**Liechtenstein Law Gazette**

**2002 No. 55 issued on 8 May 2002**

# Data Protection Act

of 14 March 2002

I hereby grant My consent to the following resolution adopted by the Diet

## I. General provisions

Article 1

*Objective*

1) This Act shall seek to protect the personality and fundamental rights of those individuals about whom data is processed

2) This Act implements EU Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (EEA Compendium of Laws Appendix XI - 5e 01)

Article 2

*Scope*

1) This Act shall regulate the processing of data about natural and legal persons undertaken by

a) private individuals

b) authorities

2) This Act shall also regulate the processing of all data

a) conducted as part of the activities of a branch of the file controller in Liechtenstein,

b) conducted by a file controller established in a place where the law of Liechtenstein is applicable,

c) conducted by a file controller not established in the European Economic Area and making use of automated or non-automated means located in Liechtenstein for the purpose of processing data, unless such means are used solely for the purpose of passage through the European Economic Area Notwithstanding his responsibilities to the Data Protection Office, the file controller must appoint a representative in Liechtenstein [1]

3) This Act shall not apply to

a) personal data that is processed by a natural person exclusively for personal use and that is not disclosed to a third party,

b) deliberations of the Diet and its committees,

c) pending civil, penal, or international legal assistance proceedings or public and administrative law proceedings

d) cases pending before the State Court,

e) the activities of the National Audit Office,

f) cancelled[2]

g) cancelled[3]

4) The above provisions shall be subject to differing and supplementary provisions in other Acts, provided such provisions ensure the protection of data from unauthorised processing in terms of this Act

Article 3

*Definitions*

1) The expressions below shall be defined as follows

a) "**personal data (data)**" all information relating to an identified or identifiable person,

[1] Art 2 (2)(c) amended by LGBl 2008 no 273
[2] Art 2 (3)(f) cancelled by LGBl 2009 no 46
[3] Art 2 (3)(g) cancelled by LGBl 2009 no 46

b) "**data subjects**" the natural or legal persons and legal partnerships about whom data is processed,

c) "**private individuals**" natural or legal persons and legal partnerships which are subject to private law,

d) "**authorities**" organs of the state, municipalities, corporations, foundations, establishments, and private institutions which are actively performing public duties assigned to them,

e) "**sensitive data**" data relating to

aa) religious, philosophical, or political opinions or activities,

bb) health, sexuality, or racial origin,

cc) social security files,

dd) criminal or administrative proceedings and penalties,

f) "**personal profile**" a collection of data that allows the appraisal of fundamental characteristics of the personality of a natural person,

g) "**processing of personal data**" any operations relating to personal data, such as the collection, storage, use, modification, communication, archiving, or destruction of data,

h) "**disclosure of personal data**" rendering data accessible, for example allowing the inspection, communication, or publication of personal data,

i) "**file**" any collection of personal data whose structure facilitates a search for data on a particular data subject,

k) "**file controller** (**controller**)" the private persons or authorities who decide on the purpose and content of the file,

l) "**recipient**" the private individual, authority, institution, or any other body which receives data, regardless of whether or not it constitutes a third party However, authorities which may receive data as part of an individual investigation shall not be considered recipients,

m) "**consent of the data subject**" any declaration of intent not given under duress, given for the specific case and in knowledge of the situation, by which declaration the data subject accepts that data relating to him will be processed

n) "**public place**" a place the accessibility of which is determined by general criteria that may be met by any person [1]

2) Unless otherwise specified in this Act, the masculine terms used in this Act and related to natural persons shall indicate members of both the male and female sexes

# II. Use of data

## A. General provisions

Article 4

*Principles*

1) Personal data may only be processed in a lawful manner [2]

2) Processing must be conducted in good faith and must not be excessive

3) Personal data may only be processed for the purpose which was either given during its collection or which is provided for by law [3]

4) If the consent of the data subject is required for the processing of personal data, such consent is not valid unless it has been given voluntarily and following adequate information In the processing of sensitive data or personal profiles, such consent shall be required to be given expressly [4]

[1] Art 3 (n) inserted by LGBl 2009 no 46
[2] Art 4 (1) amended by LGBl 2009 no 46
[3] Art 4 (3) amended by LGBl 2009 no 46
[4] Art 4 (4) inserted by LGBl 2009 no 46

Article 5

*Prior information*

1) In the event that data is collected, the file controller must provide the data subject with the following information at the least, unless the data subject already has such information

a) the identity of the file controller,

b) the purpose of the processing

2) The government may enact a regulation requiring that additional information be provided if such is essential for processing the data in good faith considering the specific circumstances under which the data is collected, for example

a) the categories of the data which is being processed,

b) the recipients or the categories of the recipients of the data,

c) rights to information and correction

3) If the data was not collected from the data subject, the controller must provide the data subject with the information pursuant to paragraph 1 upon commencing storage of the data or, in the event the controller intends to pass the data on to third parties, upon initial disclosure at the latest

