Prime Minister's Office

Act on Processing of Personal Data

Act no. 73 on the 8 May 2001 as amended by Act no. 24 on the 17 May 2004

Chapter 1
Objectives

1. The objective of this Act is to protect natural persons, when personal data is being processed, to ensure that the processing of personal data respects their fundamental rights and freedoms and is based on personal data of high quality.

Chapter 2
Definitions

2. For the purpose of this Act:

1) "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject").
2) "Processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, disclosure, adaptation etc. or any combination of this whether electronic or not.
3) "Personal data filing system" ("filing system") shall mean any structured set of personal data, which are accessible according to specific criteria whether centralized, decentralized or dispersed on a functional or geographical basis.
4) "Controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data and determines which equipment can be used.
5) "Processor" shall mean a natural or legal person, public authority, agency or any other body which, processes personal data on behalf of the controller.
6) "Third party" shall mean a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
7) "Recipient" shall mean a natural or legal person, public authority, agency, or any other body to whom data are disclosed, whether a third party or not; however, public authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.
8) "The data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
9) "Sensitive data" shall mean data about colour and ethnic origin, about religion, philosophy or political opinions, about criminal convictions and offences or sexual life, health, trade union connections, material social problems and other purely private matters.

10) "Foreign countries": Denmark and Greenland are also to be considered as foreign countries.

Chapter 3
Scope of the Act

Material scope

3. This Act shall apply to the processing of personal data in the private and public sector:
1) if the processing is wholly or partly by automatic means, and
2) to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) This Act shall not apply to the processing of personal data undertaken by a natural person with a view to the exercise of activities of a purely private nature.
(3) The Minister of Justice may decide that the provisions of this Act shall apply, in full or in part, to the processing of data concerning companies, institutions, firms, etc., which are performed for private or public entities.
(4) The Minister of Justice may decide to provide specific rules on the processing of personal data within particular activities, particular types of companies, particular branches of trade and within certain fields of responsibility.
(5) The Minister of Justice may decide that the provisions of this Act shall not apply, in full or in part, to particular institutions and particular fields of responsibility.

Other legislation

4. Any rules on the processing of personal data in other legislation, which give the data subject a better legal position, shall take precedence over the rules laid down in this Act.

Access with reference to the Act of Public Administration

5. This Act shall not restrict access according to the Act of Public Administration, the Act of Public Access to documents or according to other legislation concerning access to personal data.
(2) If other legislation would provide the data subject access to more personal data than this Act, the controller shall by own initiative inform the data subject of these other rights.

The freedom to speech

6. Processing of personal data, which takes place exclusively for artistic, literary or journalistic purposes shall be governed only by Article 31 and Article 46.
(2) Information databases for journalistic purposes which only contain data which already has been published shall be governed exclusively by Article 31 and Article 46, provided that the data are stored in the database in the original version published.

Territorial scope

7. This Act shall apply to processing of personal data carried out on behalf of a controller who is established in the Faroe Island and to processing of personal data carried out on behalf of a public controller, if this controller is within the home rule authority.
(2) This Act shall also apply to a controller who is established outside the Faroe Island, if:
1) the processing of data is carried out with the use of equipment situated in the Faroe Island, unless such equipment is used only for purposes of transit of data, or
2) the collection of data in the Faroe Islands takes place for the purpose of processing in a foreign country.

(3) A controller who within the scope of this Act in accordance with paragraph 2 shall designate a representative established in the Faroe Islands.

(4) The controller shall inform the Data Protection Authority in writing of the name and address of the designated representative, cf. paragraph 3. The rules applicable to the controller are also applicable to the representative.

Chapter 4
Processing of personal data

Principals relating to the processing of personal data

8. When personal data is processed the controller shall notify the data subject, cf. Articles 18 to 25, notify the Data Protection Authority, cf. Articles 32 to 35, and see to that personal data is processed in accordance with good practices in a way which fulfils these conditions:

1) the personal data is processed lawfully,
2) personal data is only collected for specified purposes which are based on the legitimate activity of the controller and that further processing is compatible with these purposes,
3) the personal data shall be relevant and not excessive in relation to the purposes for which the data are collected and the purposes for which they are subsequently processed,
4) the personal data shall not be used for other purposes which are not compatible with the original purpose without the data subject has given his explicit consent,
5) personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing, and
6) personal data is accurate and kept up to date. Necessary checks should be made to ensure that data, which turns out to be inaccurate or misleading shall be erased or rectified without delay.

(2) If further processing of personal data takes place exclusively for historical, statistical or scientific purposes, this processing shallbe considered compatible with the original purposes for which the data were collected if the disadvantages for the data subject are overridden by significant public interests. .

Requirements when processing personal data

9. Personal data may be processed only if, the data subject has given his consent, the processing is authorised or laid down in law or processing is necessary:

1) for the performance of a contract with the data subject or to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract,
2) for compliance with a legal obligation to which the controller is subject,
3) in order to protect the vital interests of the data subject,
4) for the performance of a task carried out in the public interest,
5) for the performance of a task carried out in the exercise of official authority vested in the controller or a third party to whom the personal data are disclosed, or
6) for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

(2) The processing of personal data concerning the financial standing and creditworthiness of the data subject for the purpose of warning others from contracting with the data subject or for employment matters, shall be subject to the consent from the data subject.

