The Data Protection Act
Act on the Protection of Privacy as regards the 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. (Act. No. 77/2000 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). **Contents** CHAPTER I. Objective, definitions and scope. Article 1. Objective. Article 2. Definitions. Article 3. Scope. Article 4. Electronic surveillance. Article 5. Connections with freedom of expression. Article 6. Geographical application. CHAPTER II. General rules on processing of personal data. Article 7. Main principles relating to data quality and processing. Article 8. General rules regarding permission for processing of personal data. Article 9. Special conditions governing the processing of sensitive personal data. Article 10. The usage of the national identification number. Article 11. Risk assessment, security and integrity of personal data. Article 12. Internal audit. Article 13. The processor's obligation of confidentiality when processing personal data. Article 14. Time limits for fulfilling requirements. Article 15. Payment of costs CHAPTER III. Right of access and duty to provide information. Duty to provide guidance and warning. Right to reasoning. Article 16. The right to access general information on personal data processing. Article 17. Public register of permits given and notifications received. Article 18. The data subject's right of access. Article 19. Restrictions of the data subject's right of access. Article 20. Duty to inform in case of collection of personal data from the data subject. Article 21. Duty to inform the data subject about a processing of personal data when they are obtained from Article 22. Reasoning for individual decisions that are based on automated data processing. Article 23. Warnings concerning use of personal profiles Article 24. Warnings regarding electronic surveillance CHAPTER IV. Rectification, erasure, blocking, etc. Article 25. Rectification and deletion of incorrect and misleading personal data. Article 26. Erasure, and prohibition of use, of personal data that are neither incorrect nor misleading. Article 27. The right to a decision based on manual processing of data. Article 28. The data subject's right to object and the Statistical Bureau of Iceland's restricted registry. CHAPTER V. Transfer of personal data abroad. Article 29. Transfer of personal data to a country that provides an adequate level of personal data protection. Article 30. Transfer of personal data to a country that does not provide an adequate level of personal data protection. CHAPTER VI. Obligation to notify, permit requirements, etc. Article 31. Obligation to notify. Article 32. Contents of notification. Article 33. Processing which requires a permit. Article 34. Prerequisites for the issue of permits, etc. Article 35. Conditions set by the Data Protection Authority regarding the processing of personal data. CHAPTER VII. Monitoring and sanctions. Article 36. Organisation and administration of the Data Protection Authority. Article 37. The task of the Data Protection Authority. Article 38. The Data Protection Authority's access to information, etc. Article 39. Exceptions from obligations of secrecy. Article 40. Cessation of processing. Article 41. Daily fines. Article 42. Sanctions. Article 43. Remedies. CHAPTER VIII. Correlation with other acts of law, entry into force, etc. Article 44. Correlation with other acts of law. Article 45. Regulations regarding individual categories of activity. Article 46. Entry into force.

::::::::::::::::::::::::::::::::::

Act
on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 (with amendments)

CHAPTER I.
Objective, definitions and scope.
Article 1. *Objective.*
The objective of this Act is to promote the practice of personal data processing in accordance with fundamental principles and rules regarding data protection and privacy, and to ensure the reliability and integrity of such data and their free flow within the internal market of the European Economic Area. A specific institution, the Data Protection Authority, is responsible for monitoring the application of this Act and those administrative rules that are based on it, cf. further Article 36.

Article 2.
Definitions.
For the purpose of this Act, words and terms shall have the following meaning: 1. Personal data: Any data relating to the data subject (identified or identifiable), i.e. information that

can be traced directly or indirectly to a specific individual, deceased or living. 2. Processing: Any operation or set of operations, which is performed upon personal data, whether the processing is manual or automatic. 3. File: Any structured set of personal data where data on individual persons can be found. 4. Controller: The party that determines the purposes of the processing of personal data, the equipment that is used, the method of the processing and other usage of the data. 5. Processor: The party that processes 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 number of people normally traverses. The concept entails:
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. 1)
7. Consent: A specific, unambiguous declaration, which is given freely by an individual, signifying that he agrees to the processing of particular personal data relating to him, and that he is aware of the purpose of the processing, how it will be conducted, how data protection will be ensured, that the individual can withdraw his consent, etc. 8. Sensitive data: a. Data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies. b. Data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence. c. Health data, including genetic data and data on use of alcohol, medical drugs and narcotics. d. Data concerning sex life (and sexual behaviour). e. Data on trade-union membership. 9. Automated individual decision: A decision that defines legal rights and/or duties concerning one or more particular individuals. 1) Act No. 46/2003, Art. 1.

Article 3.
Scope.
The Act applies to any electronic processing of personal data. The Act also applies to manual processing of personal data that form, or are intended to form, a part of a filing system. Articles 16, 18–21, 24, 26, 31 and 32 of the Act do not apply to processing of personal data that concern public security, national defence, State security and the activities of the State in areas of criminal law. The Act does not apply to the processing, by an individual, of personal data that only relates to the individual himself or is purely intended for personal use.

Article 4.
Electronic surveillance.
Electronic surveillance must always be conducted for legitimate purposes. Electronic surveillance of premises where a limited number 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: Art. 7., 24., 40. and 41. gr., and, where applicable, Art. 31, 32 and 38. 1) 1) Act. No. 46/2003, Art. 2.

Article 5.
Connections with freedom of expression.
To the extent that it is necessary to reconcile the right to privacy on the one hand with the freedom of expression on the other, derogations can be made from provisions in the Act in the interest of journalism, art or literature. When personal data are solely processed in the interest of news coverage or a literary or artistic activity, only the provisions of Article 4, Article 7 (1) and (4), Articles 11 through 13 and Articles 24, 28, 42 and 43 shall apply.