4) The above provisions shall not apply if notifying the data subject is impossible, would involve disproportionate efforts, or if storage or communication of the data is expressly required by law, especially in the event of data processing for the purposes of statistics, or historical or scientific research

Article 6

*Automated decisions*

1) Decisions which are made exclusively on the basis of automated data processing for the purpose of evaluating individual aspects of a person, such as his professional ability, creditworthiness, reliability, or conduct shall constitute a breach of the data subject's privacy provided such decisions have legal consequences and result in substantial impairments

2) Decisions pursuant to paragraph 1 shall be lawful if

a) such decisions are made as part of the conclusion or performance of a contract, at the request of the data subject or after the data subject was given opportunity to comment, or

b) such decisions are allowed by a law

## Article 6a[1]

*Use of devices for the recording and transfer of images in public places*

1) The use of devices for the recording and transfer of images in public places (video surveillance) shall only be admissible where it is necessary

a) for authorities, to fulfil their legal duties,

b) to safeguard domestic authority, or

c) to safeguard justified interests for specifically regulated purposes

2) The processing of the data collected under paragraph 1 shall only be admissible if such processing is necessary to achieve the purpose pursued and if there are no indications that interests warranting protection of the data subject prevail They may only be processed for other purposes if this is necessary

a) to avert danger to the public safety or to the safety of the State,

b) to avert serious danger to life, limb, freedom, or property, or

c) to prosecute criminal offences and to secure evidence

In the event of sentence 2, the Liechtenstein Police may demand that data collected be disclosed

3) The use of video surveillance must be approved by the Data Protection Office before installation Approval shall not be required for the real-time transfer of images without the option of recording or of other ways of processing The decision on approval may be appealed within 14 days to the Data Protection Commission The government shall regulate further details by ordinance

[1] Art 6a inserted by LGBl 2009 no 46

4) The fact that video surveillance is being conducted and the person responsible shall be shown by suitable means

5) If data collected through video surveillance are related to a specific person, such person shall be informed about any processing in accordance with Art 5 (3)

6) The person responsible for using video surveillance shall take all measures necessary to ensure the safety of the data In this, it must be ensured depending on the type of the data collected and the amount and purpose of processing, as well as in consideration of what is technically possible and economically feasible that

a) processing happens duly and in a purpose-oriented way,

b) the data is protected from random or unlawful destruction and from loss, and

c) the data is inaccessible by unauthorised third parties,

The government shall regulate further details by ordinance

7) The data shall be deleted immediately, but no later than within 30 days, if

a) they are no longer necessary to achieve the purpose, or

b) interests warranting protection of the data subjects stand against further storing of the data

Article 7

*Accuracy of data*

1) Whoever processes personal data must verify that the information is accurate

2) Any data subject may request the rectification of inaccurate data

Article 8[1]

*Cross-border data flows*

1) No personal data may be transferred abroad if the personal privacy of the data subjects could be seriously endangered, in particular where there is no legislation that provides adequate protection This shall not apply to states which are EEA member states

2) If there is no legislation offering adequate protection, personal data may only be transferred abroad if

a) the person responsible for processing provides - in particular by contractual clauses - sufficient guarantees concerning the protection of privacy, the basic rights and fundamental freedoms, and the exercising of the rights connected with them,

b) the data subject has given his consent in the specific case,

c) processing is in direct connection with entering into or performing an agreement and the data in question are data of the contracting party,

d) disclosure in the specific case is indispensable in particular for the safeguarding of an overriding public interest or for the declaration, exercising, or enforcement of legal claims in court,

e) disclosure is necessary in the specific case to protect the life or the physical integrity of the data subject,

f) the data subject has made the data publicly available and has not expressly prohibited processing, or

g) disclosure happens within the same legal person or company or between legal persons or companies that are under the same leadership, provided that the participants are subject to common data protection rules that ensure adequate protection

3) The disclosure of data in terms of paragraph (2)(a) and (g) shall require approval from the government Prior to such approval, the Data Protection Office shall make a recommendation as to whether the guarantees or common data protection rules ensure adequate protection The government shall regulate more specific details by ordinance

[1] Art 8 amended by LGBl 2009 no 46

4) The adequacy of the level of protection shall be assessed in consideration of all circumstances that are of importance concerning the transfer of data or concerning a category of data transfers, in particular, the type of data, the purpose of processing, the duration of the planned processing, the country of origin and the country of final destination, the legal rules applying to the recipient in question, and the professional rules and security measures applying to such recipient may be taken into account

5) The government shall by ordinance and on the basis of resolutions by the EEA Joint Committee issue a list of the non-EEA countries whose data protection legislation offers an adequate level of protection

Article 9

*Data security*

1) Appropriate organisational and technical means shall be employed to ensure the protection of personal data against unauthorised processing

2) The Government shall by ordinance issue more detailed rules on the minimum requirements for data security

