Official 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 makes 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 Commissioner, the file controller must appoint a representative in Liechtenstein.

3) It 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 Constitutional Court;

e) the activities of the national audit office;

f) public registers relating to private law matters;

g) personal data which is to be collected on the basis of the Due Diligence Act.

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;

b) "**persons affected**": 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;

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

h) "**disclosure**": 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 individual;

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 office which receives data, regardless of whether the data relates to a third party or not. However, authorities which may receive data as part of an individual investigation are not considered recipients;

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

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

II. Use of data

A. General provisions

Article 4

Principles

1) Personal data must be collected in a lawful manner.

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

3) Personal data may only be processed for the purpose either for which it was collected, which is evident from the circumstances, or which is provided for by law.

Article 5

Prior notification

1) In the event that data is collected, the file controller must provide the person affected with the following information at the least, unless the person affected 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 person affected, the controller must provide the affected person 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 person affected is impossible, is only possible at unreasonable expense, 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 affected person'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 person affected or after the affected person was given opportunity to comment; or

b) such decisions are allowed by a law.

Article 7

Data accuracy

1) Whoever processes personal data must ensure that the information is correct.

2) Any person affected may request the rectification of inaccurate data.

Article 8

Transborder data flows

1) No personal data may be transferred abroad if the personal privacy of the persons affected could be seriously endangered, in particular where there is a failure to provide protection equivalent to that provided under Liechtenstein law. This shall not apply to states which are party to the EEA Agreement.

2) Whoever wishes to transmit data abroad must notify the Data Protection Commissioner beforehand in cases where:

a) there is no legal obligation to disclose the data and

b) the persons affected have no knowledge of the transmission.

3) The government shall regulate the notification procedure in detail.. The government may in particular:

a) allow simplified notifications or grant exemptions from the notification obligation, provided the data processing does not infringe on the privacy of the persons affected;

b) designate states which do not meet the requirements of paragraph 1 sentence 1 pursuant to Article 25 paragraph 4 of EU Directive 95/46.

Article 9

Data security

1) Personal data must be protected against unauthorised processing by appropriate organisational and technical means.

2) The Government shall enact more detailed provisions on the minimum data security measures.

Article 10

Data confidentiality

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 information

1) Anyone may ask a file controller if data relating to him is being processed. The Government shall enact a regulation 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 individual 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 person affected in the event of automated decisions pursuant 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 affected person 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. The government may in particular provide for a participation in costs if the provision of the information necessitates an unreasonable expense.

6) No authority shall have the right to waive their right of information in advance.

Restrictions on the right to information

Article 12

a) General

1) A file controller may refuse to provide, or restrict or defer the provision 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 provision 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 provision 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)Restriction of the right to information for 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 provision of the requested information if:

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

b) a right to examine drafts for publication must result; or

c) the freedom to shape public 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 affected party may raise an objection to the use of his data with the file controller for violation of his overriding interests resulting from his specific situation.

2) In the event of a legitimate objection, the data processing conducted by the file controller may no longer relate to the affected person's data.

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

Article 15

File register

1) The Data Protection Commissioner shall keep a file register which shall be accessible in particular via internet. Anyone may inspect the register. [1]

[1] Art. 15, paragraph 1 as amended by LGBl. 2004 No. 174

2) Authorities must declare all files to the Data Protection Commissioner for registration.

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[1]

b) the persons affected are unaware that such data is being processed.

4) The files must be registered prior to processing.

5) The registration must contain the following information:

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 the data processing.

6) The government shall regulate 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 notification duty or registration, provided such processing does not infringe on the privacy of the persons affected.

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 persons affected.

[1] Art. 15, paragraph 3 as amended by LGBl. 2004 No. 174

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

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

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

c) process sensitive data or personal profiles.

3) In principle, there shall be no breach of privacy in the event the person affected has made the data accessible to the public and had not expressly prohibited processing of the data.

