Act on Protection and Processing of Personal Data, No. 77/2000 of May 10, 2000

as amended by Act No. 90/2001, Act No. 30/2002, Act No. 81/2002 and Act no. 46/2003.

Entered into force on January 1, 2001.

Act No. 90/2001 entered into force June 15, 2001, Act No. 30/2002 entered into force April 16, 2002, Act No. 81/2002 entered into force May 17, 2002, Act No. 46/2003 entered into force 14. March 2003.

Act

on Protection of Individuals with regard to the Processing

of Personal Data No. 77/2000

CHAPTER I. Object, definitions and scope ➦

Section 1. Purpose ➦

The purpose of this Act is to promote the practice of personal data being processed in

conformity with the fundamental principles and rules of data protection and the right to privacy, to ensure reliability and quality of such data and the free flow of personal data within the internal market of the European Economic Area.

A particular authority, the Personal Data Protection Authority, shall control the implementation of this Act and any administrative rules issued in conformity with it, as further provided for in Section 36.

Section 2. Definitions ➦

For the purposes of this Act, words and terms shall mean as follows:

1. Personal data: Any information relating to an identified or identifiable natural person, i. e. information that can be directly or indirectly traced to a particular individual, living or dead.

2. Processing: Any operation or set of operations performed upon personal data, whether manually or by automatic means.

3. File: Any structured collection of personal data where data on certain individuals can be located.

4. Controller: The party who determines the purpose of the processing of personal data and decides what equipment and methods are to be used, and what shall be done with the data.

5. Processor: A party processing personal data on behalf of the controller.

6. Electronic surveillance: Surveillance, which is constant or regularly repeated, and incorporates the monitoring of individuals with the use of remote controlled or automatic equipment, and takes place in a public area or where a limited group of people normally traverses. The concept entailes:

a. surveillance which leads to, shall or may lead to the processing of personal data, and

b. tv surveillance which is conducted by using cameras, web cams or other comparable equipment, without any collection of recorded material or any other actions equal to processing personal data.

7. Consent: An explicit signified declaration, freely given, indicating that the data subject consents to the processing of certain personal data relating to him and that he is aware of the purpose of the processing, how it is to take place, how privacy is to be ensured, that he or she is free to revoke the consent, etc.

8. Sensitive data:

a. Data revealing a person's racial or ethnic origin, skin colour, political opinions, religious beliefs and other convictions.

b. Data revealing on whether a person has been suspected of, charged with, indicted for, or sentenced on account of a punishable offence.

c. Health data, including genetic data and data revealing any medical or non-medical use of drugs or alcohol.

d. Data on sexual life.

e. Data on trade union membership.

9. Automated individual decision: A decision which produces legal rights and/or duties of one or more particular individuals based solely on automated processing of data.

Section 3. Scope ➦

This Act shall apply to any automated processing of personal data. It shall also apply to manual processing of personal data that are, or are intended to be, a part of a file.

The provisions of Sections 16, 18 to 21, 24, 26, 31 and 32 shall not apply to the processing of personal data relating to public security, national defence, state security, or the activities of the state's criminal justice system. The Act shall not apply to a private individual's processing of data solely relating to his or her private affairs, or solely intended for personal use.

Section 4. Electronic surveillance ➦

Electronic surveillance must only be conducted for legitimate purposes. Electronic surveillance of premises where a limited group of people normally traverses, must also be necessary due to the nature of the activities conducted there.

The processing of personal data in connection with electronic surveillance must be in accordance with the provisions of this Act.Tv surveillance is, in addition to Para. 1, subject to the following provisions of this Act: Art. 7., 24., 40. og 41. gr., and, where applicable, Art. 31, 32 and 38.

Section 5. Connection with freedom of expression ➦

To the extent necessary in order to achieve a balance between the right to privacy on the one hand and the freedom expression on the other, exemptions may be made from the provisions of this Act in the interests of journalism, art and literature. When personal data are processed solely for the purposes of journalism or literary or artistic expression, only the provisions of Section 4, Section 7 (1) and (4), Sections 11to13, Section 24 and Sections 42 to 43 shall apply.

Section 6. Geographical application ➦

The Act shall apply to the processing of personal data on behalf of a controller established in Iceland.

The Act shall also apply to the processing of personal data on behalf of a controller established in a state outside the European Economic Area, if his equipment is located in Iceland. In such cases the controller shall nominate someone established in Iceland to represent him, and the provisions of the Act concerning controllers shall then apply to the representative as applicable.

