# Brandenburg Act for the Protection of Personal Data (Brandenburg Data Protection Act – BbgDSG)

**in the version published on May 15 2008 (GVBl. I S. 114), last amended by the Fourth Amendment Act for the Brandenburg Data Protection Act and Other Legal Provisions on May 25 2010 (GVBl. I No. 21)**

## Contents

**Part 2**
**Commissioner of the State of Brandenburg for Data Protection and Access to Information**



**Part 3**
**Special data protection**



**Part 4**
**Administrative offences, criminal offences; transitional provisions**

# Part 1
# General data protection

## Chapter 1
## General provisions

### Section 1
### Purpose

The purpose of this Act is to prevent the impairment in an inadmissible form of the basic right possessed by the individual to make decisions him/herself about the divulgement and utilisation of his/her personal data, which results from the processing of his/her personal data by public bodies (right of informational self-determination).

### Section 2
### Scope of application

(1) This Act shall apply to public authorities, institutions and other public bodies of the State, the communities and associations of local authorities, as well as to other legal persons under public law and their associations (public bodies) subject to monitoring by the State, the communities and associations of local authorities, insofar as these process personal data. This Act shall apply to the courts and to public prosecution authorities, insofar as these perform administrative duties; furthermore, only the provisions of Part 2 of this Act shall apply to public prosecution authorities, provided these do not perform administrative duties. If a private body performs the sovereign duties of a public body of the State, it shall be regarded as a public body for the purposes of this Act.

(1a) The State Parliament, its committees, members, factions, its administration and its employees shall not be subject to the provisions of this Act, with the exception of Section 31, insofar as they process personal data in the course of performing parliamentary duties. For this purpose, the State Parliament shall enact a data protection ordinance, taking its constitutional status and the basic elements of this Act into consideration.

(2) The provisions stipulated in Part 2, Sections 7a, 8, 10a. 21, 23 and 25 to 30 of this Act shall apply, insofar as

1. commercial enterprises of the communities or the associations of local authorities without their own legal entity (owner-operated businesses),

2. public utilities managed via owner-operated businesses in accordance with the corresponding regulations,

3. State enterprises,

4. competing legal persons under public law subject to monitoring by the State, the communities and the associations of local authorities,

process personal data for commercial purposes or objectives. Otherwise, the provisions of the Federal Data Protection Act applying to non-public bodies, including provisions governing criminal and administrative offences, shall apply, with the exception of Sections 4d to 4g and 38.

(3) The provisions of this Act shall take precedence over those of any administrative procedures act of the State of Brandenburg, insofar as personal data is processed during the course of the investigation into the facts. Furthermore, special legal provisions applying to the processing of personal data shall take precedence over the provisions of this Act.

## Section 3
## Definitions

(1) “Personal data” means particulars regarding the personal or material circumstances of an identified or identifiable individual (data subject).

(2) “Data processing” means the collection, storage, modification, transference, blockage, erasure or use of personal data. In particular,

1. “collecting” (“collection”) means the procurement of data regarding the data subject,

2. “storing” (“storage”) means the collection, recording or retention of data on a data storage medium for the purpose of further processing,

3. “modifying” (“modification”) means rearranging the substance of stored data,

4. “transferring” (“transference”) means the disclosure of data to third parties in such a way that the data has been passed on to the third party, or that data stored for inspection or retrieval has been inspected or retrieved by the third party,

5. “blocking” (“blockage”) means preventing the further processing of stored data,

6. “erasing” (“erasure”) means deleting stored data,

7. “using” (“use”) means any other utilisation of personal data,

regardless of the procedure applied.

(3) For the purpose if this Act,

1. “anonymisation” means modifying personal data to the extent that the particulars regarding personal or material circumstances can no longer be attributed to any identified or identifiable individual, or should this only be possible with a disproportionate amount of time, expense and labour, and

2. “pseudonymisation” means the replacement of a name and other identifying characteristics with a sign in order to exclude or significantly impede the determination of the data subject,

3. “encryption” means the replacement of clear text or characters with others in such a way that the clear text can only be made legible again with a disproportionate amount of expenditure,

4. “mobile media for the storage and processing of personal data” means a data storage medium

    a) which is intended to be utilised by the data subject,

    b) on which data can be processed with automated means beyond the initial storage phase or with which data can be automatically processed, and

    c) whose processing according to letter b is carried out by a body other than the data subject and this processing can only be influenced through the utilization of the medium by the data subject.

5. “maintenance” means the sum of measures to ensure the availability and integrity of hardware and software for data-processing equipment; this includes the installation, maintenance, inspection and correction of software, as well as the inspection, repair and replacement of hardware,

6. “remote maintenance” means the maintenance of software and hardware for data-processing equipment, which is executed at a location outside the body processing the personal data, and which utilises data communication equipment.

(4) For the purpose of this Act,

1. “data-processing body” means any public body which processes data on its own behalf, or has data processed by others,

2. “recipient” means any person or body that receives data and

3. “third party” means any body with the exception of

    a) the data-processing body itself,

    b) the data subject,

    c) contractors in the cases defined by Section 11 and Section 11a,

    d) persons authorized to process data through the immediate responsibility of the data-processing body or contractor in compliance with letter 'c)'.

(5) Data processing can be described as “automated” if it can proceed independently through the use of a controlled technical procedure.

(6) “Data-file” means a collection of personal data which can be analysed through automated procedures (“automated data file”), or any other similarly structured collection of personal data which can be ordered and analysed in accordance with specific characteristics (“non-automated data file”).

(7) A “record” means any other document serving official purposes; this also includes image and sound recording media, provided they are not data files as described in paragraph 6. It does not include drafts and notes that are not intended to constitute part of a procedure and will soon be destroyed.

## Section 4
## Admissibility of data processing

(1) The processing of personal data shall be admissible only if

1. the voluntary and express approval (consent) of the data subject has been obtained or

2. to the extent this would be admissible in accordance with the present Act or other legal provisions.

(2) Consent must be rendered in written form, provided no special circumstances warrant another form. If consent is to be supplied together with other written declarations, the data subject shall be particularly made aware of the declaration of consent in writing. The data subject shall be appropriately informed of the implications of his/her consent, especially regarding the use of the data and, in the case of any intended transference of his/her data, about the recipient of the data and the purpose of the transference; he/she shall be advised that he/she is entitled to refuse consent and to revoke it with effect for any future time.

(3) Consent may also be declared electronically if it is guaranteed that

1. it can only be declared through a clear and conscious action of the data subject,

2. it cannot be made unrecognisable,

3. the author can be identified,

4. the consent is recorded and

5. the data subject can obtain information about the contents of the consent at any time, without entailing disproportionate effort.

(4) Any decision which leads to legal repercussions or to considerable impairment of the data subject is inadmissible, if this is based on the assessment of specific characteristics of his/her person created exclusively through the automated processing of his/her data. A decision as per clause 1 may be admissible by law if it ensures that the legitimate interests of the data subject are preserved.

(5) If personal data in records is interconnected in such a way as to make its division into required and unrequired data - including through duplication or deletion - impossible, or only possible with disproportionate effort, the perusal, passing on within the data-processing body, and the transference of personal data not required for the fulfilment of the respective task shall also be admissible, provided the legitimate interests of the data subject or of a third party do not prevail in this context. Accordingly, the unrequired data shall be subject to a utilisation ban.