Article 6.
Geographical application.
[The Act applies to the processing of personal data that is conducted on behalf of a controller who is established in Iceland, if the processing of the personal data is carried out in the European Economic Area, [in a country listed as a member in the Convention establishing the European Free Trade Association]1)or in a country or a place that the Data Protection Authority lists in an advertisement in the Law and Ministerial Gazette. The Act also applies to processing of personal data despite the controller being established in a country that is outside the European Economic Area or in a country listed as a member in the Convention establishing the European Free Trade Association 1), if he makes use of equipment and facilities situated in Iceland. The Act also applies to the processing of financial and credit standing data concerning legal persons, cf. Article 45, even if the controller is not established in Iceland, if he makes use of equipment and facilities situated in Iceland. Paragraphs 2 and 3 of this Article do not apply if the equipment in question is only used to transport personal data through the

territory of Iceland. In the circumstances referred to in Paragraphs 2 and 3, the controller must designate a representative established in Iceland, and the provisions of the Act relating to controllers shall then apply to that representative as fitting.]2) 1) Act No. 72/2003, Art. 5. 2) Act No. 90/2001, Art. 1.

CHAPTER II.
General rules on processing of personal data.

Article 7.
[Main principles relating to data quality and processing.]1)
When processing personal data, all of the following shall be observed: 1. that they are processed in a fair, apposite and lawful manner and that all their use is in accordance with good practices of personal data processing; 2. that they are obtained for specified, explicit, apposite purposes and not processed further for other and incompatible purposes, but further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that proper safeguards are adhered to; 3. that they are adequate, relevant and not excessive in relation to the purposes for the processing; 4. that they are reliable and kept up to date when necessary, personal data which are unreliable or incomplete, having regard to the purposes for their processing, shall be erased or rectified; 5. that they are preserved in a form which does not permit identification of data subjects for longer than is necessary for the purposes for the processing. [It shall be for the controller to ensure that the processing of personal data is always in compliance with Paragraph 1.]1) 1) Act No. 90/2001, Art. 1.

Article 8.
[General rules regarding permission for processing of personal data.]1)
Personal data may only be processed if one of the following criteria is met: 1. [the data subject has unambiguously agreed to the processing or given his consent, as it is defined in Article 2 (7)]1) 2. the processing is necessary to honour a contract, to which the data subject is a party, or to take measures at the request of the data subject before a contract is established; 3. the processing is necessary to fulfil a legal obligation of the controller; 4. the processing is necessary to protect vital interests of the data subject; 5. the processing is necessary for a task that is carried out in the public interest; 6. the processing is necessary in the exercise of official authority vested in the controller or in a third party to whom data are transferred; 7. the processing is necessary for the controller, or a third party, or parties to whom data are transferred, to be able to safeguard legitimate interests, except where overridden by fundamental rights and freedom of the data subject, which shall be protected by law.2) [The Data Protection Authority can authorize processing of personal data in other instances than those that are detailed in Paragraph 1, if it is apparently in the vital interests of the public or individuals, including the interests of the data subject. In that case, the need for the processing shall clearly outweigh the consideration for it not to take place. The Data Protection Authority can set conditions for the processing, as it deems necessary in each case, to protect the interests of the data subject.]1) 1) Act No. 90/2001, Art. 3. 2) Act No. 46/2003, Art. 3.

Article 9.
[Special conditions governing the processing of sensitive personal data.]1)
[Processing of sensitive personal data is prohibited, unless at least one of the conditions in Article 8, Paragraph 1, has been met, and one or more of the following requirements has also been fulfilled:] 1. the data subject gives his consent to the processing; 2. the processing is specifically authorized in another Act of law; 3. the controller is required, by contracts between the Social Partners, to carry out the processing; 4. the processing is necessary to protect vital interests of the data subject or of another party who is incapable of giving his consent in accordance with (1); 5. the processing is carried out by an organization with a trade-union aim or by other non-profit organizations, such as cultural, humanitarian, social or ideological organizations, on condition that the processing is carried out in the course of the organization's legitimate activities and relates solely to the members of the body or to individuals who according to the organization's goals are, or have been, in regular contact with it; it is however prohibited to disclose such personal data to a third party without the data subject's consent. 6. the processing extends only to information that the data subject himself has made public; 7. the processing is necessary for a claim to be established, exercised or defended because of litigation or other such legal needs. 8. the processing is necessary because of a medical treatment or because of the routine management of health care services, provided that it is carried out by an employee of the health care services who is subject to an obligation of secrecy. 9. the processing is

necessary for the purposes of statistical or scientific research, provided that the privacy of individuals is protected by means of specific and adequate safeguards. [Material, such as audio and visual material, that is produced by means of electronic surveillance and includes sensitive personal data, may be collected even though the requirements of Paragraph 1 are not fulfilled, if the following conditions are met: 1. the surveillance is necessary and is conducted for the purposes of security and property protection. 2. the material produced by the surveillance may not be handed over to anyone else or processed further except with the consent of the subject of the recording, or in accordance with a decision by the Data Protection Authority; however, material that contains data on accidents or a punishable legal offence may be turned over to the police, but in that case care should be given to deleting all other copies of the material; 3. the material, that is collected in conjunction with the surveillance, shall be deleted when there is no longer an apposite reason to preserve it, unless a special permit by the Data Protection Authority, under Paragraph 3, provides for further preservation.]2) The Data Protection Authority can permit the processing of sensitive personal data in other instances than those articulated in [Paragraphs 1 and 2] if it considers that to be of urgent public interest. The Authority issues such permits on any conditions that it deems necessary in each case in order to protect the interests of the data subjects. The Data Protection Authority, having received the opinion of the Science Ethics Committee, issues rules on how individuals may be selected and approached for their participation in scientific research, and on what information shall be given to them before they are asked to give their consent. The Data Protection Authority rules on whether particular personal data shall be considered to be sensitive or not. 1) Act No. 90/2001, Art. 4. 2) Act No. 81/2002, Art. 1.