Article 10

*Confidentiality of data*

Whoever processes data or has data processed must keep data from applications entrusted to him or made accessible to him based on his professional activities secret, notwithstanding other legal confidentiality obligations, unless lawful grounds exist for the transmission of the data entrusted or made accessible to him

Article 11

*Right of access*

1) Anyone may ask a file controller if data relating to him is being processed The Government shall enact an ordinance establishing a period within which the information must generally be provided

2) The file controller must provide information on

a) all data relating to the data subject that is contained in the file and its origin,

b) the purpose and if necessary the legal basis for the processing, the categories of processed data, the individuals participating in the collection of the data, and the individuals designated to receive the file,

c) the logical structure of the automated processing of the data relating to the data subject in the event of automated decisions in terms of to Article 6, and

d) the correction, destruction, or restriction on communication of data whose processing does not comply with the provisions of this Act, in particular if such data is incomplete or inaccurate

3) The file controller may disclose data relating to the health of the data subject via a doctor designated by the person

4) In the event the file controller has the personal data processed by a third party, the file controller shall remain responsible for providing the information that is requested The third party shall be obliged to provide information in the event that it does not disclose the name of the file controller or in the event the controller is not resident in Liechtenstein

5) The information should, as a general rule, be submitted in writing in printed form or as a photocopy and be provided free of charge The government shall regulate exemptions from the foregoing by ordinance The government may in particular provide for a participation in costs if the providing of the information necessitates an unreasonable expense

6) Nobody shall have the right to waive their right of information in advance

*Restrictions on the right of access*

Article 12

*a) General*

1) A file controller may refuse to provide, or restrict or defer the providing of the requested information in cases where

a) a law so provides,

b) disclosure of the requested information is prohibited by order of the courts or an authority, or

c) he is required to do so due to the overriding interest of a third party

2) In addition, an authority may refuse to provide, or restrict or defer the providing of the requested information in cases where

a) it is required to do so due to overriding public interests, and in particular in the interests of the internal or external security of the State, or

b) the communication of the information may compromise criminal proceedings or other investigative processes

3) A private file controller may additionally refuse to provide, restrict or defer the providing of the requested information when it is in his own overriding interest and on the condition that the data is not passed on to a third party

4) The file controller must indicate the reason why he is refusing, restricting or deferring access to the information

Article 13

*b) Concerning media employees*

1) A file controller who uses a file for the sole purpose of publication in the editorially-controlled section of a periodically published media organ may refuse, restrict or defer the providing of the requested information if

a) the personal data provides information as to its source,

b) access to drafts of publications would have to be granted, or

c) the public's freedom to form an opinion would be compromised

2) Journalists may additionally refuse, restrict or defer communication of the requested information if a file is being used exclusively as a personal work aid

Article 14

*Right to object*

1) Unless the use of data is required by a law, each data subject may raise an objection to the use of his data with the file controller on the grounds of violation of his overriding interests warranting protection as a result of his specific situation

2) In the event of a legitimate objection, the data processing conducted by the file controller may no longer relate to such data

3) In the event data is processed for the purpose of direct advertising, the data subject is to be notified in advance (Art 5) and is to be informed of the no-cost and immediately effective right to object to which he is entitled

## Article 14a[1]

*Certification procedure*

1) In order to increase the protection and safety of data, the manufacturers of systems or programmes for data processing as well as private individuals or authorities processing personal data may have their products, systems, procedures, and organisation assessed by recognised independent certification bodies

2) The government shall by way of ordinance issue rules on the accreditation of certification procedures and on the introduction of a data protection quality label In this, it shall take into account international law and the internationally recognised technical standards

## Article 15

*File register*

1) The Data Protection Office shall keep a file register which shall be accessible in particular via the Internet Anyone may inspect the register [2]

2) Authorities must declare all files to the Data Protection Office for registration [3]

3) Private individuals who regularly process sensitive data or personal profiles or communicate personal data to a third party must register their files if

a) the processing of such data is not subject to a legal requirement, or

b) the data subjects are unaware that such data is being processed [4]

3a) Files of private individuals to which paragraph 3 is not applicable shall be registered unless they are subject to an exception pursuant to paragraph 6 [5]

4) The files must be registered prior to opening

5) The application for registration must contain the following information

---

[1] Art 14a inserted by LGBl 2009 no 46
[2] Art 15 (1) amended by LGBl 2004 no 174 and LGBl 2008 no 273
[3] Art 15 (2) amended by LGBl 2008 no 273
[4] Art 15 (3) amended by LGBl 2004 no 174
[5] Art 15 (3a) inserted by LGBl 2009 no 46

a) the name and address of the file controller,

b) the name and complete designation of the file,

c) the person with whom the right of information can be exercised,

d) the purpose of the file,

e) the categories of the personal data being processed,

f) the categories of the recipients of the data

g) the categories of persons dealing with the file, i e third parties entering data into the file and authorised to modify the data,

h) a general discussion allowing a preliminary assessment as to whether the measures in accordance with Article 9 are sufficient to guarantee the security of data processing