## Section 4a
## Processing particular categories of personal data

Provided that other legal provisions do not expressly allow for, or presuppose with statutory force, the processing of personal data regarding racial and ethnic background, political opinion, religious or ideological convictions, union membership, health status or sexual activity, shall only be admissible

1. if the data subject has expressly consented,

2. on the basis of Sections 15, 28, 29, 31, 33a, 33b and 33c, or

3. if it is for the protection of vital interests on the part of the data subject or a third party, and the data subject is unable to provide his/her consent due to legal or effective reasons.

The processing of this data is only permissible if it is obvious that the data has been made public by the data subject.

## Section 4b
## Right of objection of the data subject for special reasons

If the data subject can establish in writing that the lawful processing of his/her data conflicts with a specific legitimate personal interest, the processing of the data shall only be admissible if - in the individual case - public interest in the data processing outweighs the personal interests of the data subject. The data subject shall be informed of the result in writing, and the reasons shall be given.

## Section 5
## Rights of the data subject

(1) In accordance with this Act, every individual is entitled to

1. the access to information and notification regarding stored data about his/her person, as well as the inspection of records (Section 18),

2. counter-response due to a legitimate and specific personal interest (Section 4b),

3. the inspection of the procedures list (Section 8 paragraph 4),

4. the rectification, erasure or blockage of his/her stored personal data (Section 19),

5. appeal to the Commissioner of the State of Brandenburg for Data Protection and Access to Information (Section 21 paragraph 1).

These rights cannot be effectively waived by the data subject.

(2) If data involving the data subject is stored through an automated procedure in which several bodies are authorized to store the data, he/she may appeal to any of these bodies. This body shall be obliged to forward the petition of the data subject to the data-processing body. The data subject shall be informed about the forwarding and the data-processing body in question. Insofar as they store personal data in fulfilment of their statutory duties to monitor and audit within the scope of application defined by the Fiscal Code, the bodies named in Section 19 paragraph 3 of the Federal Data Protection Act, public prosecution authorities, the police and fiscal authorities may inform the Commissioner of the State of Brandenburg for Data Protection and Access to Information, instead of the data subject, about the forwarding and the data-processing body in question. In this case, further procedures shall be conducted in accordance with Section 18 paragraph 6.

## Section 6
## Confidentiality

Persons in public bodies or their contractors, who have access to personal data for official purposes, shall be prohibited from processing or disclosing such data in an unauthorized manner for any purposes other than those related to the lawful fulfilment of their specific duties. These persons are obliged to maintain confidentiality, even after their activities have been concluded.

## Section 7
## Securing data protection

(1) The highest State authorities, communities and associations of local authorities, as well as other legal persons under public law subject to monitoring by the State and their associations, shall ensure the implementation of this Act and other data protection provisions in their respective fields of activity. They shall conceive procedures for the processing and use of personal data which pursue the objective of making the processing and use of such data unnecessary, or of limiting the processing and use of such data as much as possible. Data processing shall be structured so as to enable the distinction of data according to the respective objectives pursued and the various data subjects involved during processing, but especially during the transference of data, the perusal of data within the context of fulfilling duties, and the inspection of data.

(2) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be consulted before legal and administrative provisions concerned with the processing of personal data have been enacted. The Commissioner shall be informed in due time about plans of the State for the establishment or significant alteration of automated information systems, insofar as personal data is to be processed by the systems.

(3) The first use of automated procedures for processing personal data, or their first essential alteration, which require the compilation of a procedures list in compliance with Section 8, shall require written clearance. This shall only be granted if

1. a security plan developed from a risk analysis has ascertained that the dangers for the rights and liberties of the data subjects, which have arisen from these procedures, can be brought under control through technical and organisational measures in accordance with Section 10 paragraphs 1 and 2, and

2. prior checking in compliance with Section 10a has ensued in connection with procedures which engender significant risks for the rights and liberties of the data subjects.

The determination of the technical and organisational measures to be implemented shall be repeated at appropriate intervals in compliance with standards of technological development. Clearance for common

procedures in their entirety or in parts shall be granted by the bodies designated by the participating bodies in accordance with Section 9 paragraph 1a clause 1. Clearance may also be granted by the highest responsible State authority, or by another body designated by the latter.

## Section 7a
## Data protection official

(1) Data-processing bodies shall appoint a data protection official. Only persons may be appointed who are endowed with the required specialist knowledge and reliability for fulfilling their duties, and who will not be exposed to any conflict of interests with other official duties through this activity. His/Her appointment can only be revoked against his/her will for an important reason in compliance with Section 626 of the German Civil Code.

(2) Data-processing bodies may appoint employees of another data-processing body as the data protection official.

(3) In this function, the data protection official may appeal directly to the management of the data-processing body. He/She shall be independent in his/her role as the data protection official. He/She may not be disadvantaged due to the fulfilment of his/her tasks. In case of doubt, the data protection official may directly approach the State Commissioner for Data Protection and Access to Information.

(4) The data protection official shall be bound to secrecy in respect to the identity of the data subject and any circumstances allowing conclusions to be drawn about the data subject, provided he/she has not been released from this obligation by the data subject.

(5) The data protection official shall have the task of supporting data-processing bodies in implementing data protection provisions. His/Her tasks include, in particular:

1. to work towards the observance and enforcement of data protection provisions,

2. to familiarize those persons active in processing personal data with the provisions of this Act and other legal regulations relevant to the data-processing body, and

3. to support the data-processing body in implementing the required measures in accordance with Section 7 paragraph 3 and Sections 8, 10, 11, 11a and 26, and

4. to execute prior checking as per Section 10a.

He/She may inspect such processing procedures concerned with personal data which are required for the fulfilment of his/her duties. Professional secrecy or official confidentiality of a special nature cannot be used as objections against him/her.

## Section 8
## Procedures list

(1) As regards the automated processing of personal data, the data-processing body shall compile a procedures list in written or electronic form, which contains:

1. the description of the procedure,

2. the name and address of the data-processing body,

3. the purpose and legal basis of the data processing,

4. the data subjects involved and their corresponding data or data categories,

5. the recipients or recipient categories to whom the data will be transferred,

6. the intended transfers of data in compliance with Section 17 paragraph 2.,

7. in the case of Section 11: the contractor,
8. standard periods for the blockage and erasure of data,

9. a description of measures in compliance with Section 10,

10. a general description regarding the type of data-processing equipment to be used and of the software to be implemented, and

11. the declaration of clearance, and if relevant, results from the prior checking.

In cases defined by Section 7 paragraph 3 clause 5, the determinations required by clause 1 may be made by the highest State authority, or by a body designated by the latter.

(2) The data protection official shall be charged with keeping the procedures list.

(3) The procedures list shall be updated in the event of significant alterations.

(4) Details in the procedures list in accordance with paragraph 1 may be inspected by anyone at the data-processing body free of charge. This shall not apply to the details as per paragraph 1 no. 7 to 11, insofar as this would negatively affect the security of the procedure. Clause 1 shall not apply to

1. procedures undertaken by authorities for the protection of the Constitution,

2. procedures serving the aversion of danger or criminal prosecution and

3. procedures for the investigation of tax offences,

insofar as the data-processing body declares the inspection of data to be irreconcilable with the fulfilment of its duties in the individual case.

(5) Paragraph 1 shall not apply to

1. procedures whose sole purpose is to keep a register intended for the general information of the public, or which are open to inspection by all persons who can substantiate a warranted interest,

2. procedures, insofar as they are used to compile such sets of data for temporary use which will be erased within three months after their compilation,

3. procedures that function through the utilisation of standard commercial writing programmes,

4. procedures that exclusively serve data protection and data protection regulation,

5. procedures that exclusively serve to locate other procedures, applications or records (registry procedures).