Article 10.
The usage of the national identification number.
The national identification number may be used if it is done for apposite purposes and it is necessary to ensure a correct identification of a person. The Authority can prohibit or order that the national identification number be used.

Article 11.
[Risk analysis, security and integrity of personal data.
The controller shall implement appropriate technical and organizational measures to protect personal data against unlawful destruction, against accidental loss or alteration and against unauthorized access. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. The controller is responsible for having risk analysis and security measures, that are implemented in the processing of personal data, conform with laws, rules 1) and instructions given by the Data Protection Authority on how to ensure information security, including standards that the Authority decides that shall be followed. The controller is responsible for risk analysis being reviewed routinely and security measures upgraded to the extent necessary to fulfil the requirements of this article. The controller shall document how he produces a security policy, conducts a risk analysis and decides on security measures to be implemented. The Data Protection Authority shall be granted access to information regarding these issues at any time.]2) 1) Rules No. 299/2001. 2) Act No. 90/2001, Art. 5.

Article 12.
Internal audit.
[The controller shall conduct internal audits on the processing of personal information to ensure that they are processed in accordance with prevailing laws and regulations and the security measures that are to be implemented. Internal audits shall be conducted routinely. The frequency and intensity of the audits shall be relative to danger associated with the processing, the nature of the data processed, the technology used to ensure the security of the data and the cost associated with conducting the audits. They shall none the less be conducted at least annually. The controller shall see to it that a report is written on each of the measures that the internal audit is comprised of. In such a report, the results of each part of the audit shall be described. Internal audit reports shall be preserved in a secure manner. The Data Protection Authority has the right to review these reports at any time. The Data Protection Authority may provide further instructions 1) on how to conduct internal audits, and give exemptions from the obligation to conduct such audits, or limit what parts of the processing shall be audited.]2) 1) Rules No. 299/2001 2) Act No. 90/2001, Art. 6.

Article 13.
[The processor's obligation of confidentiality when processing personal data.

A controller is permitted to contract a third party to take care of the processing, in whole or in part, which the controller is responsible for according to this Act. This is contingent upon the controller having beforehand verified that the processor in question is able to carry out the required security measures and conduct internal audits in accordance with Article 12 of this Act. A contract entered into under Paragraph 1 shall be in writing and at least in duplicate. The contract must in particular stipulate that the processor shall act only on instructions from the controller and that the obligations set out in this Act shall also be incumbent on data processing carried out by the processor. The data processor and data controller shall each keep a copy of the contract. Anyone who acts in the name of the controller or the processor, including the processor himself, and has access to personal data, may only process personal data according to the instructions of the controller, unless legislative acts stipulate otherwise. If the processor is established in another state within the European Economic Area than the controller, cf. Article 6, Paragraph 1, then it shall also be stipulated in a contract that the laws and regulations of the state in which the processor is established shall govern the security measures to be applied to the processing of personal data. The Data Protection Authority may require, e.g. in an advertisement in the Law and Ministerial Gazette, that such a contract shall contain certain standard contractual clauses, in accordance with a decision made by the European Union Commission. The same applies when the controller is established in a state within the European Economic Area but the processor is not, if the processing takes place in a country or at a physical place that is listed in an advertisement published by the Data Protection Authority.]1) [The provisions of Paragraph 4 also apply if the data processor is established in another member state to the Convention establishing the European Free Trade Association than the data controller, cf. Art. 6, Paragraph 1, or and if the data controller is established in a member country to the Convention establishing the European Free Trade Association and the processor is not.]2) 1) Act No. 90/2001, Art. 6. 2) Act No. 72/2003, Art. 6.

Article 14.
Time limits for fulfilling requirements.
The controller shall process any request under Articles 16, 18, 22, 25, 26, 27 or 28 as soon as possible and no later than one month after receiving it. If extraordinary circumstances make it impossible for the controller to process a request within a month, he may do so at a later date. In that case, the controller shall, within the one-month time limit, provide the person in question with a written explanation of the reasons for the delay, and information on when a reply is to be expected.

Article 15.
Payment of costs.
Any request under Articles 16, 18, 22, 25, 26, 27 or 28 shall be processed free of charge. However, if high costs are involved, e.g. due to photocopying of documents, payment may be collected in accordance with a list of tariffs, according to a regulation issued by the Minister of Justice.

CHAPTER III.

Right of access and duty to provide information. Duty to provide guidance and warning. Right to reasoning.

Article 16.
The right to access general information on personal data processing.
The controller shall give general information, on any personal data processing conducted on his behalf, to any person that requests such information. Any person who so requests shall also, as far as a particular kind of processing is concerned, be supplied with information on the following: 1. the name and address of the controller and, where relevant, his representative according to Article 6; 2. who bears the day-to-day responsibility of the controller's duties, under this Act, being fulfilled; 3. the purpose of the processing; 4. a definition and other characterization of the categories of personal data being processed; 5. where the data have been obtained; 6. the recipients of the data, including whether the data are intended to be exported and if so, to whom. A request under Paragraph 1 shall be directed to the controller, or his representative according to Article 6, and a written explanation may be demanded regarding the issues on which information is requested.

Article 17.
Public register of given permits and received notifications
The Data Protection Authority shall maintain a register of all the processing that it has been notified of in accordance with Article 31 and the processing that it permits in accordance with Article 33. The register shall at least include the items found in Paragraph 2 of Article 16. The

register shall be accessible to the public by a method determined by the Data Protection Authority.