The provisions of the second paragraph shall not apply if the equipment in question is solely used to send personal data through Iceland.

CHAPTER II. General principles concerning processing of personal data ➦

Section 7. General principles concerning processing of personal data ➦

When processing personal data, all the following shall be observed:

1. that they are fairly, appropriately and lawfully processed, and that they are processed as required by good practice in processing such data;

2. that they are obtained for an explicit and clear purpose and not processed any further in a different and incompatible purpose; however, further processing for historical, statistical or scientific purposes shall not be deemed incompatible provided reasonable security precautions are observed;

3. that they are adequate and relevant, and that they do not exceed what is necessary with a view to the purpose of the processing;

4. that they are accurate and updated as necessary. Personal data that are unreliable or incomplete, having regard to the purpose for which they where collected, shall be erased or rectified;

5. that they are not kept in a form which permits identification of the data subjects for a longer time than necessary with a view to the purpose for which they where collected.

Section 8. Processing of general personal data ➦

Processing of personal data is legitimate if one or more of the following requirements are met:

1. that the data subject has provided his or her consent;

2. that the processing is necessary for the performance of a contract concluded by the data subject, or in order to take measures upon the request of the data subject before a contract is concluded;

3. that the processing is necessary in order for the controller to comply with a legal obligation;

4. that the processing is necessary in order to protect the vital interests of the data subject;

5. that the processing is necessary for the performance of a task in the public interest;

6. that the processing is necessary in exercising public authority vested in the controller or a third party to whom the data are transferred;

7. that the processing is necessary in order to enable the controller, a third party or any other parties to whom the data are transferred, to safeguard lawful interests, if this is not prevented by the fundamental rights and freedoms of the data subject given protection in

law.

Section 9. Processing of sensitive personal data ➦

Processing of sensitive personal data is prohibited unless one or more of the following requirements have been met:

1. that the data subject has given his consent to the processing;

2. processing is specifically allowed in other acts of law;

3. that the controller is obliged to process the data according to an agreement concluded by the social partners;

4. that the processing is necessary in order to protect important interests of the data subject or other person who is unable to provide consent as required in Point 1 above;

5. that the processing is conducted by a trade-union or other non-profit-seeking organisation, such a an organisation with cultural, humanitarian, social or idealistic aims, provided the processing is a part of such organisation's lawful activity and only relates to its own members or persons who have, or have had, regular connection with the organisation in the context of its aims. Such personal data may however not be disclosed to others without the data subject's consent.

6. that the processing only relates to data that the data subject himself has made public;

7. that the processing is necessary in order to delineate a claim, submit a claim or present a defence against a claim in litigation or on account of other similar legal needs;

8. that the processing is necessary on account of medical treatment or in the routine exercise of public administration in the field of public health, and the processing is performed by an employee of the health care system subject to the duty of maintaining secrecy;

9. that the processing is necessary on account of statistical or scientific research.

The Personal Data Protection Authority may allow the processing of sensitive personal data in other instances than enumerated under the first paragraph, if the Authority deems that important public interests recommend this. For this the Authority may set the conditions it deems necessary in each case in order to secure the interests of the data subjects, and that privacy is ensured by specific safeguards as applicable.

Having obtained the opinion of the Science Ethics Committee, the Personal Data Protection Authority shall issue rules on how people can be selected and approached for participation in scientific research, and what information they shall be given before they are asked to give their consent.

The Personal Data Protection Authority shall resolve any disputes as to what personal data shall be deemed sensitive.

Section 10. The use of national identification numbers ➦

National identification numbers may only be used for pertinent purposes and if it is necessary in order to ensure reliable personal identification. The Personal Data Protection Authority may prohibit or order the use of the national identification numbers.

Section 11. Reliability and quality of personal data ➦

The controller shall be responsible for security assessment and safeguards as required by the standards of the Personal Data Protection Authority and other rules set by the Authority concerning data security. The controller shall also make certain that personal data are processed as required by Section 7.

The controller is responsible for conducting regular security assessments and taking systematic safety measures in order to comply with the requirements of the first paragraph.

The controller shall maintain a register of his security assessments and the safety measures taken, to which the Personal Data Protection Authority shall have access at any time.

Section 12. Internal control ➦

The controller shall exercise internal control and prepare regular reports thereon. The reports shall include information on the system used for the control and how it ensures compliance with the requirements of this Act and the conditions set in permits issued under Section 35 and/or orders issued under Section 40.

The Personal Data Protection Authority may issue further instructions on internal control.