6) The government shall regulate by ordinance the registration and updating of files in detail, as well as the maintenance and publication of the register The government may exempt specific kinds of files from the obligation to declare a file or from registration, provided such processing does not infringe on the privacy of the data subjects

## B. Processing of personal data by private individuals

Article 16

*Breach of privacy*

1) Whoever processes personal data may not unlawfully breach the privacy of the data subjects

2) In particular, he must not, without lawful justification,

a) process personal data in violation of the principles set down in Article 4, Article 7 (1), Article 8 (1), and Article 9 (1),

b) process data relating to a person against the express will of that person,

c) process sensitive data or personal profiles

3) Normally, if the data subject has made the data accessible to the public and has not expressly prohibited the processing of the data, processing shall not constitute a breach of privacy

*Lawful justification*

Article 17

*a) Personal data*

1) An infringement of privacy in the processing of personal data shall be unlawful unless it is justified by

a) the consent of the data subject,

b) an overriding public or private interest, or

c) the law

2) The overriding interests of the processing person shall in particular be taken into account where the processing person

a) in direct connection with the conclusion or performance of a contract, processes personal data about his contractual partner,

b) is in or wishes to enter into commercial competition with another person and processes personal data for this purpose, without disclosing the personal data to a third party,

c) processes personal data for the purpose of evaluating the creditworthiness of another person, provided the data is neither sensitive nor constitutes a personal profile, and provided that the processing person only discloses such data to a third party in the event that it is required for the conclusion or performance of a contract with the data subject,

d) processes data on a professional basis for the sole purpose of publication in the editorially-controlled section of a periodically published media organ,

e) processes data for non-personal purposes, and in particular in the context of research, planning, or statistics, and publishes the results in such a manner that the identity of the data subjects cannot be established,

f) processes data that are accessible by the general public,[1]

g) gathers data relating to a public person, provided the data concerns his public life

Article 18

*b) Sensitive data and personal profiles*

An infringement of privacy in the processing of sensitive data and personal profiles shall not be unlawful where

a) a law expressly provides for such processing,

b) such processing is indispensable for the fulfilment of a task clearly defined in a law,

c) the data subject in the specific case has authorised such processing or has personally made the data accessible to the public,

d) the processing of the data is necessary to protect interests essential to the life of the data subject or a third party, provided the data subject is incapable of granting consent for physical or legal reasons,

e) the processing of the data is conducted by non-profit organisations, under the condition that the processing only relates to members of such organisations or persons who maintain regular contact with such organisations in connection with their functions, and provided that the data is not passed on to third parties without the consent of the data subject,

f) the processing of the data is necessary for the assertion, exercise, or defence of legal claims before a court, or

g) the processing of the data is necessary for the purpose of health care, medical diagnosis, medical care or treatment, or the administration of health services, and is conducted by persons subject to professional secrecy obligations

Article 19

*Data processing by a third party*

1) The processing of personal data may be entrusted to a third party provided

a) the mandating party ensures that no processing occurs that he would not be permitted to carry out himself, and

[1] Art 17 (2)(f) amended by LGBl 2009 no 46

b) the processing is not prohibited by any legal or contractual duty of confidentiality

2) The third party shall be subject to the same duties and may assert the same grounds of lawful justification as the mandating party

3) For the purpose of securing evidence, the elements of the contract relating to data protection provisions and the requirements with respect to measures in accordance with paragraphs 1 and 2 shall be documented in written or another form

Article 19a[1]

*Anonymising and destruction of personal data*

1) Private individuals shall anonymise or destroy personal data if such data is no longer needed to achieve the purpose for which they were processed

2) There need be no anonymising or destruction if the personal data is kept beyond the original processing for historical, statistical, or scientific purposes In this case, the holder shall ensure the safe storage of the personal data by suitable organisational and technical means The government shall regulate further details by ordinance

## C. Processing of personal data by authorities

Article 20

*Responsible authority*

1) Any authority that processes personal data or has such data processed in the execution of its legal duties shall be responsible for ensuring the protection of such data

2) In the event that an authority processes personal data jointly with other authorities or with private persons, the government may regulate the specific responsibilities with regard to data protection

Article 21

*Legal principles*

1) Authorities may process personal data only if there is a legal basis for doing so

2) Sensitive data or personal profiles may be processed only if a law expressly provides therefor or if, as an exception

[1] Art 19a inserted by LGBl 2009 no 46

a) such processing is indispensable for the fulfilment of a task clearly defined in a law,

b) the Government has authorised such processing because the rights of the data subjects are not jeopardised, or[1]

c) the data subject in the specific case has granted his consent, or if his data is accessible by the general public and processing has not been forbidden [2]

Article 22

*Collection of personal data*

1) Any authority that systematically collects data, in particular through the use of questionnaires, must specify the objective of and the legal basis for the processing, the categories of persons dealing with the file, and the recipients of the data

2) The collection of sensitive data or of personal profiles must be carried out in a manner that is visible to the data subjects