Article 18.
The data subject's right of access.
The data subject has a right to information from the controller on the following: 1. what data on him are being or have been processed: 2. the purpose of the processing; 3. who receives, has received or will receive data on him; 4. where the data have been obtained; 5. what security measures are applied to the processing, provided that this will not diminish the security of the processing; A request for access under Paragraph 1 shall be directed to the controller, or his representative according to Article 6. The information shall be provided in writing, if requested.

Article 19.
Restrictions of the data subject's right of access.
The data subject's right of access under Article 18 does not extend to data which are used solely for statistical processing or scientific research, provided that their processing can not have direct influence on his interests. The provisions of Article 18 do not apply where the rights of the data subject, under that clause, are deemed secondary, in part or wholly, to the interests of others or of his own. In such cases, the considerations to be taken into account include the data subject's health and the interests of his family members. However, the information may be disclosed to a representative of the data subject there being no special arguments to the contrary. The right of the data subject to access, under article 18, does not extend to data that are exempted from access under the Access to Information Act or the Administrative Procedures Act. When the data medium is in the possession of other processors than public authorities, the provisions of Article 18 do not extend to knowledge of the contents of preliminary documents or other comparable medium prepared by the controller himself or on his behalf, e.g. by specialized consultants or experts. Even if data media are exempted from the data subject's right of access under Paragraph 3, he may still request an explanation of their material contents, an excerpt or other forms of description, unless he is able to acquaint himself with the facts of the matter by other means. If the disclosure of information on certain data decreases the potential for concluding a case that is pending, the disclosure may be postponed until the matter has been prepared for resolution. The Data Protection Authority may issue rules, which are confirmed by the Minister, containing conditions for the exercise of the data subject's right of access.

Article 20.
[Duty to inform in case of collection of personal data from the data subject.
When a controller obtains personal data from the data subject, the controller must provide the following information to the data subject: 1. the name and address of the controller and, where relevant, his representative according to Article 6, 2. the purposes of the processing, 3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to enable the data subject to protect his interests, including information on: a. the recipients or categories of recipients of the data, b. whether he is obliged or not to provide the requested data, as well as the possible consequences of failure to reply, c. the provisions of the Act regarding the data subject's right of access, as well as the data subject's right to rectification and deletion of wrong or misleading data on him. The provisions of Paragraph 1 do not apply if the data subject has already received information on the items listed in Paragraph 1 (1) through (3).] 1) Act No. 81/2002, Art. 2.

Article 21.
[Duty to inform the data subject about the processing of personal data when they are obtained from someone else than the data subject himself.
When a controller collects personal data from someone other than the data subject, the controller shall concurrently inform the data subject about the collection and of the items listed in Paragraph 3. If, however, the intent of the controller is to disclose the data to a third party within a moderate time period from their collection, then he may postpone that until he discloses the data for the first time. In spite of the second sentence of Paragraph 1, a controller who discloses financial and credit standing data shall notify the data subject 14 days before such data is disclosed for the first time. A notice to the data subject shall contain information on the following: 1. the name and address of the controller and, where relevant, his representative according to Article 6, 2. the purposes of the processing, 3. other information, in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed,

to enable the data subject to protect his interests, including information on: a. the types or categories of the data being processed, b. where the data come from; c. the recipients or categories of recipients of the data, d. the provisions of the Act regarding the data subject's right of access, as well as the data subject's right to rectification and deletion of wrong or misleading data on him. The provisions of Paragraph 1 do not apply if: 1. it is impossible to inform the data subject or if it would place a heavier burden upon the controller than can reasonably be demanded, 2. it may be assumed that the data subject is already aware of the processing, 3. recording or disclosure of the data is laid down by law or 4. the data subject's interests, of receiving notice of the data, are deemed secondary to vital public or private interests, including his own interests.] 1) Act No. 81/2002, Art. 3.

Article 22.
Reasoning for individual decisions that are based on automated data processing.
If an individual decision, which is solely based on automated processing of personal data, has been made, then the person to whom the decision relates may demand reasoning for the conclusion. In the reasoning, the controller shall articulate the principles, on which the electronic processing is based, and which make up the foundations for the decision.

Article 23.
Warnings concerning use of personal profiles.
When a personal profile defining certain behaviour, taste, ability or need is used as a basis 1. of an individual decision as defined in Article 2 (9) or 2. for approaching the data subject, selecting a sample or a target group, etc., the Data Protection Authority can, when it has received a notification of such processing, decide that the controller shall notify the data subject and inform him who the controller of the processing is, what data he is using and where that data is obtained. When making a decision in accordance with Paragraph 1, the Data Protection Authority shall, among other things, consider whether it is impossible to give warning or if it would place a heavier burden upon the controller than can reasonably be demanded.

Article 24.
Warnings regarding electronic surveillance.
When electronic surveillance is conducted at a place of work or in public, a clear warning shall be given of that fact by a sign or in another noticeable way, stating also who the controller is.

CHAPTER IV.
Rectification, erasure, deletion, blocking, etc.

Article 25.
Rectification and deletion of incorrect and misleading personal data.
If incorrect, misleading or incomplete personal data have been registered, or if personal data have been registered without a proper authorization, then the controller shall see to it that the data be rectified, erased, deleted or improved upon, if the defect in question is liable to affect the interests of the data subject. If such data have been disclosed or used, then the controller shall, to the extent that he is possibly able to, prevent it from affecting the interests of the data subject. If erasure, deletion or alteration, of the data referred to in Paragraph 1, is not allowed according to provisions of other acts, then the Data Protection Authority may prohibit the use of the data.