Section 13. A processor's processing of personal data ➦

A processor may not use personal data for any other purpose than originally decided, unless the controller requests so. A processor may not deliver data to others for safekeeping or for processing except in consultation with the controller.

Section 14. Time limits for compliance ➦

A controller shall act upon any communication sent him under the provisions of Sections 16, 18, 22, 25, 26, 27 and 28 as soon as possible, and no later than one month after receiving it.

If, due to extraordinary circumstances, a controller can not bring a matter to a conclusion within one month, he may do so later. In such cases the controller shall, within the time limit of one month, explain the reasons for the delay to the party in question, in writing, and state when a reply may be expected.

Section 15. Payment of costs ➦

Communications received as provided for in Sections 16, 18, 22, 25, 26, 27 and 28 shall be acted upon free of charge. If the costs involved are high, for example due to photocopying of documents, payment may however be collected in accordance with a rate issued by the Minister of Justice in the form of an administrative regulation.

CHAPTER III. Right to receive, and duty to provide, information ➦

Duty to provide guidance and warning

Right to reasoning

Section 16. The right to general information on the processing of personal data ➦

A controller has the duty of providing any person with general information on the processing of personal data taking place on his behalf.

As regards any particular category of processing, any person who so requests shall furthermore be provided with information on the following points:

1. the name and address of the controller and, as the case may be, his representative under Section 6;

2. the identity of the party responsible for routine compliance with the duties if a controller under this Act;

3. the purpose of the processing;

4. a definition or other characterisation of the kind of personal data processed;

5. the origin of the data;

6. the recipients of the data, including whether the plan is to send the data abroad, and if so, to whom.

A request according to the first paragraph shall be directed to the controller or his representative according to Section 6. A clarification in writing may be requested of the points on which information is asked.

Section 17. Publicizing of processing operations ➦

The Personal Data Protection Authority shall maintain a record of all processing notified to the Authority as provided for in Section 31, and any processing it permits as provided for in Section 33. The record shall contain, as a minimum, the points enumerated in the second paragraph of Section 16.

The record shall be accessible by the public in a manner to be decided by the Personal Data Protection Authority.

Section 18. The data subject's right of access ➦

A data subject shall be entitled to obtain from the controller information about:

1. what data on relating to him are being, or has been. processed;

2. the purpose of the processing;

3. who receives, has received or will receive, data relating to him;

4. the origin of the data;

5. what safeguards have been established for the processing, provided this does not compromise the security of the data.

A request for access as provided for in the first paragraph shall be directed to the controller or his representative under Section 6. The information shall be provided in writing if requested.

Section 19. Restrictions of the data subject's right of access ➦

The right of the data subject's right of access under Section 18 does not cover data solely used for statistical processing or scientific research in cases where its processing can not directly affect his interests.

The provisions of Section 18 shall not apply if the data subject's right under that section is deemed subordinate, in part or in whole, to the interests of others, or other interests of his own. In this, the considerations to be taken into account shall include the data subject's health and the interests of his family members. A representative of the data subject may however be provided the information if there are no specific reasons against this.

The right of the data subject under Section 18 does not cover data to which access is restricted by the Information Act or the Administrative Procedures Act. As regards data in the possession of other controllers than administrative authorities, the provisions of Section 18 shall not reach to information contained in preparatory documents and other similar data prepared by the controller himself or persons working on his behalf, such as councillors or experts.

Even if the data subject is not entitled to access by reason of the provisions of the third paragraph, he may request a written exposition of the contents of the data or an excerpt or summary thereof, unless he is able to acquaint himself with the facts of the matter by other means.

If the provision of certain data compromises the possibility of concluding a matter for resolution, such data may be withheld until the matter has been prepared for resolution.

The Minister may, by an administrative regulation, issue provisions setting conditions for exercise of a data subject's access to data.

Section 20. The duty to provide information in cases of collection of data from the data subject ➦

When personal data are obtained from the data subject, he or she shall be provided with information on the identity of the controller, the purpose of the collection of the data, how the data will be identified, to whom the data will be disclosed, and whether the data subject is under a duty to provide the requested data or whether he may decline to do so, and what effect a denial may have. This duty rests with the controller, or, as the case may be, the processor, but shall not apply if the data subject has already been informed of these facts.

Further information shall be provided if this is necessary in order to enable the data subject to guard his interests; he shall then for example be informed of his right to information under Section 18, cf. Section 19, and of his right to demand correction or erasure of data.