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 person affected;

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 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 person affected;

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 persons affected cannot be established;

f) processes data which the person affected has personally made accessible to the public;

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 when:

a) a law expressly provides therefore;

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

c) the person affected 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 affected person or a third party, provided the person 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, provided the data is not passed on to third parties without the consent of the affected person;

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

b) the processing is not prohibited by a 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.

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, exceptionally:

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

b) the Government has authorised such processing because rights of the persons affected are not jeopardised; or

c) the person affected in the specific case has granted express consent or has personally made the data accessible to the public.

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 persons affected.

Article 23

Disclosure of personal data

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

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

b) the person affected has given his express consent in the specific case or the circumstances imply such consent;

c) the person affected has made the data accessible to the public; or

d) the recipient credibly asserts that the person affected is refusing to give consent or prohibiting disclosure in order to prevent the recipient from asserting legal rights or from safeguarding other interests that are worthy of protection: whenever possible, the person affected must be allowed the opportunity to state his case.

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 therefore. Sensitive data or personal profiles may only be made available via remote access provided a law provides therefor.

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

a) essential public interests or if the clear interests of the person affected so require, or if

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

Article 24

Prohibition of disclosure

1) A person affected who credibly asserts a legitimate interest 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.

Article 25

Making data anonymous, destroying data

Authorities must make personal data that they no longer require anonymous or destroy such data unless the data:

a) is to be retained as evidence or for security purposes, or

b) is to be delivered to the National Archives or other archives in terms of the Archives Act.

Article 26

Processing for the purposes of research, planning, and statistics

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

a) the data is made anonymous as soon as the objective of the data processing allows;

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 persons affected.

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

a) Article 4 paragraph 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 paragraph 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 of such private law activities shall be conducted in accordance with the provisions applicable to Authorities.

III. The Data Protection Commissioner and the Data Protection Commission

A. The Data Protection Commissioner

Article 28

Appointment and status

1) The Data Protection Commissioner shall be appointed by the government.

2) He shall perform his duties autonomously and may be affiliated with a government department.

3) The government shall regulate the specific details with respect to organisation and compensation.

Article 29

Supervision of authorities

1) The Commissioner shall supervise compliance by authorities with this Act and other regulations relating to data protection. The government shall be exempted from such supervision.

2) The Commissioner shall investigate cases on his own initiative or at the request of third parties.

3) In order to investigate cases, he may request the production of documents, obtain information and have data processing activities explained to him. 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 Code of Criminal Procedure shall apply by analogy.

4) In the event that an investigation reveals that data protection provisions have been infringed, the Commissioner may recommend that the responsible authority modify or cease data processing activities. He shall inform the government of his recommendation.

5) In the event that a recommendation is not complied with or is rejected, the Commissioner may refer the matter to the Data Protection Commission for decision. Notice of the decision shall be given to the persons affected.

Article 30

Investigations and recommendations in the private sector

1) The Commissioner shall conduct investigations on his own initiative or at the request of a third party when

a) the methods of processing are capable of infringing the privacy of a large number of persons;

b) files must be registered (Article 15);

c) disclosure of data abroad must be declared (Article 8).

2) He may request the production of documents, obtain information and have data processing activities explained to him. The right to refuse to give evidence in terms of Article 108 of the Code of Criminal Procedure shall apply by analogy.

3) On the basis of his investigation, the Data Protection Commissioner may recommend the modification or cessation of the data processing activities.

4) In the event that a recommendation is not complied with or is rejected, he may refer the matter to the Data Protection Commission for decision.

Article 31

Information

1) The Commissioner shall submit a report at regular intervals and as required to the government. These periodical reports shall be published.

2) In cases of public interest, he may inform the public of his findings and recommendations. He may only disclose data that has been given to him subject to official secrecy if he has the consent of the competent authority. In the event such consent is withheld by the authority, the Data Protection Commission shall make a decision, which shall be final.