Article 23

*Disclosure of personal data*

1) Authorities may disclose personal data provided they have legal grounds for doing so in terms of Art 21 or if

a) the data is indispensable for the recipient in the specific case in order to fulfil his legal duties,

b) the data subject has given his consent in the specific case or the circumstances imply such consent,

c) the data of the data subject are accessible by the general public, or[3]

d) the recipient credibly asserts that the data subject is refusing to give consent or prohibiting disclosure in order to prevent the recipient from asserting legal rights or from safeguarding other interests warranting protection whenever possible, the data subject must be allowed the opportunity to state his case before disclosure

2) Authorities may, on request, disclose the name, first name, the address and the date of birth of a person even if the conditions set forth in paragraph 1 are not fulfilled

3) Authorities may make personal data available via remote access, provided express provision is made for this Sensitive data or personal profiles may only be made available via remote access if a law expressly provides for it

[1] Art 21 (2)(b) amended by LGBl 2009 no 46
[2] Art 21 (2)(c) amended by LGBl 2009 no 46
[3] Art 23 (1)(c) amended by LGBl 2009 no 46

4) The authority shall refuse to disclose data, or restrict such disclosure or make it subject to conditions if

a) essential public interests or interests clearly warranting protection of a data subject so require, or if

b) a statutory duty of confidentiality or a specific data protection rule so requires

## Article 24

*Right to block disclosure*

1) A data subject who credibly asserts an interest warranting protection may request the responsible authority to prohibit the disclosure of certain personal data

2) The authority may refuse to prohibit disclosure or revoke any such prohibition if

a) there is a legal duty of disclosure, or

b) the performance of its duties would be compromised otherwise

## Article 25[1]

*Archiving and destroying of personal data*

1) Authorities shall offer all data that they no longer require to the National Archive in accordance with the *Archivgesetz* (Archive Act)

2) Authorities shall destroy all personal data not considered worthy of archiving by the National Archive unless the data

a) has been anonymised, or

b) is to be retained as evidence or for security purposes

## Article 26

*Processing for the purposes of research, planning, and statistics*

1) Personal data may be processed for reasons not related to the data subjects, and in particular for the purposes of research, planning, and statistics, provided that

a) the data is anonymised as soon as the objective of data processing allows it,

b) the recipient shall only pass on the data to a third party with the consent of the controller, and

c) the results of the data processing are published in a form that does not allow identification of the data subjects

[1] Art 25 amended by LGBl 2009 no 46

2) The requirements of the following provisions need not be met

a) Article 4 (3) on the purpose of the data processing,

b) Articles 18 and 21 on the legal basis for the processing of sensitive data and personal profiles, and

c) Article 23 (1) on the disclosure of personal data

Article 27

*Private law activities of the authorities*

1) In the event that an authority acts on the basis of private law, the provisions on the processing of personal data by private persons shall apply

2) Supervision shall be conducted in accordance with the provisions applicable to authorities

## III. The Data Protection Office and the Data Protection Commission[1]

### A. The Data Protection Office[2]

Article 28[3]

*Appointment and status*

1) A Data Protection Office shall be installed, which shall be organisationally attached to the Diet

2) The Data Protection Office shall consist of the Data Protection Commissioner as its head and of the other personnel

3) The Data Protection Office shall perform its duties independently and shall not be bound by any instructions

4) The Data Protection Office shall enter into an agreement with the government on the handling of organisational and administrative matters

[1] Heading before Art. 28 amended by LGBl. 2008 no. 273
[2] Heading before Art. 28 amended by LGBl. 2008 no. 273
[3] Art. 28 amended by LGBl. 2008 no. 273

Article 28a[1]

*The Data Protection Commissioner*

1) The Data Protection Commissioner shall be elected by the Diet for a term of office of eight years on the basis of a proposal by the government and after hearing the *Geschaftsprufungskommission* (Supervisory Committee of the Diet) Re-election shall be possible

2) The Data Protection Commissioner must not be a member of the Diet, the government, a court, or an administrative authority, nor may he be the head of a Liechtenstein municipality or sit on a Liechtenstein municipal council He shall lose such offices upon being appointed Data Protection Commissioner

3) The Diet may remove the Data Protection Commissioner after hearing the government in the event of a grave breach of duty, of conduct damaging the country's reputation, or for other important reasons, before his term of office is complete

4) The Data Protection Commissioner shall issue organisational regulations after hearing the Supervisory Committee of the Diet

5) Otherwise, the Data Protection Commissioner shall mutatis mutandis be subject to the *Staatspersonalgesetz* (Act on Civil Servants), the *Besoldungsgesetz* (Act on Remuneration), and the *Gesetz uber die Pensionsversicherung fur das Staatspersonal* (Act on Pension Insurance for Civil Servants)

Article 28b[2]

*Other personnel*

1) The other personnel of the Data Protection Office shall be employed by the government in agreement with the Data Protection Commissioner within the framework of the budget approved by the Diet, Art 28a (2) shall apply mutatis mutandis