Section 21. Duty to provide warning when personal data are collected from others than the data subjects ➦

When personal data are collected from others than the data subject, the controller shall at the same time notify the data subject and inform him of the points enumerated in the second paragraph of Section 16. If the plan is to disclose the data within a reasonable period of time from its collection, such warning may be delayed until the data are disclosed for the first time. Any controller engaged in dissemination of data on financial matters and credit rating shall however provide such warning within14 days before the data are disclosed for the first time.

The provisions of the first paragraph shall not apply if:

1. the Personal Data Protection Authority deems a warning impracticable or that a warning would place a heavier burden upon the controller than can reasonably be demanded;

2. the data subject may be assumed to be already aware of the processing, or

3. filing and disclosure of that data is allowed by law.

Section 22. Reasoning to be provided ➦

For automated individual decisions

If an automated decision has been taken, which is exclusively based on automated processing of personal data, the party to whom the decision relates can request reasoning for the decision. In the reasoning, the rules applying to the automated data processing, on which the decision is based, shall be explained.

Section 23. Warnings concerning use of personal profiles ➦

When a personal profile defining a certain behaviour, taste, ability or need is used as a basis for

1. bringing in automated individual decision as referred to in the second paragraph of Section 9;

2. contacting a data subject, selecting a sample or a target group, etc,

the Personal Data Protection Authority can, when it has received a notification of such processing, order the controller to notify the data subject and inform him who controls the processing, what data are being used and where that data comes from.

In taking a decision in accordance with the first paragraph the Personal Data Protection Authority's assessment of whether a warning is practicable, or whether it places a heavier burden upon the controller than can reasonably be demanded, shall be among the factors taken into consideration.

Section 24. Warnings of video surveillance ➦

When a workplace or a public space is monitored by video surveillance, a clear warning shall be given of that fact by a sign or otherwise, stating the controller's identity.

CHAPTER IV. Corrections, deletions, closures, etc ➦

Section 25. Correction and deletion of incorrect or incomplete data ➦

If incorrect, misleading or incomplete personal data have been processed, or if the processing of such data has not been legitimate, the controller shall have the data corrected, deleted or improved, if the shortcoming in question is suited to affect the interests of the data subject. If such data have been disclosed or used, the controller shall to the extent possible prevent it from affecting the interests of the data subject.

If deletion or change of the data referred to in the first paragraph is not allowed by reason of the provisions of other laws, the Personal Data Protection Authority may prohibit use of the data.

Section 26. Deletion of, and prohibition of use of, personal data that is neither incorrect nor incomplete ➦

When there is no longer a valid reason to preserve personal data, the controller shall have it deleted. Valid reasons to preserve data may include provisions of law, or that the controller is still processing the data in conformity with the original purpose of their collection.

If the provisions of other laws do not stand in the way, a data subject may nevertheless request deletion of data concerning him, or a prohibition of their use, if this is deemed justified following a comprehensive assessment of the interests involved. In making such interest assessment the interests of others, general considerations of privacy, public interests, and the measures necessary for complying with the request shall be taken into account.

The Personal Data Protection Authority may, in individual cases as well as by the issue of general provisions, prohibit the use of such data or order their deletion.

Section 27. The right to a decision based on manual processing of data ➦

If an automated decision, as defined in Section 2 (9), has been taken, the party to whom the decision relates, or any party otherwise directly affected by the matter, may request a manual processing of the decision, provided that decision relates to the personal situation or traits of the party in question and is of significance for him.

The provisions of the first paragraph shall not apply if adequate measures have been taken in order to guard the privacy interests of the party in question, and the decision is based on the provisions of law or relates to the preparation or performance of a contract.

Section 28. Processing for marketing purposes etc ➦

The Statistical Bureau of Iceland shall maintain a registry of individvals not willing to allow the use of their names in product marketing. Controllers engaged in direct marketing, and those who process names, addresses, etc., or disseminate such data to third parties in connection with direct marketing shall, before such data is used for that purpose for the first time, and subsequently at one-monthly intervals, compare such files with the registry of the Statistical Bureau in order to prevent target mail being sent to people who is opposed to it and to prevent them being contacted by telephone. The Personal Data Protection Authority may make exemptions from this duty in special cases.

The name of the controller shall be prominently displayed on sent target mail, with information stating whom persons, unwilling to receive such mail and telephone calls, can turn to. Any person receiving target mail is entitled to know the origin of the information leading to the sending of mail or a telephone call. This does not, however, apply to a controller's marketing of his own products or services using his own customer registry, provided the identity of the sender is stated.