Article 26.
Erasure, and prohibition of use, of personal data that are neither incorrect nor misleading.
When there is no longer an apposite reason to preserve personal data, the controller shall erase them. An apposite reason for preserving data may i.a. stem from a provision of law or from the fact that the controller is still processing the data in conformity with the original purpose of their collection. If provisions of other acts do not preclude it, the data subject may still demand that data relating to him, under Paragraph 1, be erased or their usage prohibited, if that is considered justifiable, following a comprehensive assessment of the interests involved. In making such an assessment, the interests of others, general considerations of privacy, public interests, and the measures necessary for complying with the demand, shall be taken into account. The Data Protection Authority may, in individual cases or by issuing a general ordinance, prohibit the use of such data or order that they be erased.

Article 27.
The right to a decision based on manual processing of data.
If an automated individual decision, according to Article 2 (9), has been made and it is solely based on an automated processing of personal data, the individual to whom the decision relates, or is directly affected by the matter, may insist that the decision is made via manual means, provided that the decision in question

concerns his personal situation or attributes and is of significant importance to him. The right outlined in Paragraph 1, does not exist in situations where appropriate measures are applied in order to protect the privacy interests of the individual in question and the relevant decision is based on a legal provision or relates to the construction or honouring of a contract.

Article 28.
The data subject's right to object.
The Statistical Bureau of Iceland's registry of restrictions.
The data subject may object, on compelling legitimate grounds relating to his particular situation, to the processing of personal data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data. The Statistical Bureau of Iceland shall maintain a registry of those individuals who object to their names being used for marketing purposes. The Statistical Bureau shall issue an ordinance dictating the assembly and usage of such registries and what information shall be registered there, in cooperation with the Data Protection Authority. Controllers engaged in direct marketing, and those who use a list of names, addresses, e-mail addresses, phone numbers and similar data, or disclose them to a third party in connection with a similar enterprise, shall, prior to using such a list for the described purposes, compare it with the Statistical Bureau's registry, in order to prevent direct mail from being sent to, or phone calls being made to, those who have objected to it. The Data Protection Authority can make exemptions from this duty in special cases. All use of the restricted registry in Paragraph 2, for other purposes than those articulated there, is forbidden. The controller's name shall be prominently displayed on sent target mail, with information on where those who object to receiving such target mail and phone calls can turn to. The recipient of target mail is entitled to know the origin of the data that is the basis for the mailing or phone call. This does not apply to the controller's marketing of his own products and services using his own customer list, provided that that it is stated, on the material which is sent out, where it is sent from. [If target mail is sent by electronic means, it shall be made clear as soon as it is received that it is of target mail nature.]1) The controller may disclose registries of a fellowship's members, of employees or of customers for use in direct marketing, provided that: 1. the disclosure does not include any sensitive personal data, 2. each of the data subjects has, before the disclosure, been given an opportunity to object to data relating to him appearing on the disclosed registry, 3. it is not in violation of the rules or codes of the association in question, 4. the controller examines if any of the data subjects has registered their objection with the Statistical Bureau, cf. Paragraph 2, and erases data relating to the individual in question, before disclosing the registry. The provisions of Paragraph 5 do not apply if the disclosure of a registry of a fellowship's members, of employees or of customers, for the purpose of distributing target mail, is based on the consent of the data subject, cf. Article 8, Paragraph 1 (1). The provisions of Paragraphs 1 through 5 apply, where appropriate, also to market surveys, consumption surveys and opinion polls. The Data Protection Authority may exempt scientific research and comparable research from such restrictions, provided that it is considered obvious that they could seriously compromise the reliability of the outcome of the research.]2) 1) Act No. 30/2002, Art. 23. 2) Act No. 90/2001, Art. 8.

CHAPTER V.
Transfer of personal data abroad.

Article 29.
Transfer of personal data to a country that provides an adequate level of personal data protection.
The transfer of personal data to another country is permitted if the laws of that country provide an adequate level of personal data protection. A country which complies with the European Union Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is considered having fulfilled the requirements of Paragraph 1. [The same applies to those countries or places which the Data Protection Authority lists in an advertisement in the Law and Ministerial Gazette, having considered the decisions of the Commission of the European Union.]1) When considering whether a country, which does not comply with Directive 95/46/EC, fulfils the requirements of Paragraph 1, that country's rules on the processing of personal data and on good business practices, and the security measures taken by the recipient, shall be among the factors taken into account. Ratification by the respective country of the Council of Europe 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. 1) Act No. 90/2001, Art. 9.

Article 30.
Transfer of personal data to a country that does not provide an adequate level of personal data protection.
The transfer of personal data to a country that does not provide an adequate level of personal data protection is prohibited, unless: 1. the data subject has consented to the transfer, or 2. it is necessary for the fulfilment of obligations under international law or as a result of Iceland's membership of an international organization, or 3. such a transfer is authorized in another legislative act, or 4. the delivery is necessary to establish or fulfil a contract between the data subject and the controller, or 5. the transfer is necessary to establish or fulfil a contract in the interest of the data subject, or 6. the delivery is necessary in order to protect vital interests of the data subject, or [7. if dissemination is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims or 8. the data in question are accessible to the general public. The Data Protection Authority can authorize the transfer of data to a country referred to in Paragraph 1, if it determines that special circumstances warrant it, even if the conditions of the provision are not met. In such cases the nature of the data, the planned purpose of the processing and its duration are among the factors that shall be taken into account. [The Data Protection Authority can authorize the transfer of data to third countries even if they have not been thought of as providing the citizens with an adequate level of privacy protection. This is contingent upon the controller having, in the opinion of the Authority, provided sufficient guarantees to meet these concerns. The Authority can for example require that the controller enter into a written contract with the recipient and that the contract contains certain standard contractual clauses in conformance with a decision which the Data Protection Authority has advertised in the Law and Ministerial Gazette, having considered the decisions of the Commission of the European Union, cf. Article 29, Paragraph 2 of this Act. The Data Protection Authority may issue further instructions regarding the transfer of personal data abroad.]1). 1) Act No. 90/2001, Art. 10.