6. procedures that exclusively serve the monitoring of time periods and deadlines,

7. lists of rooms, inventory and software,

8. library catalogues and indexes for information sources, or

9. lists of addresses which are exclusively used for the transference of information to data subjects.

(6) The State Government shall be authorized to regulate particulars of the procedures list through legal enactment, especially for the purpose of simplifying the procedure and to relieve the data-processing body.

## Section 9
## Concurrent procedures, automated retrieval and regular data transference

(1) The establishment of an automated procedure facilitating the processing of personal data through several data-processing bodies based upon a common database (concurrent procedure), or the transference of personal data to third parties through data retrieval procedures (automated data retrieval procedures), may be established only insofar as this procedure is appropriate in relation to the legitimate interests of the data subject and the duties of the involved bodies. Legal provisions concerning the admissibility of individual data retrieval procedures remain intact. The State Commissioner for Data Protection and Access to Information must be informed in advance.

(1a) Prior to the establishment of a concurrent procedure, the participating bodies must designate a body for the planning, installation and execution of the concurrent procedure, thereby committing in writing

1. the official title and duties of the participating bodies, including the responsibility for clearance decisions in accordance with Section 7 paragraph 3, as well as those areas within the processing sector for which these bodies must bear responsibility in a specific case, and

2. the technical and organisational measures which must be taken in order to execute the concurrent procedure in compliance with Section 10 paragraph 2.

The body entrusted with the execution of the concurrent procedure must maintain in its safekeeping a double of the procedures list which must be kept by each of the participating bodies in accordance with Section 8, including the information required by clause 1 number 1. Section 8 paragraph 4 applies accordingly.

(1b) Data subjects may exercise their rights as defined by Section 5 paragraph 1 numbers 1 to 4 in respect to each of the bodies participating in the concurrent procedure, irrespective of which of these bodies is responsible for processing the data in the specific case. The body which the data subject has approached must forward the corresponding petition to that body responsible for the specific case. The right of access to information according to Section 18 also extends to the information defined by paragraph 1a clause 1 number 1.

(2) The bodies involved in an automated data retrieval procedure must ensure that the admissibility of such data retrieval procedures can be regulated. In addition to this, the bodies must commit to writing:

1. the motivation and purpose of the data retrieval procedure,

2. the recipient of the data,

3. the type of data to be transmitted, as well as

4. the technical and organisational measures in compliance with Section 10.

The required determinations may also be made by the supervisory authorities.

(3) The recipient of the data shall assume responsibility for the admissibility of the individual data retrieval procedure. The transferring body shall only examine the admissibility of the retrieval provided that sufficient grounds exist. The transferring body shall examine the transference of personal data by means of suitable random sampling procedures.

(4) Paragraph 1 clauses 1 and 2, as well as paragraphs 2 and 3, shall correspondingly apply to the establishment of automated data retrieval procedures by a public body.

(5) Paragraphs 1 to 3 shall not apply to data stock open to use for persons without any authorization, or with special rights of access, or for data stock whose publication would be admissible.

(6) Paragraphs 1 and 2 to 5 shall apply correspondingly to the admission of regular data transferences.

**Section 10**
**Technical and organisational measures**

(1) Data-processing bodies, or bodies acting on their behalf, shall take the technical and organisational measures required by paragraphs 2 and 3 in order to ensure the implementation of the provisions put forth by this Act. The measures shall be appropriate to the desired purpose of protection, and shall be determined by the risks to be taken into consideration in the individual case and the respective standard of technical advancement .

(2) If personal data is to be processed through automated procedures, appropriate measures shall be taken to ensure that

1. only authorized persons can gain access to this data (confidentiality),

2. this data remains undamaged, complete and current during processing (integrity),

3. this data is accessible in a timely manner and can be processed with standard procedures (accessibility),

4. this data can be attributed to its original source at all times (authenticity),

5. it can be ascertained who has processed what personal data, as well as when and in which manner this was done (revisability),

6. the procedural method used to process this data is complete, current and documented in such a way that it can be comprehended within an acceptable length time (transparency).

(3) If personal data is not processed by automated procedures or is processed in records, measures shall be especially taken to prevent unauthorized access during its processing, storage, transportation and destruction.

**Section 10a**
**Prior checking**

(1) The processing of personal data in automated procedures, which engender special risks for the rights and liberties of data subjects, shall be subject to investigation (prior checking) by the data protection official. In cases defined by Section 2 paragraph 3 clause 4, prior checking may be carried out by the data protection official of the highest State authority, or by a body designated by the latter.

(2) Prior checking shall be executed most particularly insofar as

1. a procedure defined by Section 9 paragraph 1 is involved, or mobile media for the storage and processing of personal data have been implemented, or

2. the procedure involves the processing of personal data belonging to one of the categories defined by Section 4a, or is subject to professional secrecy or official confidentiality of a special nature.

(3) In order to execute prior checking, the necessary documentation, especially the results of the risk analysis and the security plan, as well as the procedures list as per Section 8, shall be sent to the data

protection official. In case of doubt, he/she must consult the Commissioner for Data Protection and Access to Information.

**Section 11**
**Processing of personal data on commission**

(1) If personal data is processed on commission for a data-processing body (client) by other persons or bodies (contractors), the commissioning body shall remain responsible for the enforcement of the provisions of this Act and other data protection provisions. The rights of the data subject shall be asserted in relation to this body. To the extent the provisions of this Act cannot be applied to the contractor, the client shall be obliged to ensure in contractual form that the contractor observes the provisions of this Act and facilitates at all times the controls he/she has initiated.

(2) The commission shall be issued in written form and must determine an object, the scope of data processing, technical and organisational measures, and eventual subcontracting arrangements. The contractor must offer guarantees for the enforcement of the technical and organisational measures as defined by Section 10. Should data with existing legal or other confidentiality obligations be processed on commission, special technical and organisational measures must be taken to ensure the preservation of secrecy. The commission may also be issued by the supervisory authority, which would then be effective for those public bodies of the State subject to its supervision; these bodies must be instructed about this development.

(3) The contractor may only process the personal data within the instructional framework of the commissioning body.

(4) If the contractor is a body as described in Section 2 paragraph 1 clause 1 or 2, only Sections 6, 7a, 10 and 11a, as well as 21, 23, 25, 26, and 38 shall apply to the contractor.

(5) In order to execute consulting or appraisal tasks on commission for the data-processing body, the transference of personal data is admissible provided that the transferring body commits the commissioned persons

1. to processing the data only for the purposes for which it was entrusted to them, and

2. to returning the data entrusted to them after the commission has been completed, and to erasing the stored data in their possession, unless special legal provisions forbid this.

Paragraphs 1 to 3 shall apply correspondingly.

**Section 11a**
**Maintenance**

(1) Data-processing systems shall be set up so that they can be serviced without allowing access to personal data. If this is not guaranteed, the data-processing body shall ensure through technical and organisational measures that only the personal data absolutely necessary for the service is accessible.

(2) Beyond the requirements of paragraph 1, service work may only be carried out by other bodies with written approval. For this purpose, Section 11 paragraph 2 clauses 1 and 2 shall apply respectively. Persons entrusted with maintenance work are obliged to preserve confidentiality.

(3) Within the context of an audit as per Section 11 b, if it has been ascertained that only access to data in coded, pseudonymised or anonymised form is possible during maintenance work, so that it is not possible for the body entrusted with the maintenance work to re-identify the data subject, only measures in accordance with paragraph 2 clauses 1 and 3 shall be required.