The provisions of the first and second paragraphs shall also apply, as applicable, to market surveys, consumer surveys and opinion polls as the Personal Data Protection Authority may provide for in further detail. The Authority may waive the requirements provided for in the first paragraph in relation to scientific and similar research, if such requirements are deemed likely to compromise to a significant extent the reliability of the outcome.

CHAPTER V. Transfer of personal data to foreign countries ➦

Section 29. Transfer of personal data to a state providing for adequate protection of such data ➦

Personal data may be transferred to another state, provided its laws ensures for an adequate level of protection for such data.

A state that implements Directive of the European Communities No. 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, shall be deemed to fulfil the condition set in the first paragraph.

When considering whether a state that does not implement Directive No. 95/46/EC fulfils the condition set in the first paragraph, the rules in effect in that state concerning the processing of personal data, the rules on good business practices and the security measures taken by the recipient shall be among the factors taken into account. Ratification by the state in question of the Council of Europe´s Convention No. 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, shall also be taken into consideration.

Section 30. Transfer of personal data to a state not providing for adequate protection of such data ➦

Transfer of personal data to a state not ensuring adequate protection for such data is prohibited, unless:

1. the data subject has provided his consent to the transfer;

2. this is necessary in order to comply with obligations under international law or by reason

of Iceland's membership of international organisations;

3. the transfer is allowed by other acts of law, or

4. delivery of the data is necessary in order to prepare or perform a contract between the data subject and the controller, or

5. the transfer is necessary in order to prepare or perform a contract for the benefit of the data subject, or

6. delivery of the data is necessary in order to protect important interests of the data subject.

The Personal Data Protection Authority may allow the transfer of data to a state referred to in the first paragraph if it deems that there are special reasons to do so, even if the conditions set in the paragraph are not fulfilled. In such cases the nature of the data, the planned purpose of the processing, and its duration, shall be among the factors taken into account. The Personal Data Protection Authority may issue further provisions on transfer of personal data to other countries.

CHAPTER VI. Duty of notification; licence requirements, etc ➦

Section 31. Duty of notification ➦

Any controller carrying out any wholly or partly automatic processing of personal data as allowed in Section 8 and the second paragraph of Section 9 shall, in a timely manner before it commences, notify the Personal Data Protection Authority of the processing on a form designed for the purpose. Notification shall also be made of any changes occurring from the original notification.

The duty of notification does not apply to processing of already collected data that is accessible to the public.

The Personal Data Protection Authority may decide that certain categories of processing shall be exempt from the duty of notification, or that simpler notification requirements shall apply to them. The Authority may furthermore decide that certain categories of processing shall be subject to prior checking and permits. The Authority may issue orders relating to processing that is exempt from notification requirements, which may include the matters referred to in the second paragraph of Section 35. The Authority may also order measures to be taken in order to minimise the inconvenience such processing of personal data may cause the data subject.

Section 32. The contents of notifications ➦

A notification to the Personal Data Protection Authority shall contain the following:

1. The name and address of the controller and, as the case may be, his representative as provided for in Section 6;

2. The identity of the person responsible for the daily fulfilment of the controller's duties;

3. The purpose of the processing;

4. A definition or other clarification of the kind of data to be processed;

5. Where the data has been obtained;

6. In what manner collection of the data is authorised;

7. To whom the data will be delivered;

8. Whether transfer of the data abroad is planned;

9. Whether publication of the data on the Internet is planned;

10. What security measures will be taken in the course of processing;

11. Whether, and when, the personal data or identifying data will be erased.

The Personal Data Protection Authority may issue provisions on the form and contents of notifications in further detail, and provide for the manner in which the duty of notification is to be complied with.

The controller shall at any particular time see to that the Personal Data Protection Authority possesses correct information on his processing of the data. When three years have passed since the Personal Data Protection Authority was sent a notification, the Authority shall be sent a new notification with updated information, unless changes in processing have already been notified. The Authority may order measures to be taken for securing the quality of notifications and the reliability of notified information, and decide on different notification periods depending on the category and nature of processing.

Section 33. Prior checking ➦

In cases of processing of general or sensitive personal data which may entail particular danger of infringement of the rights and freedoms of the data subjects, the Personal Data Protection Authority may suspend the commencement of the processing until the Authority has examined and approved the processing by the issue of a permit. The Authority may decide that permits shall no longer be required when general rules and security standards have been issued for processing of that kind.

Section 34. Prerequisites for the issue of permissions, etc ➦

A controller may only be issued a permit in accordance with Section 33, or any other permits provided for in this Act, if he is likely to be able to comply with his duties under this Act and the orders issued by the Personal Data Protection Authority.