CHAPTER VI.
Obligation to notify, permit requirements, etc.

Article 31.
Obligation to notify.
Each controller, who uses electronic technology to process personal data, cf. Article 8 and Article 9, shall notify the Data Protection Authority of the processing, using a form intended for that purpose, in a timely manner before beginning the processing. Any changes that are made from the original notification shall also be notified. The obligation to notify does not apply if the processing extends only to data that have been and are accessible to the public. The Data Protection Authority may decide 1) that certain categories of processing of general information shall be exempt from notification, or that they shall be subject to simpler notification requirements. The Data Protection Authority can also decide 1) that certain categories of processing shall require a permit. The Data Protection Authority can issue instructions regarding processing which is exempt from notification, and these may, among other things, include the factors referred to in Article 35, Paragraph 2. The Data Protection Authority can also dictate measures to be taken in order to reduce the inconvenience that the data subject may suffer as a result from this type of personal data processing. 1) Rules No. 90/2001, cf. No. 170/2001.

Article 32.
Contents of notification.
A notification to the Data Protection Authority, according to Article 31, shall contain the following information: 1. the name and address of the controller and, where relevant, his representative according to Article 6; 2. who bears the day-to-day responsibility of fulfilling the controller's duties 3. the purpose of the processing; 4. a definition and other characterization of the categories of data that will be used for the processing; 5. where the data are obtained; 6. what sanctions the processing is based on; 7. to whom the data will be disclosed; 8. whether export of the personal data is planned; 9. whether publication of the personal data on the Internet is planned; 10. what security measures will be implemented in the processing; 11. whether and when personal data or personal identifiers will be deleted; [12. how the conditions of Articles 20 and 21 are fulfilled.]1) The Data Protection Authority can issue further instructions 2) regarding the form and contents of notifications and on other aspects of the obligation to notify. The controller shall see to it that the Data Protection Authority has always up-to-date information regarding the processing. When three years have passed since a notification was sent to the Data Protection Authority, a new notification,

containing updated information, shall be sent to the Authority, unless changes in the processing have already been notified. The Data Protection Authority can dictate measures to be taken, in order to ensure the quality and dependability of notifications, and decide on different notification time limits depending on the category and nature of the processing. 1) Act No. 81/2002, Art. 4. 2) Rules No. 90/2001.

Article 33.
Processing which requires a permit.
If certain processing of general or sensitive personal data is likely to present specific risks to the rights and freedoms of data subjects, then the Data Protection Authority can decide 1) that the processing may not begin until it has been examined by the Authority and approved of, by the issuing of a special permit. The Data Protection Authority can decide 2) that such permits will no longer be required when general rules and security standards, to be observed in this kind of processing, have been issued. 1) Rules No. 90/2001, cf. No. 170/2001. 2) Rules No. 170/2001, cf. 157/2003.

Article 34.
Prerequisites for the issue of permits, etc.
A controller may only be issued a permit in accordance with Article 33, or other provisions of this Act, if it is likely that he can fulfil his duties according to the Act, or the instructions of the Data Protection Authority. The Data Protection Authority shall, when handling cases which concern the processing of sensitive personal data, determine, within the limits set in Chapter II of the Act, whether the processing is liable to cause the data subject so much inconvenience that it can not be redressed by way of conditions set in accordance with Article 35. If such inconvenience can occur, then the Data Protection Authority shall determine if interests recommending the processing outweigh the interests of the data subject.

Article 35.
Conditions set by the Data Protection Authority r egarding the processing of personal data.
When a controller is granted a permit in accordance with Article 33, the Data Protection Authority shall set conditions, e.g. the encryption of personal identities and other conditions which the Authority deems essential in each case, in order to reduce or prevent the data subject's potential inconvenience resulting from the processing. The same applies, where relevant, when the Data Protection Authority receives a notification about the processing of sensitive personal data that falls under Article 9, Paragraph 1. When deciding on what conditions to set, the Data Protection Authority shall among other factors consider the following: 1. whether the data subject is guaranteed the exercise of his rights under the Act, including the right to discontinue his participation in a project, and, where applicable, to have registered personal data erased, and to receive information on his rights and their application; 2. whether personal data will be adequately secure, reliable and updated according to the purpose of the processing, cf. Article 7; 3. whether personal data will be handled with the care dictated by rules regarding obligations of secrecy and by the purpose of the processing; 4. whether it has been planned, how the data subject will be provided with information and instructions, within the boundaries of what is reasonable to expect, having regard to the extent of the processing and to other security measures which are implemented. 5. whether security measures, which are normal in relation to the purpose of the processing, have been established. The Data Protection Authority can decide that the controller and the processor, and any employees working on their behalf, shall sign a declaration stating their promise to keep secret any sensitive personal data that they will gain knowledge of during the data processing. The controller or his deputy shall attest to the validity of the signature and date on such a declaration, and deliver it to the Data Protection Authority within a given time limit. A breach of this obligation of secrecy shall be punishable according to Article 136 of the General Penal Code. The obligation of secrecy shall continue to be maintained after the termination of employment. The Data Protection Authority can handle a case regarding the processing of sensitive personal data by stipulating, that a special data protection official be appointed to oversee, on behalf of the Data Protection Authority, that the processing is in compliance with law, and that the controller pay all costs stemming from this arrangement.