2) The following entities shall have competence to take decisions under employment law concerning the other personnel of the Data Protection Office

a) the Data Protection Commissioner as far as matters are concerned that under the legislation on civil servants are up to the head of an office for independent decision,

b) the government in agreement with the Data Protection Commissioner in all other matters

3) Otherwise, the employment relationship of the other personnel shall mutatis mutandis be subject to the Act on Civil Servants, the Act on Remuneration, and the Act on Pension Insurance for Civil Servants

[1] Art 28a inserted by LGBl 2008 no 273
[2] Art 28b inserted by LGBl 2008 no 273

Article 28c[1]

*Budget and accounting*

1) The Data Protection Office shall submit the draft of its annual budget to the government after such draft has been preliminarily discussed by the Supervisory Committee of the Diet. The government shall forward the draft budget without changes to the Diet for discussion and decision.

2) The Data Protection Office shall keep its own accounts. Accounting shall be audited by the Financial Control Office within the framework of its legal powers and on instruction of the Supervisory Committee of the Diet.

Article 29

*Supervision of authorities*

1) The Data Protection Office shall supervise compliance by authorities with this Act and other regulations relating to data protection. The Government shall be exempt from such supervision.[2]

2) The Data Protection Office shall investigate cases on its own initiative or as a result of reports by third parties.[3]

3) In order to investigate cases, the Data Protection Office may request the production of documents, obtain information and have data processing activities demonstrated to it. The authorities shall be obligated to co-operate in the investigation of any case. The right to refuse to give evidence in terms of Article 108 of the *Strafprozessordnung* (Code of Criminal Procedure) shall apply mutatis mutandis.[4]

4) In the event that an investigation reveals that data protection provisions have been infringed, the Data Protection Office shall recommend that the responsible authority modify or cease data processing activities. It shall inform the Government of its recommendation.[5]

5) In the event that a recommendation is not complied with or is rejected, the Data Protection Office may refer the matter to the Data Protection Commission for decision. Notice of the decision shall be given to the data subject. The Data Protection Office may appeal against the decision of the Data Protection Commission.[6]

[1] Art. 28c inserted by LGBl. 2008 no. 273.
[2] Art. 29 (1) amended by LGBl. 2008 no. 273.
[3] Art. 29 (2) amended by LGBl. 2008 no. 273.
[4] Art. 29 (3) amended by LGBl. 2008 no. 273.
[5] Art. 29 (4) amended by LGBl. 2008 no. 273.
[6] Art. 29 (5) amended by LGBl. 2008 no. 273.

## Article 30

*Investigations and recommendations in the private sector*

1) The Data Protection Office shall conduct investigations on its own initiative or as a result of a report by a third party if[1]

a) the methods of processing are capable of infringing the privacy of one or more persons, [2]

b) files must be registered (Art 15),

c) the disclosure of data abroad must be reported (Art 8)

2) During such investigation, it may request the production of documents, obtain information and have data processing activities demonstrated to it The right to refuse testimony in terms of Article 108 of the Code of Criminal Procedure shall apply mutatis mutandis [3]

3) On the basis of its investigation, the Data Protection Office may recommend the modification or cessation of the data processing activities [4]

4) In the event that a recommendation given by the Data Protection Office is not complied with or is rejected, it may refer the matter to the Data Protection Commission for decision It may appeal against the decision of the Data Protection Commission [5]

## Article 31

*Reporting; information*

1) The Data Protection Office shall annually submit a report to the Diet and to the government, in which report it shall provide information on the scope and emphases of its activities as well as on findings and recommendations as well as their implementation These reports shall be published [6]

2) In cases of public interest, the Data Protection Office may inform the public of its findings and recommendations Personal data that are subject to official secrecy may only be published by the Data Protection Office if it has the consent of the competent authority In the event such consent is withheld by the authority, the Data Protection Commission shall take a decision, which shall be final [7]

---

[1] Art 30 (1) introductory sentence amended by LGBl 2008 no 273
[2] Art 30 (1)(a) amended by LGBl 2009 no 46
[3] Art 29 (2) amended by LGBl 2008 no 273
[4] Art 29 (3) amended by LGBl 2008 no 273
[5] Art 29 (4) amended by LGBl 2008 no 273
[6] Art 31 (1) amended by LGBl 2008 no 273
[7] Art 31 (2) amended by LGBl 2008 no 273

Article 32

*Other duties*

1) The Data Protection Office shall in particular have the following additional duties

a) it shall support private individuals and authorities by giving a general introduction and providing individual consulting services,

b) it shall submit opinions on questions of data protection in pending cases at the request of the decision-making bodies or appellate authorities,

c) it shall certify the extent to which foreign data protection laws offer adequate protection, [1]

d) it shall comment on bills and decrees of significance for data protection and shall in particular review their compliance with the provisions of EU Directive 95/46,

e) it shall co-operate with data protection authorities both within and outside Liechtenstein,

f) it shall represent the Principality of Liechtenstein in the Working Party on the Protection of Individuals with regard to the Processing of Personal Data pursuant to Article 29 of EU Directive 95/46 [2]

g) it shall examine the guarantees and data protection rules reported to in pursuant to Art 8 (3) [3]

h) it shall examine the certification procedures pursuant to Art 14a and may issue statements in terms of Art 29 (4) or Art 30 (3) It may also be given the duties of an accreditation body [4]