When handling applications for a permission to process sensitive personal data the Authority shall, within the limits provided for in Chapter II of this Act, assess whether the processing may cause the data subject inconvenience that is impossible to relief by means of conditions set as provided for in Section 35. If such inconvenience can not be relieved, the Personal Data Protection Authority shall assess whether the interests recommending processing outweigh the interests of the data subject.

Section 35. Conditions defined in permissions for processing personal data

When a controller is granted a permit under Section 33, the Personal Data Protection Authority shall make this subject to any conditions the Authority deems necessary in each instance for preventing or diminishing any possible inconvenience resulting from the processing for the data subject. The same shall apply, as applicable, when the Personal Data Protection Authority receives a notification of the processing of sensitive personal data coming within the scope of the first paragraph of Section 9.

When assessing what conditions shall be set for processing, the factors to be considered by the Personal Data Protection Authority shall include:

1. Whether the data subject is certain to be able to exercise his rights under this Act, including by ceasing participation in a particular project, and, as applicable, have personal data deleted and receive information on his rights and his exercise of them;

2. Whether the personal data will be sufficiently safe and reliable, and updated as required by the purpose of processing, cf. Section 7;

3. Whether the personal data will be treated with the care demanded by the rules on secrecy and the purpose of processing;

4. Whether any decisions have been taken on the manner in which information and guidance will be provided to the data subject within the limits found reasonable with a view to the purpose of processing and other safety measures taken;

5. Whether safeguards have been established that are reasonable with a view to the purpose of the processing.

The Personal Data Protection Authority may decide that the controller and the processor, and any personnel working on their behalf, shall sign a declaration to the effect that they promise to keep secret any sensitive data coming to their knowledge in the course of processing. The controller or his representative shall attest to the correct signature and the date of the declaration, and forward it to the Personal Data protection Authority within the time limit to be stated. A violation of the duty of maintaining secrecy constitutes a criminal offence under Section 136 of the General Penal Code. The duty of maintaining secrecy shall survive the duration of employment.

The Personal Data Protection Authority may grant a petition relating to the processing of sensitive personal data on the condition that a supervisor is appointed to oversee, on behalf of the Authority, that the processing takes place in the manner required by law, and that the controller will pay all costs ensuing from this arrangement.

CHAPTER VII. Control and sanctions

Section 36. Organisation and administration of the Personal Data Protection Authority

The Personal Data Protection Authority shall be an independent authority with a board of its own, administratively subject to the Minister of Justice.

The Personal Data Protection Authority shall discharge its functions independently, and its decisions can not be referred to any superior administrative authority.

The Minister shall appoint five persons to the board of the Authority, and the same number of alternates, for a term of four years at a time. The Minister shall appoint the chairman and the vice-chairman without nomination. They shall be lawyers with the qualifications required for the office of district court judge. The Supreme Court of Iceland shall nominate one board member, and the Icelandic Society for Information Processing shall nominate another board member possessing expert knowledge of electronic data processing and technology. The alternate members shall have the same qualifications as the principal members.

The Minister shall decide on the remuneration of the board members.

When the board members do not agree, the matter in question shall be decided by majority vote. If votes are equal for and against, the vote of the chairman shall be decisive.

The Minister, having received the recommendations of the board, shall appoint a managing director for the Personal Data Protection Authority for a term of five years. The managing director shall attend meetings of the board, and shall have the right to speak and make proposals.

The managing director shall be in charge of daily management and shall engage other personnel for the authority.

The managing director shall be responsible for the financial and personnel management of the Authority. The board of the Authority shall in other respects decide on the distribution of responsibilities between the board and the Authority's personnel.

Section 37. The functions of the Personal Data Protection Authority ➦

The Personal Data Protection Authority shall control that this Act, and any administrative provisions issued in accordance with it, is duly complied with.

The Personal Data Protection Authority shall decide in cases of dispute concerning the processing of personal data. The Authority may consider individual cases on its own accord, or upon the reception of a communication from someone alleging that data has not been handled according to the requirements of this Act, any administrative provisions issued in accordance with it, or individual orders.