**Section 11b**
**(deleted)**

### Section 11c
### Data protection audit

In order to improve data protection and data security, as well as to achieve the greatest possible data economy, public bodies may have their data protection concept and their technical facilities tested and assessed by independent, approved auditors, and have the results of the audit published. They may also use already tested and assessed data protection concepts and programmes. The precise requirements of the test and the assessment, the procedure and the selection and approval of the auditors, shall be regulated by a separate law.

## Chapter 2
## Legal basis for data processing

### Section 12
### Collection

(1) The collection of personal data shall only be admissible if knowledge of it is required for the lawful fulfilment of the duty allocated to the collecting body by law, and for the purposes directly associated with this duty.

(2) Generally, personal data shall be collected from the data subject with his/her knowledge. In such a case, he/she must be informed about the use intended for the data. In connection with an intended transference of data, this duty to disclose information must also extend to include the recipient of the data. If the data has been collected on the basis of a legal provision, the data subject must be appropriately informed of this. Insofar as a duty to provide information exists, or should the information be the prerequisite for the granting of legal benefits, the data subject shall be informed about this, or otherwise about the voluntariness of his/her disclosure of information.

(3) Under the legal circumstances defined by Section 13 paragraph 2 clause 1 letters a and c to f, personal data about the data subject shall only be collected by other bodies or persons without his/her knowledge, provided this is required by a legal provision, provided this is an urgent prerequisite in connection with a legal provision of the federal government, or provided the protection of life and health, or the deterrence of a significant endangerment to normal livelihood make this necessary.

(4) If data has been collected from a third party or a private body, these shall, on request, be informed about the purpose. If a duty to provide information applies, the third party or private body shall be informed of this, or about the voluntariness of their information.

(5) If data has been collected from the data subject without his/her knowledge, he/she shall be notified about this as soon as this no longer endangers the lawful fulfilment of the duty. Paragraph 2 clauses 1 and 2 apply correspondingly. Should the data not have been collected from the data subject, the notification may be omitted if

1. the law has expressly determined that the data must be collected by other bodies or persons,

2. the data subject has acquired knowledge of the processing by other means, or

3. the notification is either impossible or would require disproportionate effort.

### Section 13
### Limitation of use for the purpose of storage, modification and use

(1) The storage, modification and use of personal data shall be admissible if it is required for the lawful fulfilment of duties by the public body. The data may only be stored, modified or used for the purposes for

which it was collected. Data which the body has obtained without collection may only be used and modified for the purposes for which it was initially stored.

(2) If personal data is to be stored, modified or used for purposes for which it was not collected or initially stored, this shall only be admissible provided

a) a legal regulation allows this, or the performance of a specific duty required by law or by legal decree has the processing of this data as a necessary prerequisite,

b) the data subject has consented,

c) the processing of an application submitted by the data subject is not possible without changing the purpose of the data, or it is required that details concerning the data subject be examined due to indications that inaccuracies exist,

d) it is required to avert significant disadvantages for the public welfare, or other immediately pending dangers to public security, or to avoid a serious impairment of rights for other individuals,

e) consent cannot be obtained from the data subject, or only with disproportionate effort, but it is obvious that it is in his/her interest and he/she would consent once aware of the other purpose,

f) it can be obtained from generally accessible sources, or the data processing body would be permitted to publish it, unless the interests of the data subject in preventing the storage or publication of the stored data predominate, or

g) that, in the course of the lawful fulfilment of duties, indications of criminal or administrative offences arise, and the notification of the authorities responsible for prosecution or execution seems necessary.

If the personal data is subject to professional secrecy or official confidentiality, and should this data have been transferred to the data processing body by the person committed to secrecy in the performance of his/her professional or official duties, clause 1 letters c to g shall not apply.

(3) Processing for other purposes shall not be deemed to have occurred, if this serves the exercise of supervisory or executive powers, auditing procedures, or the execution of organisational investigations. In this sense, access to personal data shall only be admissible insofar as it is indispensable for the performance of these powers. Personal data may only be used for training and vocational education purposes if this is indispensable, and if this does not conflict with the legitimate interests of the data subject; personal data may not be used for testing and examination purposes.

**Section 14**
**Transference within the public sphere**

(1) The transference of personal data to public bodies is admissible if this is required for the lawful fulfilment of duties by the communicating body or the recipient, and the prerequisites of Section 13 paragraph 1 clause 2 or 3 or of paragraph 2 clause 1 have been met, as well as those for the performance of duties in accordance with Section 13 paragraph 3. Communication shall also be admissible if the participation of several public bodies is required for decision-making in an administrative procedure.

(2) (abrogated)

(3) The transferring body shall be responsible for the admissibility of the transference. If the transference has been executed on the basis of a request by the recipient, the transferring body shall only examine whether the transference request lies within the sphere of duties administered by the recipient. The body shall only examine the lawfulness of the request, provided there exist grounds for doing so in the individual case; the recipient shall provide the transferring body with the information required for this examination. If the transference has been performed via an automated retrieval procedure (Section 9), the recipient shall be responsible for the lawfulness of the retrieval.

(4) The recipient may only process communicated data for the fulfilment of the purposes for which they were transferred to him/her; Section 13 paragraph 2 shall apply correspondingly.

(5) Paragraphs 1 to 4 shall apply accordingly, if personal data is forwarded within a public body.

**Section 15**
**Transfer of data to public-law religious societies**

Provided that provisions regulating the transference of data to public bodies have been correspondingly applied, the transference of personal data to public-law religious societies shall be admissible, if it has been ensured that the data protection measures taken by the recipient are sufficient.

**Section 16**
**Transfer of data to persons or bodies outside the public sphere**

(1) Provided these need the data in order to pursue their commercial purposes or objectives, the transfer of personal data to bodies in accordance with Section 2 paragraph 2 clause 1, and to persons or bodies outside the public sphere, shall be admissible if

a) it is required for the lawful fulfilment of the duties for which the transferring body is responsible, and the prerequisites of Section 13 paragraph 1 have been met,

b) the prerequisites of Section 13 paragraph 2 clause 1 letters a, b, d or f have been met,

c) the person or body requesting the information can substantiate a lawful interest in knowledge about the data to be transferred, and no grounds exist for assuming that confidentiality concerns of the data subject predominate, or
d) it is in the public interest or a warranted interest has been asserted in this respect and the data subject has not objected to these cases of data transfer.

(2) In cases defined by paragraph 1 letter d, the data subject shall be appropriately informed about the intended transfer, the type of data to be transferred and the purpose of the transference. This shall not apply if it can be assumed that he/she will become aware of these facts by other means.

(3) The recipient may only process the transferred data for the purposes it was transferred for.

(4) The transferring body may attach conditions to the transfer of data which ensure data protection on the part of the recipient.

**Section 17**
**Transfer of data to foreign and international bodies**

(1) The admissibility of transferring personal data to bodies in other Member States of the European Union, in other contracting Member States of the Agreement on the European Economic Area, or of organs and institutions of the EU, shall be determined by Section 4.

(2) For the transference of personal data to bodies other than those named in paragraph 1, as well as to supranational and international bodies, Section 16 paragraphs 1, 2 and 4 shall only be applied in accordance with the laws and agreements regulating this transference, if these bodies guarantee an adequate level of data protection.