CHAPTER VII.
Monitoring and sanctions.

Article 36.
Organization and administration of the Data Protection Authority.
The Data Protection Authority is an independent authority with a specific board of directors and is administratively subject to the Minister of Justice. The Data Protection Authority acts with independence in exercising its functions and its

decisions according to this Act cannot be referred to a higher administrative authority. The Minister shall appoint five persons to the Data Protection Authority's board of directors and an equal number of alternative members, for a period of four years at a time. The chairman and vice-chairman of the board are appointed without nomination and they shall be lawyers and fulfil the job requirements of district court judges. The Supreme Court of Iceland nominates one board member and the Icelandic Society for Information Processing shall nominate another and he shall be an expert in the field of computers and technology. Alternative board members shall fulfil the same requirements as the principal members. The Minister decides 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 of directors, appoints the Data Protection Commissioner for a period of five years at a time. The Commissioner attends the board meetings with the right to speak and make proposals. The Commissioner is in charge of daily management and hires other employees of the Authority. The Commissioner is responsible for the financial matters and personal management of the Data Protection Authority. The Data Protection Authority's board decides in other respects the division of duties between the board and its staff.

Article 37.
The tasks of the Data Protection Authority.

The Data Protection Authority monitors the application of this Act and those administrative rules that are issued according to it. The Data Protection Authority rules on cases of dispute concerning the processing of personal data [in Iceland, whether or not the laws governing the processing are Icelandic or not].1) The Data Protection Authority can consider individual cases on its own initiative or on the basis of a communication from someone who maintains that his or her personal data has not been processed in compliance with this Act, and those administrative rules which are issued according to it, or with individual instructions. The tasks of the Data Protection Authority include the following: 1. to handle applications for permits, receive notifications and dictate, as needed, measures relating to technology, security and organization of the processing in order for it to comply with the provisions of the Act, 2) 2. to monitor the compliance with the Act, and other rules regarding the processing of personal data, and that flaws and mistakes are corrected, 3. to observe general trends in the field of personal data protection, domestically and abroad, and maintaining an overall view of, and providing an introduction to, the main issues connected with the processing of personal data, 4. to define and circumscribe where protection of personal data is at risk and provide advice on potential solutions, 5. to guide those who plan to process personal data, or to develop a system for such processing, on personal data protection issues by, among other things, assisting with the production of professional and ethical codes of conduct for individual associations, groups and professions, 3) 6. to express views, either by request or on its own initiative, on issues regarding the processing of personal data, and to provide opinions on bills of law and on other rules of significance for the protection of personal data. 7. to publish an annual report on its activities. The Data Protection Authority can decide that the controller shall pay the cost resulting from monitoring that he complies with the conditions of this Act, and those administrative rules that are issued according to it, or with individual instructions. The Data Protection Authority can also decide that the controller pay the costs associated with an audit of an operation, when the issuance of a processing permit or other handling is being prepared. [The Data Protection Authority issues rules on electronic surveillance and the processing of material which is produced by the surveillance, such as audio and visual material, including rules on its security, preservation and usage. It can also give instructions on the data subject's right to view pictures that have been taken of him or her. The Data Protection Authority also issues rules and gives instructions regarding the destruction of material that is produced by means of electronic surveillance, dictates the processing procedure and preservation period and permits its disclosure in other instances than those that fall under Article 9 Paragraph 2.]] 4) 1) Act No. 90/2001, Art. 11. 2) Rules No. 340/2003. 3) Advertisement No. 1001/2001. 4) Act No. 81/2002, Art. 5.

Article 38.
The Data Protection Authority's access to information, etc.

The Data Protection Authority can demand from controllers, processors and from those working on their behalf, any information and written

explanation that it needs to perform its role, including information that it needs in order to determine if a particular operation or processing is subject to the provisions of the Act. The Data Protection Authority can also summon controllers, processors and those working on their behalf, to provide verbal information and explanations regarding a certain processing of personal data. The Data Protection Authority has, in its monitoring role, the right to access, without a court order, any premises where processing of personal data is conducted or data media are maintained, including premises where files, pictures, cf. Article 4, personal data which are subject to electronic processing, and equipment used to process them, are maintained. The Data Protection Authority can carry out any test or monitoring procedure that it deems necessary, and require the needed assistance of employees of such facilities in order to conduct evaluations or monitoring. The Data Protection Authority can request police assistance if anyone seeks to hinder it in its monitoring capacity. The Data Protection Authority's right to request information or access to facilities and equipment will not be restricted on the grounds of rules regarding the obligation to maintain secrecy.

Article 39.
Exceptions from obligations of secrecy.
Provisions dictating the obligation of secrecy shall not prevent the Data Protection Authority from disclosing information to foreign data protection supervisory authorities, when necessary for the Data Protection Authority or the foreign supervisory authorities to be able to decide upon or carry out actions to ensure the protection of personal data.

Article 40.
Cessation of processing, etc.
The Data Protection Authority can order the cessation of processing of personal data, including collection, documenting or disclosure, order the erasure of personal data or the deletion of records, wholly or partially, prohibit further use of data or instruct the controller to implement measures that ensure the legitimacy of the processing. When deciding whether such measures are to be taken, and which ones are to be applied, the Data Protection Authority shall among other things take into consideration the factors listed in Article 35 Paragraph 2. If a processing is discovered, which violates provisions of this Act, or those administrative rules which are issued according to it, the Data Protection Authority can assign to the Chief of Police the task of halting temporarily the operations of the party in question and seal its place of operation without delay. If someone does not comply with the instructions of the Data Protection Authority according to Paragraph 1, then the Authority can revoke a permit that it has granted according to the provisions of this Act until it concludes that the necessary improvements have been made.