The tasks of the Personal Data Protection Authority include:

1. Deciding on applications for permits, receiving notifications, and ordering, as necessary, any measures relating to technology, safety and organisation of data processing in order to ensure that this takes place as required in this Act;

2. Controlling that laws and regulations on the processing of personal data are complied with, and that any shortcomings and mistakes are rectified;

3. Monitoring the general trends within the field of personal data protection domestically as well as abroad, and maintaining an overall view of, and providing information on, the chief issues in the field of personal data protection;

4. Defining and circumscribing where the protection of personal data is endangered and

providing counsel on possible solutions;

5. Providing guidance to parties planning to process personal data, or developing systems for such processing as regards protection of personal data, including by provision of assistance in the compilation of professional and ethical codes for individual groups and professions;

6. Providing statements, upon request or of its own initiative, on issues concerning the processing of personal data, and providing opinions on bills and proposed administrative provisions of significance for the protection of personal data;

7. Issuing an annual report on its activities.

The Personal Data Protection Authority may decide that a controller shall pay the cost ensuing from controlling that he fulfils the requirements of his Act, any administrative provisions issued in accordance with it, or individual orders. The Authority may also decide that a controller shall defray the costs of examining his procedures when the issue of a permit or other service is in preparation.

Section 38. Access of the Personal Data Protection Authority to information, etc ➦

The Personal Data Protection Authority may request from a controller, a processor and any party working on their behalf any information and written explanations necessary in order for it to perform its functions, including any information necessary in order to determine whether this Act applies to a certain operation or processing. The Authority may also summon a controller, a processor or any party working on their behalf to a meeting for provision of oral information and explanations concerning a certain processing of personal information.

When exercising its control functions, the Personal Data Protection Authority shall, without judicial warrant, have access to premises where personal data are being processed and where data are stored, including places where files, pictures, cf., Section 4, personal data in electronically accessible form, and equipment for accessing them, are kept. The Authority may perform any test or control measure it deems necessary, and can request the necessary assistance of personnel on the scene for performing a test or control measure. The Authority may request police assistance if an attempt is made to hinder the performance of its duties.

The right of the Personal Data Protection Authority to demand information and its right to access to premises and equipment can not be restricted by a reference to the duty of maintaining secrecy.

Section 39. Exemptions from the duty of maintaining secrecy ➦

The provisions on secrecy shall not prevent the Personal Data Protection Authority from providing information to similar foreign agencies when this is necessary in order to enable the domestic or foreign authority to decide on, or to perform, measures safeguarding privacy.

Section 40. Cessation of processing ➦

The Personal Data Protection Authority may order cessation of the processing of personal

data, including collection, registration and disclosure, order partial or total erasure of personal data or deletion of files, prohibit further use of personal data, or order the controller to take measures that ensure lawful processing. When assessing whether to take such measures, and what measures to take, the Authority shall take its decision with a view to all considerations including those enumerated in the second paragraph of Section 35.

In the case of processing of personal data in a manner that is contrary to this Act, or any administrative provisions issued in accordance with it, the personal Data Protection Authority may commit to the commissioner of police to stop the activity provisionally, and to close immediately the premises used for the purpose.

If someone does not comply with the orders of the Personal Data Protection Authority, the Authority may revoke any permits it may have issued under the provisions of this Act, until the Authority deems that the necessary improvements have been carried out.

Section 41. Daily penalties ➦

If an order of the Personal Data Protection Authority issued in accordance with the provisions of Sections 10, 25, 26 or 40 is not complied with, the Authority may impose daily penalties upon the addressee of the order, until the Authority deems that improvements have been made. Such penalties may amount to up to ISK 100,000 for each day that commences without the order having been complied with.

If a decision of the Personal Data Protection Authority on daily penalties is referred to the courts, daily penalties shall only begin to accrue when a final judgement has been rendered. The penalties shall convert to the State Treasury, and they may be collected by distress without prior judgement.

If an offence has been committed in the course of the operations of a legal person, the legal person may be fined as provided for in Chapter II A of the General Penal Code.

Section 42. Criminal sanctions ➦

Subject to other acts of law providing for heavier criminal sanctions, any person who commits a violation against this Act or any administrative provisions issued in accordance with it shall be fined or imprisoned for up to three years. The same sanctions shall be ordered if orders issued by the Personal Data Protection Authority have not been complied with.

Section 43. Compensation ➦

If a controller or a processor has processed personal data in a manner contrary to the provisions of this Act or the rules or orders of the Personal Data Protection Authority, the controller shall compensate the data subject for any loss he may have suffered in consequence. A controller shall however not be obliged to compensate for any loss he may establish was not caused by his own or the processor's negligence or mistake.

CHAPTER VIII. Connection to other laws, entry into force, etc ➦

Section 44. Connection to other laws ➦

This Act shall apply to processing and processing of personal data taking place subject to the provisions of other laws, unless a different arrangement is provided for there.