(3) The adequacy of data protection standards shall be judged taking into consideration all circumstances which are of importance to the transference of data, or to a category of data transference; in particular, the type of data, the purpose, the duration of the planned processing, the country of origin and the country of destination, the legal norms applicable to the bodies as per paragraph 2, and the locally valid rules of conduct and security measures shall be assessed.

(4) Insofar as an adequate level of data protection in accordance with paragraph 2 cannot be guaranteed, the transference of data shall only be admissible provided that

1. the data subject has given his/her consent,

2. the transference of data is required for the fulfilment of contractual obligations between the transferring body and the data subject, or required for the execution of pre-contractual measures initiated by the data subject,

3. the transference of data is required for the conclusion or fulfilment of a contract which has been or will be settled with a third party in the interests of the data subject,

4. the transference of data is required to preserve interests of a primarily public nature, or required to enforce, execute or protect legal interests,

5. the transference of data is required to protect the vital interests of the data subject,

6. the transference of data ensues in connection with a register determined for the general public, which is intended to provide information to the general public, or which may be inspected by all persons able to substantiate a legitimate interest in the data, insofar as legal prerequisites exist in the given individual case,

7. the body receiving the data offers adequate guarantees in respect to the protection of basic rights.

(5) Transferences of data in accordance with paragraph 4 no. 7 shall be communicated to the member of the State Government responsible for internal affairs.

(6) The body receiving the transferred data shall be advised that this data may only be processed for reasons which can be reconciled with the original purposes for whose fulfilment the same date has been transferred.

(7) The transferring body assumes responsibility for the admissibility of data transference.

### Section 17a
### (deleted)

## Chapter 3
## Rights of the data subject

### Section 18
### Access to information and inspection of records

(1) Upon request, the data-processing body shall inform the data subject about

1. the data stored regarding his/her person,

2. the purpose and legal basis of the data processing,

3. the source of both the data as well as the data transferred to the recipient, insofar as these have been stored,

4. recipients of regular transfers of data,

5. in connection with automated decisions in compliance with Section 4 paragraph 4, the logical structure of the automated data-processing procedure involved.

This shall not apply to personal data stored on the sole basis of laws which regulate data storage and which forbid the erasure of such data, or which exclusively serve the purposes of data security or data protection control.

(2) The data-processing body shall determine the procedure, in particular the form of providing information, exercising due discretion; if the data has been stored in records or by non-automated procedures, the data subject shall be granted inspection of these on demand. Inspection of records shall be limited to those parts of the records containing the personal data of the data subject, provided no law of administrative procedure puts forth other provisions. Information taken from records or the inspection of records shall be granted, provided the data subject provides information to enable the data to be found with reasonable effort. The access to information and the inspection of records are free of charge; the reimbursement of expenses may be demanded.

(3) The obligation to provide information or to grant the inspection of records shall not apply if the personal data or the fact of its storage must be kept secret in accordance with a legal regulation or the overriding legitimate interests of a third party, and the interest of the data subject in access to the information must be accordingly subordinated.
(4) Grounds for refusing to provide information may only be waived if communicating these grounds would endanger the objectives pursued through the very refusal to provide information. In this case, the essential grounds for the decision shall be recorded.

(5) If the access to information or inspection of records concerns the source of personal data of authorities concerned with the protection of the Constitution, with the Office of the Public Prosecutor, with the police and State fiscal administrations, insofar as these store personal data for the fulfilment of their statutory duties within the scope of application defined by the Fiscal Code for monitoring and auditing purposes, as well as the authorities named in Section 19 paragraph 3 of the Federal Data Protection Act, these shall only be admissible with the approval of the aforenamed bodies. The same shall apply to the transference of personal data to these authorities. Insofar as this Act applies to the aforenamed authorities, paragraphs 5 and 6 shall apply correspondingly in respect to the refusal of consent.

(6) If the data subject has not been provided with information, it shall be provided to the Commissioner of the State of Brandenburg for Data Protection and Access to Information on his/her request, provided the highest responsible State authority involved in the matter does not ascertain that this would endanger the security of the Federation or of a State in the individual case. The notification sent by the Commissioner of the State of Brandenburg for Data Protection and Access to Information to the data subject shall not allow any conclusions to be drawn regarding the extent of knowledge possessed by the data-processing body, if this body does not approve more extensive access to information.

## Section 19
## Rectification, erasure and blockage of data

(1) Personal data shall be rectified if it is incorrect. If personal data is to be rectified which has not been processed in automated procedures or which exists in records, it shall be made identifiable in a suitable form at which point in time, and for which reason, this data was or became incorrect.

(2) Personal data shall be erased if

a) its storage is inadmissible, or

b) knowledge of it is no longer required for the data-processing body to fulfil its duties.

Should personal data be stored in records, erasure in accordance with clause 1 letter b shall only be executed if the entire record is no longer required for the fulfilment of duties, unless the data subject demands the erasure and continued storage would unreasonably disadvantage him/her. Insofar as an erasure cannot be considered, the personal data shall be blocked on request of the data subject.

(3) Personal data shall be blocked instead of erased if

a) its correctness is contested by the data subject, and neither its correctness not its incorrectness can be established,

b) the data subject demands blockage instead of erasure in accordance with paragraph 2 clause 1 letter a,

c) continued storage is required in the interests of the data subject,

d) it has only been stored for the purposes of data protection or data protection control, or

e) the prerequisites defined by paragraph 2 clause 1 letter b have been met, and the data may not be erased due to statutory safekeeping periods.

In cases described by clause 1 letter c, the grounds shall be recorded. For data processed by automated methods, blockage shall be ensured through technical measures as a rule; a corresponding note shall be made in addition. Blocked data may only be processed without the consent of the data subject provided this is for scientific purposes, to remedy an acute lack of evidence, or for other such reasons in the predominant interests of either the responsible body or a third party which are indispensable or required in order to properly execute supervisory or regulatory functions as well as auditing procedures, and provided the data in this context could be processed, had it not been blocked.

(4) With the exception of the cases described in paragraph 2 clause 1 letter a, erasure shall not be executed to the extent the stored data should be entrusted to the responsible public archive in compliance with the Brandenburg Archive Act, and will be received by this body.

(5) Those bodies which are recipients of data transferences shall be notified immediately about the rectification of incorrect data, the blockage of contested data and the erasure of inadmissibly stored data. Notification shall not be necessary if this would require considerable effort, and if disadvantageous consequences for the data subject are not to be feared. Clauses 1 and 2 apply accordingly, should data have been passed on within a public body.

## Section 20
## Compensation

(1) Should any property loss ensue on the part of the data subject, which has been caused by the impermissible or incorrect processing of his/her personal data in accordance with the provisions of this Act or other data protection regulations, the data-processing body or its carrier is obliged to provide compensation. In serious cases the data subject may also demand fair compensation in cash for damages caused which are not of a pecuniary nature. A duty to provide compensation does not exist insofar as the data-processing body is not culpable for the causal circumstances giving rise to the damages. The burden of proof in this context is the responsibility of the data-processing body or its carrier. In respect to the data subject, the data-processing body is also responsible for such circumstances for which contractors are responsible as defined by Sections 11 and 11a. Claims are limited to a total of Euro 125,000.

(2) Sections 254, 839 paragraph 3 and Section 852 of the German Civil Code shall apply correspondingly in respect to any culpable contributory negligence on the part of the data subject, and to the statutory limitation of compensation entitlements.

(3) More extensive compensation entitlements shall remain unaffected.

(4) Legal action may be taken through a court of law.