2) It may consult authorities even where this Act is not applicable in accordance with Article 2 (3)(c) through (f) Such authorities may allow the Data Protection Office to inspect their papers [5]

## B. The Data Protection Commission

Article 33

*The Data Protection Commission*

1) The Data Protection Commission shall consist of three members which shall be elected by the Diet for a term of four years together with two substitute members The Diet shall designate the President and Vice President of the Commission

[1] Art 31 (1)(c) amended by LGBl 2009 no 46
[2] Art 32 (1) amended by LGBl 2008 no 273
[3] Art 31 (1)(g) inserted by LGBl 2009 no 46
[4] Art 31 (1)(h) inserted by LGBl 2009 no 46
[5] Art 32 (2) amended by LGBl 2008 no 273

2) Members of the Data Protection Commission shall be subject to the provisions of the *Landesverwaltungspflegegesetz* (LVG, Act on General Administrative Procedure) on work stoppages, responsibilities, and the prohibition on reporting. Such members must take the oath of office prior to taking office.

Article 34

*Duties*

The Data Protection Commission makes decisions on

a) the recommendations of the Data Protection Office (Art. 29 (5), Art. 30 (4)) that are laid before it, [1]

b) appeals against decisions made by the authorities relating to data protection matters with the exception of those made by the government

c) appeals against decisions of the Data Protection Office pursuant to Art. 6a (3). [2]

Article 35

*Interim measures*

1) Upon the request of a party or the Data Protection Office, the President of the Data Protection Commission may take interim measures which appear necessary for the interim regulation of an existing state of affairs or to guarantee legal relations which are at risk. [3]

2) Appeals against interim measures shall not have a suspensive effect.

3) The Data Protection Commission shall decide on appeals against measures taken by the President. The appeals period shall be 14 days.

Article 36

*Compensation*

Members of the Data Protection Commission shall be compensated for their activities pursuant to the provisions of the Act on the Remuneration of Members of the Government, the Courts, and the Commissions.

---

[1] Art. 34 (1)(a) amended by LGBl. 2008 no. 273.
[2] Art. 31 (1)(h) inserted by LGBl. 2009 no. 46.
[3] Art. 35 (1) amended by LGBl. 2008 no. 273.

# IV. Legal safeguards

## A. Processing of personal data by private individuals

Article 37

*Claims and legal procedures*

1) Legal proceedings or interim measures (protective measures) relating to the protection of privacy are governed by Articles 39 through 41 of the *Personen- und Gesellschaftsrecht* (Persons and Companies Act) The plaintiff in any legal proceedings may specifically request that the personal data be corrected or destroyed, or that its disclosure to third parties be prohibited

2) If neither the accuracy nor the inaccuracy of personal data can be established, the plaintiff may request that the particular data be marked accordingly

3) The plaintiff may request the notification of third parties or the publication of the judgment relating to the data or its correction, destruction, prohibition of communication, or the marking of the data as to its litigious character

4) The procedural provisions on non-contentious matters shall apply in the event of actions for the assertion of the right for information

## B. Processing of personal data by authorities

Article 38

*Rights and procedures*

1) Anyone with an interest warranting protection may request that the responsible authority

a) refrain from proceeding with unlawful data processing,

b) nullify the effects of unlawful data processing,

c) declare the unlawful nature of the data processing

2) If neither the accuracy nor the inaccuracy of personal data can be established, the authority shall be required to mark the data with a note to this effect

3) The person making the request may in particular request that the authority

a) correct or destroy the data or ensure that it is not disclosed to a third party,

b) publish or communicate to third parties its decision, namely to correct or destroy the personal data or prohibit its disclosure or to mark it as being of contentious nature

4) The procedure shall be governed by the Act on General Administrative Procedure (LVG)

5) The decisions and orders of the authorities shall be subject to a right of appeal to the Data Protection Commission within 14 days from service The decisions made by the Commission shall be subject to a right of appeal to the *Verwaltungsgerichtshof* (Administrative Court) within 14 days from service [1]

6) Decisions made by the Government may be appealed to the Administrative Court within 14 days from service [2]

## V. Penal Sanctions

### Article 39

*Unauthorised collection of personal data*

Whoever collects sensitive personal data without authorisation from a file which is not freely accessible shall at the request of the injured party be punished by the *Landgericht* (Court of Justice) by imprisonment for up to one year or by a fine of up to 360 daily rates

### Article 40

*Breach of duties to provide information, to register data, and to co-operate*

1) Private individuals who fail to fulfil their duties as set out in Art 5 and Art 11 to 13 by intentionally providing inaccurate or incomplete information shall at the request of the injured party be punished by a fine of up to 20,000 Swiss francs, and by a term of detention of up to three months in the event the fine is uncollectible [3]