This Act shall not limit access to information as provided for in the Information Act and the Administrative Procedures Act.

Section 45. Administrative regulations on individual categories of activity ➦

Administrative regulations may be issued to govern the processing of personal data in certain fields of activity and with the members of individual professions.

The activity of processing data revealing financial matters, and the credit standing of enterprises and other legal persons, in the purpose of disseminating such data, shall be governed by an administrative regulation. For such activity the permission of the Personal Data Protection Authority shall be required, and the following provisions of this Act shall apply to it: Section 11 on the security and quality of information; Section 12 on internal control, Section 13 on a processor's processing; Section 18 on the right of the data subject to information; Section 21 on the duty to provide a warning when data are being collected from others than the data subject; Section 25 on correction and deletion of incorrect and incomplete data; Section 26 on deletion and prohibition of use of data that are neither incorrect nor incomplete ; Section 33 on processing for which permits are required; Section 34 on the conditions for the issue of permits; Section 35 on conditions to be laid down; Section 38 on the Personal Data Protection Authority's access to information, etc.; Section 40 on cessation of processing, etc., Section 41 on daily penalties, Section 42 on criminal sanctions, and Section 43 on compensation.

The Minister shall, having received the opinion of the Personal Data Protection Authority, issue a regulation providing in further detail for the Authority's control of automated processing of personal data by the police. This shall include provisions on the duty of the police to notify the Personal Data Protection Authority of any automated processing by the police, and the contents of such notifications. There shall furthermore be provisions regulating when and how a data subject shall have a right to access personal data relating to him that is or has been processed by the police, and the right of the police to delay the disclose of data in certain situations. There shall finally be provisions on the security of personal data and the police's duty to carry out internal control to secure that personal data is processed as required by law. There shall also be provisions on the period of time during which personal data shall be stored.

A regulation shall also be issued to provide in further detail on activities involving the use of name lists and the preparation of name inscriptions, including in marketing and in the preparation of market surveys and opinion polls.

Section 46. Entry into force ➦

This Act shall enter into force 1 January 2000. At the same time Act No. 121/1989, on Registration and Processing of Personal Data, shall be repealed.

At the time of entry into force, the following amendments of the following acts of law shall also enter into force:

1. The words "Act on Registration and Processing of Personal Data, No. 121/1989" in the

final sentence of Section 20 of the Child Welfare Act, No. 58/1992, shall be replaced by the words "Act on Protection of Private Information and Processing of Personal Data".

2. The words "Data Protection Committee, cf. Act No. 121/1989 on Registration and Processing of Personal Data" in the fourth paragraph of Section 24 of the Pharmaceuticals Act, No. 93/1994, shall be replaced by the words "Personal Data Protection Authority, cf. Act on Protection of Private Information and Processing of Personal Data".

3. The words "Data Protection Committee" in the third paragraph of Section 15 of the Rights of Patients Act, No. 74/1997, shall be replaced by the words "Personal Data Protection Authority".

4. The words "Data Protection Committee" in the second paragraph of Section 14 of the Act on Electronic Ownership Registration of Securities, No. 131/1997, shall be replaced by the words "Personal Data Protection Authority".

5. The words "Data Protection Committee" in Section 4 of the Act on a Database in the Health Sector, No. 139/1998, and the same words in Sections 5, 6, 7, 10, 12 and 17, shall be replaced by the words "Personal Data Protection Authority".

6. The words "Data Protection Committee" in Sections 18 and 19 in the Act on the Schengen Information System in Iceland, No. 16/2000, shall be replaced by the words "Personal Data Protection Authority".

Temporary provision

When this Act has been published, the Minister shall immediately appoint the members of the board of the Personal Data Protection Authority and advertise the office of the Authority's Director vacant. When the Director has been engaged he shall, as necessary, engage other personnel to prepare the entry into effect of this Act and to exercise administrative functions as provided for in the second paragraph.

Notwithstanding the provisions of the first paragraph of Section 46, the Personal Data Protection Authority shall, immediately when its board has been appointed, assume control of that personal data are, in the Schengen Information System in Iceland, handled as required by Act No. 16/2000 on the Shengen Information System.

Any controller who makes use of electronic technology for processing personal data at the time this Act enters into force shall notify the Personal Data Protection Authority of his processing on a form made for the purpose, as required in Sections 31 and 32, within six months from when the Act enters into force.

Permits issued by the Data Protection Committee shall retain their validity, provided they do not conflict with the provisions of this Act.