Article 41.
Daily fines.
If the Data Protection Authority's instructions according to Articles 10, 25, 26 or 40 are not observed, the Authority can decide to impose daily fines upon the receiver of the instructions, until it concludes that the necessary improvements have been made. Fines can amount to ISK 100.000 per each day that passes or is passing without the Data Protection Authority's instructions being observed. If a Data Protection Authority's decision to impose daily fines is referred to the courts, then the fines will not begin to accrue until a final judgement has been rendered. Daily fines are deposited to the State Treasury and may be collected by distress without prior judgement.

Article 42.
Sanctions.
Infringements of the provisions of this Act, and of regulations issued according to it, are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law. The same punishment shall apply if instructions by the Data Protection Authority are not observed. If an offence is committed as part of the operations of a legal person, then that legal person can be fined as provided for in Chapter II A of the General Penal Code.

Article 43.
Remedies.
If a controller or a processor has processed personal data in violation of this Act, rules or instructions by the Data Protection Authority, then the controller shall compensate the data subject for the financial damage suffered by him as a result of this. A controller will, however, not be made to compensate for any detriment which he proves that can neither be traced to his mistake nor to any negligence on his or his processors' behalf.

CHAPTER VIII.
Correlation with other acts of law, entry into force, etc.

Article 44.
Correlation with other acts of law.
This Act applies to the processing and handling of personal data conducted according to other legislation, unless otherwise specifically stated in those laws. This Act does not in any way limit the right of access to information prescribed by the Access to Information Act and the Administrative Procedures Act.

Article 45
Regulations regarding individual categories of activity.
The handling of personal data in a particular field of practice, and by individual professions, can be prescribed in a governmental regulation. Permission to collect and register financial and credit standing data of companies, and other legal persons, for the purpose of disclosing such information to others, shall be governed by a regulation. 1) A permit issued by the Data Protection Authority is required for this activity and the following provisions of the Act apply to it: Article 11 on the security and integrity of personal data, Article 12 on internal audits, Article 13 on the handling of data by processors, Article 18 on the data subject's right of access, Article 21 on the duty to provide warning when data are collected from someone else than the data subject himself, Article 25 on rectification and deletion of incorrect and misleading personal data, Article 26 on erasure, deletion, and prohibition of use, of data which are neither incorrect nor misleading, Article 33 on processing which requires a permit, Article 34 on prerequisites for the issue of permits, Article 35 on conditions, Article 38 on the Data Protection Authority's access to information, etc., Article 40 on cessation of processing etc., Article 41 on daily fines, Article 42 on sanctions and Article 43 on remedies. After receiving the opinion of the Data Protection Authority, the Minister shall in a regulation 2) prescribe the Data Protection Authority's role in the monitoring of electronic personal data processing conducted by the police. Among other things, the regulation shall prescribe the duty of the police to notify the Data Protection Authority on electronically processed files that it maintains and the contents of such notifications. It shall also dictate in which cases, and by what method, the data subject may access personal data on himself, which have been registered by the police, and the right of the police to disclose personal data in other instances. Finally, it shall address the security of personal data and internal audits by the police concerning legal compliance in personal data processing, and dictate how long registered data shall be preserved. A regulation shall also address in more detail the practices of those who use lists of names, prepare name inscriptions, for uses that include marketing, and in conducting marketing surveys and opinion polls. 1) Regulation No. 246/2001. 2) Regulation No. 322/2001.

Article 46.
Entry into force.
This Act will enter into force on January 1, 2001. When it enters into force, the Act No. 121/1989, on Registration and Processing of Personal Data, will be repealed. When the Act enters into force, the following amendments to other acts of law will take place: 1. The words "Act Respecting Systematic Recording of Personal Data, No. 121/1989" in the last sentence of Article 20 of the Child Protection Act, No. 58/1992, will be replaced with: Act on the Protection of Privacy as regards the Processing of Personal Data. 2. The words "the Data Protection Commission, cf. Act No. 121/1989, Respecting Systematic Recording of Personal Data," will be replaced with: the Data Protection Authority, cf. Act on the Protection of Privacy as regards the Processing of Personal Data.. 3. The words "The Data Protection Commission" in Article 15, Paragraph 3 of the Act on the Rights of Patients, No. 74/1997, will be replaced with: the Data Protection Authority. 4. The words "The Data Protection Commission" in Article 14, Paragraph 2 of the Act on Electronic Ownership Registration of Securities, No. 131/1997, will be replaced with: the Data Protection Authority. 5. The words "the Data Protection Commission" in Article 4 of the Act on a Health Sector Database, No. 139/1998, and the same words in Articles 5, 6, 7, 10, 12 and 17, will be replaced with: the Data Protection Authority. 6. The words "the Data Protection Commission" in Articles 18 and 19 of the Act on the Schengen Information System in Iceland, No. 16/2000, shall be replaced with: the Data Protection Authority.

Temporary provision.
Immediately after the publishing of this Act, the Minister shall appoint the board of directors and advertise the office of the Data Protection Commissioner vacant. After the appointment of a Commissioner, he will hire other staff as needed to help prepare the Act's entry into force and handle administrative functions in accordance with Paragraph 2. In spite of Article 46 Paragraph 1, the Data Protection Authority shall, immediately after the appointing of its board of directors, begin monitoring the

compliance of the Schengen Information System in Iceland with Act No. 16/2000, on the Schengen Information System in Iceland. Each controller, who uses electronic technology to process personal data when this Act enters into force, shall notify the Data Protection Authority of the processing, using a form intended for that purpose, in accordance with the provisions of Articles 31 and 32, within six months of their entry into force.