### Section 21
### Right of appeal of the data subject

(1) Every individual has the right to appeal to the Commissioner of the State of Brandenburg for Data Protection and Access to Information, if he/she is of the opinion that his/her rights have been violated through the processing of his/her personal data by a body subject to the control of the State Commissioner; this also applies to employees of public bodies, in which case it is not necessary to adhere to the official channels.

(2) Nobody may be disadvantaged or reprimanded because he/she has appealed to the Commissioner of the State of Brandenburg for Data Protection and Access to Information.

## Part 2
## Commissioner of the State of Brandenburg for Data Protection and Access to Information

### Section 22
### Appointment and legal status

(1) The State Parliament shall elect a Commissioner of the State of Brandenburg for Data Protection and Access to Information through more than one-half of the statutorily required number of its members. He/She must qualify for the office of judgeship or for a higher office, or have equivalent qualifications in accordance with the German Unification Treaty, and possess the specialised knowledge required for the fulfilment of his/her duties.

(2) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall take the following oath before the President of the State Parliament:

> "I swear that I will execute my office justly and impartially in faithful allegiance to the Basic Law of the Federal Republic of Germany, to the Constitution of Brandenburg and the law in general, and to devote all my effort in doing so."

The oath may also include a religious declaration.

(3) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall continue to fulfil the functions of his/her office until his/her successor has been appointed, however, for a maximum of six months subsequent to the expiration of his/her term of office.

(4) The office of the Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be established by the President of the Brandenburg State Parliament. The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be independent in executing his/her office, and shall be subject only to the law. He/She shall be subject to supervision by the President of the State Parliament. The personnel and material resources required for the fulfilment of duties shall be supplied, and these resources shall be presented as an individual fiscal plan in a separate chapter of the budget of the State Parliament. The employees shall be appointed by the President of the State Parliament at the proposal of the Commissioner of the State of Brandenburg for Data Protection and Access to Information. They may only be relocated or deputized with the approval of the Commissioner of the State of Brandenburg for Data Protection and Access to Information. The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be their superior, to whose instructions they are exclusively bound. The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall appoint one employee as his/her deputy. The deputy shall conduct procedures whenever the Commissioner of the State of Brandenburg for Data Protection and Access to Information is prevented from executing his/her office.

(5) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be the highest official as defined by Section 96 of the Code of Criminal Procedure. He/She shall be solely

responsible for making decisions concerned with the authority to issue statements for him/herself and his/her employees.

(6) The Commissioner of the State of Brandenburg for Data Protection and Access to Information may not execute any salaried office, trade or profession in addition to his/her office, nor belong to the management, the supervisory board or the administrative council of any enterprise involved in commercial acquisitions, nor to any government or any legislative body of the Federation or of a State.

(7) At the same time, the State Commissioner for Data Protection shall execute the duties of a Commissioner for the Right to Inspect Records in accordance with provisions of the Privacy and Freedom of Information Act. The designation of his/her office and function shall be: “The Commissioner of the State of Brandenburg for Data Protection and Access to Information”; this may be used in either the masculine or the feminine form.

**Section 23**
**Duties**

(1) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall monitor the enforcement of this Act and other provisions concerning data protection, as well as the observance of the Inspection of Records and Access to Information Act by public bodies in accordance with Section 11 paragraph 2 of this Act, insofar as these bodies or other public bodies are subject to the jurisdiction of this Act in accordance with Section 2 or have subjected themselves to the regulation of data-processing bodies as per Section 11 paragraph 1 clause 3.

(1a) The Commissioner of the State of Brandenburg for Data Protection and Access to Information is also the supervisory authority in accordance with Section 38 of the Federal Data Protection Act for the data-processing activities of bodies outside the public sector.

(2) The Commissioner of the State of Brandenburg for Data Protection and Access to Information may make recommendations for the improvement of data protection. In particular, he/she may advise the State Government and individual ministers, the communities and the associations of local authorities, as well as other public bodies in questions concerned with data protection.

(3) Furthermore, the Commissioner of the State of Brandenburg for Data Protection and Access to Information shall pursue information regarding matters and procedures which directly concern his/her field of duty at the request of the State Parliament, the Committee on Petitions or the Committee for Internal Affairs. In addition, he/she shall also pursue information arising from the assertion of rights by the data subject as per Section 21.

(4) The State Parliament and the State Government may entrust the Commissioner of the State of Brandenburg for Data Protection and Access to Information with preparing appraisals and official statements, or with conducting investigations into questions concerning data protection. Section 22 paragraph 4 clause 2 remains unaffected.

(5) The Commissioner of the State of Brandenburg for Data Protection and Access to Information may participate in meetings of the State Parliament and its committees in compliance with the valid parliamentary rules of procedure, and may comment on matters of significance for data protection. The State Parliament and its committees may demand his/her presence or his/her written or oral observations.

(6) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be authorized to process personal data required for the fulfilment of his/her duties conferred to him/her by this Act, under the conditions of this Act. He/She may also collect personal data within the framework of regulatory measures in individual cases, without the knowledge of the data subject, if the existence of a flaw in data protection procedures can only be established by this method. The data processed in accordance with clauses 1 and 2 may not be stored, altered or used for other purposes.

(7) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall cooperate with the authorities and other bodies responsible for monitoring the observance of data protection provisions at the federal level and in the States, as well as with supervisory authorities as per Section 38 of the Federal Data Protection Act. He/She shall be entitled to monitor the observance of data protection procedures on behalf of these bodies at their request, and to process personal data for this purpose; the same shall apply if a private body has subjected itself to monitoring by the Commissioner in a contract as per Section 11 paragraph 1 clause 3.

(8) The Commissioner of the State of Brandenburg for Data Protection and Access to Information is the responsible authority for the prosecution of administrative offences as defined by Section 38 of this Act, Section 43 of the Federal Data Protection Act, as well as other data protection regulations. He/She is also an authority which provides assistance in accordance with Article 13 number 2 letter a of the Convention for the Protection of Individuals in Regard to the Automatic Processing of Personal Data from January 28, 1981.

**Section 24**
**(deleted)**

**Section 25**
**Complaints lodged by the Commissioner of the State of Brandenburg for Data Protection and Access to Information**

(1) Should the Commissioner of the State of Brandenburg for Data Protection and Access to Information identify violations against the provisions of this Act or other data protection provisions, or identify other flaws in the processing of personal data or violations against the Inspection of Records and Access to Information Act, he/she shall lodge a complaint about these

1. at the State administration and directed to the highest responsible State authority,

2. at the local government administration and directed to the community responsible in this connection, or to the association of local authorities responsible in this connection,

3. at university-level institutions and colleges of higher education and directed to the president of the institution or the rector, at public schools and directed to the headmaster,

4. at other corporate bodies, institutions and public-law foundations and directed to the management or to the organ with corresponding representational authorization,

and shall demand a statement from these bodies within a deadline to be determined by him/her. In the cases defined by clause 1 nos. 2 to 4, the Commissioner of the State of Brandenburg for Data Protection and Access to Information shall also simultaneously inform the responsible supervisory authority.
(2) The Commissioner of the State of Brandenburg for Data Protection and Access to Information may abstain from lodging a complaint or from demanding statements from the respective bodies, particularly if minor flaws or flaws which have been redressed in the meantime are concerned, or if their removal has been ascertained.

(3) The Commissioner of the State of Brandenburg for Data Protection and Access to Information may combine proposals for redressing specific flaws and for otherwise improving data protection with the complaint.