Article 32

Other duties

1) The Commissioner shall have the following additional duties:

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

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

c) he shall certify the extent to which foreign data protection laws are equivalent to the data protection laws of Liechtenstein;

d) he shall comment on bills and decrees of significance for data protection law and shall particularly review their compliance with the provisions of EU Directive 95/46;

e) he shall co-operate with data protection authorities both within and outside Liechtenstein;

f) he 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) The Commissioner may consult authorities even where this Act is not applicable in accordance with Article 2 paragraph 3 letters c through f. Such authorities may allow him to inspect their papers.

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 alternate members. The Diet shall designate the President and Vice President of the Commission.

2) Members of the Data Protection Commission shall be subject to the provisions of 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 Commissioner (Article 29 paragraph 5; Article 30 paragraph 4) that are laid before it;

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

Article 35

Interim measures

1) Upon the request of a party or the Data Protection Commissioner, 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.

2) Appeals against interim measures shall 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 law relating to the remuneration of members of the government, courts, commissions, and organs of establishments and foundations of the state.

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 Civil and Corporate Law. 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) In the event the accuracy or inaccuracy of personal data cannot be established, the plaintiff may request that the particular data be marked accordingly.

3) The plaintiff may request the notification of third parties or 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 legal aid procedure 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 a legitimate interest 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 the accuracy or inaccuracy of personal data cannot 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.

5) The decisions and orders of the authorities shall be subject to a right of appeal to the Data Protection Commission within 14 days after service. The decisions made by the Commission shall be subject to a right of appeal to the Administrative Appeals Court within 14 days of service.

6) Decisions made by the government may be appealed to the Administrative Appeals Court within 14 days after service.

V. Penal Sanctions

Article 39

Unauthorised collection of personal data

Whoever collects sensitive personal data from a file which is not freely accessible without authorisation shall be punishable by the Princely Court on application for prosecution by a term of detention of up to one year or 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 Articles 11 and 13 by wilfully providing inaccurate or incomplete information shall be punishable on application for prosecution by a fine of up to 20,000 Francs, and by a term of detention of up to three months in the event the fine is not paid.

2) Private individuals who wilfully:

a) fail to declare files in terms of Article 15 or a disclosure of data abroad in terms of Article 8 or who provide false information in their declaration;

b) provide false information to the Data Protection Commissioner or refuse to co-operate in the investigation of a case (Article 30).

Article 41

Breach of professional secrecy

1) Whoever wilfully 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 be punishable on application for prosecution with detention of up to one year or a fine of up to 360 daily rates.

2) Whoever wilfully 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 shall also be punishable on application for prosecution by a term of detention of up to one year or a fine of up to 360 daily rates.

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

VI. Transitional and final provisions

Article 42

Implementation

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

a) exceptions to Article 11 paragraph 5 on information and Article 21 letter 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 paragraph 2 and remote access pursuant to Article 23 paragraph 3;

e) the use of means to identify individual persons;

f) data security.

2) The government may enact 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 persons affected in the event of a crisis or war.

Article 43

Processing of personal data in specific cases involving crimefighting and state security

1) Until an Act comes into force regulating the processing of personal data for fighting terrorism, violent extremists, organised crime, and illicit news services and to guarantee state security, the government may:

a) make exceptions to the provisions on the purpose of the data processing (Article 4 paragraph 3), the disclosure of data abroad (Article 8), the notification obligation, registration (Article 15), and the collection of personal data (Article 22);

b) approve the processing of sensitive data and personal profiles even if the requirements of Article 21 paragraph 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 Commissioner at the offices of the Data Protection Commission or the president thereof. Decisions made by the government may be appealed to the Administrative Court within 14 days after service.

Article. 44

Transitional Provisions

1) File controllers must declare any existing files that must be registered in terms of Article 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 Article 11.

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

[1] Art. 44, paragraph 3 as 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