2) The same punishment shall apply to private individuals who intentionally

a) fail to report files in terms of Art 15 or who provide false information in their report, [4]

b) in the investigation of a case (Art 30) provide false information to the Data Protection Office or refuse to co-operate [5]

---

[1] Art 38 (5) amended by LGBl 2004 no 33
[2] Art 38 (6) amended by LGBl 2004 no 33
[3] Art 40 (1) amended by LGBl 2009 no 46
[4] Art 40 (2)(a) amended by LGBl 2009 no 46
[5] Art 40 (2)(b) amended by LGBl 2008 no 273

c) transfers data abroad without permission in terms of Art 8 (3) [1]

Article 41

*Breach of professional secrecy*

1) Whoever intentionally and without authorisation discloses confidential and sensitive personal data or personal profiles that have come to his knowledge in the course of professional activities that require that he has knowledge of such data shall at the request of the injured party be punished by up to one year of imprisonment or by a fine of up to 360 daily rates

2) The same punishment shall apply to whoever intentionally and without authorisation discloses confidential and sensitive personal data or personal profiles that have come to his knowledge in the course of his activities for persons who are subject to a duty of professional secrecy or in the course of his vocational training with such persons

3) The illegal communication of confidential and sensitive data or personal profiles shall remain punishable also after the relevant person has ceased to practice his profession or has completed his vocational training

## VI. Transitional and final provisions

Article 42

*Implementation*

1) The government shall issue the ordinances necessary for implementing this Act, in particular relating to

a) exceptions to Article 11 (5) on information and Article 21 (2)(b) on the processing of sensitive data and personal profiles,

b) the categories of files which require processing regulations,

c) the requirements under which an authority may process personal data for third parties or have such data processed by third parties,

d) the disclosure of data pursuant to Article 23 (2) and remote access pursuant to Article 23 (3),

e) the use of means to identify individual persons,

f) data security

[1] Art 40 (2)(c) inserted by LGBl 2009 no 46

2) The government may provide for exceptions to Articles 12 and 13 for the provision of information through embassies and consulates of the Principality of Liechtenstein abroad

3) The government shall regulate how files are to be secured whose data can result in a danger to the life and limb of the data subjects in the event of a crisis or war

Article 43

*Processing of personal data in specific cases involving crime fighting and state security*

1) Concerning the processing of personal data for fighting terrorism, violent extremism, organised crime, and illicit intelligence gathering and to guarantee state security, the government may (until an Act comes into force regulating these matters)

a) provide for exceptions to the provisions on the purpose of data processing (Art 4 (3)), the disclosure of data abroad (Art 8), the obligation to report and register (Art 15), and the collection of personal data (Art 22),

b) approve the processing of sensitive data and personal profiles even if the requirements of Art 21 (2) are not met

2) Ballot, petition, and statistical secrecy shall be preserved

3) The government shall make its decision after consulting with the Data Protection Office instead of the Data Protection Commission or its president Decisions made by the government may be appealed to the Administrative Court within 14 days after service [1]

Article 44

*Transitional Provisions*

1) File controllers must register any existing files that must be registered in terms of Art 15 within one year of the date on which this Act comes into force

2) Within one year of the date on which this Act comes into force, they must take the measures required to allow them to disclose information in terms of Art 11

3) File controllers may continue to use existing files that contain sensitive personal data or personal profiles until 1st August 2007 without having to fulfil the requirements of Art 18 and 21 [2]

[1] Art 43 (3) amended by LGBl 2004 no 33 and LGBl 2008 no 273
[2] Art 44 (3) amended by LGBl 2004 no 174

Article 45

*Commencement*

1) This Act shall come into force on 1 August 2002, subject to paragraph 2 below

2) Articles 28 and 33 shall come into force on the date of proclamation

signed *Hans-Adam*

signed *Otmar Hasler*
Prime Minister

# Transitional Provisions

## 235.1 Data Protection Act (*Datenschutzgesetz*, DSG)

**Liechtenstein Law Gazette**

**2008 No. 273 issued on 14 November 2008**

# Act

of 17 September 2008

# on the Amendment of the Data Protection Act

...

## III.

### Transitional provisions

1) At the time this Act enters into force[1], the current Data Protection Commissioner shall become the head of the Data Protection Office and shall hold this position until 31 December 2016 Before this time period expires, the Diet shall appoint the Data Protection Commissioner in accordance with Art 28a

2) The existing employment relationships of the other personnel shall remain in force after this Act has entered into force

...

[1] Date of entering into force 1 January 2008

# Act
of 11 December 2008
# on the Amendment of the Data Protection Act

...

## II.

### Transitional provision

For existing video surveillance, approval in terms of Art 6a (3) shall be obtained immediately, but no later than within 6 months from the date this Act enters into force [1]

...

[1] Date of entering into force 1 July 2009