(4) The official statement required by paragraph 1 shall also contain a description of the measures taken as a result of the complaint lodged by the Commissioner of the State of Brandenburg for Data Protection and Access to Information. The bodies named in paragraph 1 numbers 2 to 4 shall send a copy of their statement submitted to the Commissioner of the State of Brandenburg for Data Protection and Access to Information to the responsible supervisory authority.

(5) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall be authorized to inform data subjects about the complaint and the measures taken in accordance with paragraph 4 as a result of this, exercising appropriate professional discretion.

## Section 26
## Implementation of monitoring

(1) Public bodies are obliged to support the Commissioner of the State of Brandenburg for Data Protection and Access to Information and his/her representatives in fulfilling their duties. In particular, they shall be provided with

1. information regarding their questions and the ability to inspect all procedures and records, in particular stored data and data-processing programmes concerned with the processing of personal data,

2. access to all places of work at any time.

Inspection in accordance with number 1 may also be granted by electronic means.

(2) Paragraph 1 shall not apply to the authorities named in Section 18 paragraph 5 insofar as the member of the State Government responsible in this context ascertains that inspection of the documents and records endangers the security of the Federation or of a State in the individual case. On the request of the Commissioner of the State of Brandenburg for Data Protection and Access to Information, the State Government shall state the grounds for this decision in a secret meeting of the responsible committee of the State Parliament. The decision of the committee may be published.

(3) Professional secrecy and official confidentiality shall not release public bodies from the duty to support the Commissioner and his/her representatives.

## Section 27
## Activity reports and parliamentary control

(1) The Commissioner of the State of Brandenburg for Data Protection and Access to Information shall present the State Parliament and the State Government with an annual report about his/her activities every two years in accordance with Section 23 paragraph 1. In response, the State Government shall regularly present an official statement about this report to the State Parliament within four months after its presentation. At the same time, the Commissioner of the State of Brandenburg for Data Protection and Access to Information shall also present a report on its activities to the State Parliament in accordance with Section 23 paragraph 1a.

(2) Every representative has the right to send enquiries to the Commissioner of the State of Brandenburg for Data Protection and Access to Information, and to demand information, the inspection of records, or other documentation from the Commissioner. Enquiries must be responded to immediately, thoroughly and to the best knowledge of the Commissioner. Specific formalities shall be regulated by the business agenda of the State Parliament. Requests for information or for the inspection of records may be denied, should confidentiality prove to be necessary due to public or private interests of overriding priority.

## Part 3
## Special data protection

### Section 28
### Data processing for scientific purposes

(1) Public bodies may collect, store, modify, use and transfer personal data to other bodies or individuals without consent for scientific purposes if

a) legitimate interests of the data subject will not be impaired due to the type of data, due to its accessibility, or due to the nature of its use,

b) a legal provision provides for this, or

c) public interest in the execution of the research project is considered to be more important than the legitimate interests of the data subject, and the objectives of this research cannot be achieved in any other way.

The recipient may not use the transferred data for other purposes. Persons who have access to the respective data stock within a public body as a result of their competencies may store, modify and use personal data without consent, provided the other prerequisites of clause 2 have been met. In cases as described in clause 1, the public bodies shall inform the Commissioner of the State of Brandenburg for Data Protection and Access to Information accordingly.

(2) The data shall be anonymised to the extent this is possible according to the objectives of the research. Until then, characteristic data shall be stored separately which allows particular information about personal or material circumstances to be attributed to an identified or identifiable individual. This data shall be erased as soon as the objectives of the research allow for this.

(3) Insofar as the provisions of this Act do not apply to the recipient, personal data may only be transferred to him/her provided he/she commits himself/herself to observing the provisions of paragraph 1 clause 2 and paragraph 2.

(4) Public bodies carrying out scientific research may only publish personal data if

a) the data subject has consented or

b) this is essential for the presentation of research results about events in contemporary history.

### Section 29
### Data processing for service and employment relationships

(1) The personal data of applicants and employees may only be processed if this is required for entering, implementing, terminating or executing an employment or service relationship, or for the implementation of measures concerned with internal company affairs, planning, organisation, personnel, social matters, household matters, or budgetary matters, but especially for the purposes of personnel planning and human resource allocation, or provided such processing is required by a legal provision, a collective wage agreement, an employment agreement, or a service agreement. In derogation from Section 16 paragraph 1, the transference of employee data to individuals and bodies outside the public sphere shall only be admissible if the recipient brings forth a legal interest, if this is required in the course of performing the service, or if the data subject has given his/her consent. Data communication to a future employer shall only be admissible with the consent of the data subject.

(1a) Those provisions of State law valid for public servants shall be correspondingly applied to the processing of personal data from employees, trainees and apprentices, unless special legal provisions or collective wage agreements take precedence.

(2) The storage, alteration or use of data collected for medical or psychological examinations, or for tests used to establish a service or employment relationship, shall only be admissible with the written consent of the data subject. As a rule, the employing authority may only demand from the practising doctor the transfer of results from the suitability examination as well as the risk factors established therein.

(3) Personal data collected prior to entry into a service or employment relationship shall be erased without delay as soon as it has been established that a service or employment relationship will not come about, unless the data subject has consented to continued storage. Provided it is no longer needed, personal data shall be erased after the service or employment relationship has ended, unless there are conflicting legal provisions; Section 19 paragraph 2 clauses 2 and 3 and Section 19 paragraph 4 shall apply accordingly.

(4) Insofar as the employee data has been stored within the context of implementing technical and organisational measures as per Section 10 paragraph 2, it may not be used for the purposes of monitoring behaviour or performance.

**Section 30**
**Telemetering and telecontrolling**

(1) Public bodies may only carry out remote-controlled metering or observations (telemetering services) in habitations or business offices, if the data subject has been previously informed about their intended use, their type, their extent and the duration of their implementation, and the data subject has consented in writing after receiving this information. The same applies when it is intended that a transmitting device should trigger specific effects in habitations or business offices (telecontrolling). The installation of telemetering and telecontrolling equipment shall only be admissible if the data subject can recognise when a service has been utilised and what kind of service it is; this shall not apply to telemetering and telecontrolling services performed by public utilities. The data subject may revoke his/her consent at any time, insofar as this is reconcilable with the intended purpose of the service. In case of doubt, cutting off a service shall be considered a revocation of consent.

(2) A service, the conclusion or the execution of a contractual relationship may not be made dependent on the consent of the data subject in accordance with paragraph 1 clause 1 or 2. Should he/she refuse or revoke his/her consent, this may not lead to any disadvantages for him/her exceeding the direct follow-up costs.

(3) Insofar as personal data has been collected within the context of telemetering or telecontrolling services, this may only be processed for the agreed-upon purposes. This data shall be erased as soon as it is no longer required for the fulfilment of these objectives.

**Section 31**
**Processing of personal data by the State Parliament**

(1) The State Government may use personal data collected for other purposes in order to respond to parliamentary inquiries and for the presentation of documents and reports to the State Parliament, to the extent that this is necessary for these purposes. The transference of data for purposes described by clause 1 is not admissible if this is unreasonable for the data subject due to the strictly personal nature of the data, or if the impairment of his/her right to informational self-definition is disproportionate. This shall not apply if – with regard to Section 2 paragraph 1a clause 2, or through other suitable measures – it is ensured that the legitimate interests of the data subject have not been impaired. Special legal prohibitions regarding the transference of data shall remain unaffected.

(2) Personal data transferred by the State Government may not be inserted into printed materials provided by the State Parliament's or be made generally accessible by any other means. This shall not apply if there is no indication that the legitimate interests of the data subject will be impaired.

