data Protection and Freedom of Information may demand prosecution even against the will of the data subject.