**Section 32**
**(deleted)**

## Section 33
## Data processing for journalistic and editorial purposes

(1) To the extent public bodies – especially as commercial enterprises or auxiliary enterprises of the press, of broadcasting companies or of the film industry – process personal data exclusively for journalistic and editorial purposes in order to influence public opinion, only Section 10 among the provisions of this Act shall apply.

(2) If the journalistic and editorial processing of personal data leads to the publication of counterstatements by the data subject, these counterstatements shall be taken up in the stored data and preserved for the same period of time as the data itself.

## Section 33a
## Public distinctions and tributes

(1) In preparation for public distinctions and tributes, the responsible bodies may process the requisite data without the knowledge of the data subject. This data may only be processed for other purposes with the consent of the data subject.

(2) At the request of the bodies named in paragraph 1, other public bodies may transfer the data required for the preparation of the distinction or tribute.

(3) On request, the bodies named in paragraph 1 shall provide the data subject with information regarding

a) the stored data concerning his/her person,

b) the purpose and the legal basis for this storage, and

c) the source of the data.

The form used to provide this information shall be determined with due professional discretion. For the rest, Section 18 shall not apply.

(4) Paragraphs 1 and 2 shall not be applied if the data-processing body has been informed that the data subject has rejected his/her public distinction or tribute, or the data processing associated with this.

## Section 33b
## Amnesty procedures

In amnesty procedures, the processing of personal data shall be admissible insofar as this is necessary for the application of the Amnesty Law by the responsible body. The data processing shall not be subject to monitoring by the Commissioner of the State of Brandenburg for Data Protection and Access to Information.

## Section 33c
## Video observation and video recording

(1) Public bodies may monitor publicly accessible areas using optical electronic equipment, insofar as this is necessary

1. for the fulfilment of their duties,

2. to exercise the right to determine who should be allowed or denied access,

3. to protect property or possessions,

4. to regulate access authorization,

and provided that no evidence exists which indicates a conflict with overriding legitimate interests of the data subject.

(2) The circumstance of video observation as well as the responsible body shall be made identifiable through appropriate measures.

(3) The processing of data collected in accordance with paragraph 1 is admissible, if this is required to achieve the designated objectives and no evidence exists which indicates a conflict with overriding legitimate interests of the data subject. This data may only be processed for other purposes to the extent this is necessary in order to avert dangers to public security or to prosecute criminal offences. Section 19 paragraph 2 clause 1 letter b shall remain unaffected.

(4) Should personal data obtained by means of video recording be altered, transferred or otherwise used, this shall be reported to the data subject. Section 12 paragraph 5 shall apply correspondingly.

**Section 33d**
**Mobile media for the storage and processing of personal data**

(1) The body which provides mobile media for the storage and processing of personal data must inform the data subject about

1. its identity and address,

2. the functional mode of the medium, including the type of personal data to be processed, in a generally comprehensible form,

3. how he/she can exercise his/her rights in compliance with Sections 18 and 19,

4. the measures to be taken in the event the medium has been lost or destroyed,

insofar as he/she has not already obtained prior knowledge.

(2) Communication procedures which engender processing must be identifiable to the data subject.

**Section 34**
**Personal data from former institutions**

(1) If - prior to October 3 1990 - personal data has been stored by former institutions for primarily self-designated administrative tasks which were to be performed by authorities, institutions and any other public bodies of the State, the communities, associations of local authorities, or other public bodies in accordance with Basic Law of the Federal Republic of Germany, as put forth by Section 2 paragraph 1 clause 1, the public administration carrier responsible for the administrative task shall be entitled to this data.

(2) Former institutions as defined by paragraph 1 are former State or economically active organs, collective combines, commercial operations and facilities, as well as societal organisations of the German Democratic Republic.

**Section 35**
**Processing personal data from former institutions**

(1) In derogation from Section 13 paragraph 1, the storage, modification or use of personal data from former institutions by the bodies named in Section 34 paragraph 1 shall be admissible if

1. knowledge of the data is required for the lawful fulfilment of a duty lying within the scope of responsibilities of these bodies,

2. renewed collection of this data would entail a disproportionate effort,

3. the data subject has not objected to the processing as per Section 36, and

4. the competence and responsibility of the data-processing bodies have been unequivocally determined.

(2) Personal data that may be processed as per paragraph 1 shall be considered as having initially been stored for the purpose determined in accordance with paragraph 1 no. 1.

**Section 36**
**Right of objection**

(1) The data subject may object to the processing of his/her data, if the data has been collected by a former institution and stored by the latter or by another former institution, and if the data may not be collected without his/her involvement as required by valid legal provisions.

(2) The data subject shall be personally notified by appropriate means about

1. the source of such data,

2. the nature of their original use,

3. the nature and extent of the intended processing,

4. the currently responsible data-processing body and

5. the existing possibility of objection.

Notification may also take place in a general form, insofar as individual notification does not seem prudent due to the disproportionate effort this would entail, and if legitimate interests of the data subject do not prevail.

**Section 37**
**Blocking personal data from former institutions**

(1) If the processing of personal data from former institutions is not admissible as per Section 35 paragraph 1, this data shall be handed over to the responsible State archive in derogation from Section 19 paragraph 2. Data whose storage would be inadmissible according to State law shall be treated in accordance with the provisions of Section 4 paragraphs 2 and 3 of the Brandenburg Archiving Act.

(2) In derogation from Section 19 paragraph 3, blocked data as per paragraph 1 clause 1 may only be stored, altered or used to remedy an acute lack of evidence, for scientific purposes, or with the consent of the data subject.

(3) Any data subject may demand the erasure of unlawfully collected data. The application shall be approved, provided this does not conflict with legitimate interests of the general public or of third parties.

## Part 4
## Administrative offences, criminal offences; transitional provisions

### Section 38
### Administrative offences, criminal provisions

(1) As regards personal data which has not been made publicly accessible, it is to be considered an administrative offence if – in violation of the provisions put forth by this Act or other legal provisions concerning the data protection – anyone

1. collects, stores, uses without authorization, alters, transfers, passes on, makes available for retrieval, establishes a connection to a particular individual, erases, or

2. retrieves, inspects, obtains or – under false pretences – arranges for the transfer or passing on of such personal data.

It is also to be considered an administrative offence if – under the prerequisites named in clause 1 – anyone should combine particular details about the personal or material circumstances of a no longer identifiable individual with other information, thereby making the affected individual identifiable once again.

(2) An administrative offence is punishable with a fine of up to Euro 50,000.

(3) Whoever commits an act named in paragraph 1 for remuneration, or with the intention of enriching himself/herself or another person, or with the intention of damaging another person, shall be punished with a prison sentence of up to two years, or with a fine. The act will only be prosecuted if a corresponding petition has been filed. Those parties authorized to submit such a petition are the data subject, the responsible body, and the Commissioner of the State of Brandenburg for Data Protection and Access to Information.

### Section 39
### (deleted)

### Section 40
### Transitional provisions

(1) In records which existed when this Act came into force, rectification, erasure or blockage may be undertaken if the data-processing body has ascertained the existence of the necessary prerequisites during the course of fulfilling its routine duties, or due to a verification request of the data subject.

(2) Sections 35, 35, 36 and 37 cease to have legal force after December 31, 2009.

### Section 40a
### Limitation of basic rights

This Act limits the basic right to data protection (Article 11, Section 1 in the Constitution of the Federal State of Brandenburg).

### Section 41
### (Commencement)

### Annex 1
### (deleted)

### Annex 2
### (deleted)