(3) Without the consent of the data subject a company, private entities etc. may not disclose personal data concerning a consumer to a third party for the purpose of marketing or use such data on behalf of a third party for this purpose

Specific requirements when processing of sensitive data

10. Sensitive data cfr. Article 2, subsection 9, may be processed only if, permission is obtained, cfr. Article 35, (1), and the processing fulfils one of the conditions in Article 9 (1), subsections 1 to 6, and also one of the following conditions:

1) the data subject has given his consent,
2) is authorised or laid down in law,
3) processing is necessary in order to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of giving his consent,
4) processing relates to personal data which have been made public by the data subject,
5) processing is necessary for the establishment, exercise or defence of legal claims,
6) for the performance of a task carried out in the exercise of official authority vested in the controller or a third party to whom the personal data are disclosed,
7) processing is necessary for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those personal data are processed by a health professional subject to a statutory obligation of professional secrecy,
8) processing of personal data concerning trade union affiliation is necessary for the controller's compliance with employment obligations or specific rights, or
9) processing is necessary for historical, statistical or scientific purposes, and the disadvantages for the data subject are overridden by significant public interests. Disclosure of personal data requires permission from the Data Protection Authority.

(2) The processing of sensitive data may be carried out in the course of it legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim, no matter the conditions mentioned in Paragraph 1, subsections 1 to 9, relating to the members of the body or to persons who have regular contact with it in connection with its purposes. Disclosure of personal data requires permission from the Data Protection Authority.

(3) The Data Protection Authority may grant permission to the processing of sensitive data in other situations where processing is necessary because of substantial public interest, and measures are carried out to protect the interest of the data subject. The Data Protection Authority may lay down more detailed conditions.

National identification number

11. Public authorities may process data concerning identification numbers unique identification or as file numbers.

(2) Private individuals and entities may process data concerning identification numbers where:

1) this follows from law,
2) the data subject has given explicit consent, or
3) the processing is carried out solely for historical, scientific or statistical purposes.

(3) Paragraph 2, subsection 1 and 2 do not allow disclosure, which can only take place if:

1) disclosure follows from law,
2) the datasubject has given explicit consent to the disclosure,
3) the disclosure is demanded by a public authority, or
4) the disclosure is a natural element of the ordinary operation of enterprises etc. of the type in question and the disclosure is of decisive importance for unique identification of the data subject.

(4) Paragraphs 1-3 do not allow for publication of the identification number. Publication may only take place with the data subject’s consent.

Criminal convictions

12. A complete register of criminal convictions may be kept only under the control of a public authority.
Legal information systems

13. Sensitive data cfr. Article 10 may be processed in legal information systems of significant public importance when the processing is necessary for operating such systems.
(2) The data mentioned in Paragraph 1, may not subsequently be prosessed for any other purpose. The same shall apply to the processing of other data which is carried out solely for the purpose of operating legal information systems.
(3) The Data Protection Authority may lay down more detailed conditions concerning the processing operations mentioned in Paragraph 1. The same shall apply to the personal data, which are processed solely in connection with the operation of legal information systems.

Data storage

14. Data covered by this Act may be transferred to be archived under the rules laid down in the legislation on archives .

Telecommunication

15. Official authorities, private companies etc. may not carry out any automatic registration of who their staff communicate with. However, such registration may take place with the prior authorization from the Data Protection Authority in cases of significant private or public interests. The Data Protection Authority may lay down more detailed conditions for such registration.
(2) The provision laid down in Paragraph 1 shall not apply if otherwise provided by law.
(3) The suppliers of telecommunication network and teleservices may register communication, either for own use or for use in connection with technical administration.

Chapter 5
Transfer of personal data to foreign countries

Fundamental demands

16. Transfer of personal data to a foreign country may take place only if the foreign country ensures an adequate level of protection. The adequacy of the level of protection afforded by a foreign country shall be assessed in the light of all the circumstances surrounding a data transfer, the purpose and duration of the processing operation, the nature of the data, the rules of law in force in the foreign country and the professional rules and security measures which are complied with in that country. Permission is required from the Data Protection Authority cfr. Article 35 (6).
(2) Without prejudice to Paragraph 1, the Minister of Justice may, after having received a statement from the Data Protection Authority, , lay down rules on which foreign countries personal data can be transferred to without prior permission from the Data Protection Authority.

Exceptions

17. The Data Protection Authority may authorize a transfer of personal data to foreign countries, cfr. Article 35 (6) even if the foreign country in question does not ensure an adequate level of protection if:
1) the data subject has given his consent to the transfer,
2) the transfer is required by international conventions or because of membership in an international community,
3) the transfer is necessary for the performance of a contract with the data subject or to do what is required, to implement pre-contractual measures taken in response to the data subject's request,
4) the transfer is necessary for the conclusion or performance of a contract concluded in

the interest of the data subject with a third party,
5) the transfer is necessary in order to protect the vital interests of the data subject,
6) the transfer is necessary for the establishment, exercise or defence of legal claims,
7) the transfer is laid down in law or necessary for the protection of important public interests, or
8) it is authorised in law to require data from a public register.

(2) The Data Protection Authority may authorise transfer of personal data to a foreign country, which does not comply with the conditions laid down in Paragraph 1, where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject. The Data Protection Authority may lay down more detailed conditions for the transfer.

Chapter 6
Access and information of processing personal data

Public access

18. Everyone has the right to know which personal data a controller is processing, and be provided with the following information:
1) the name and address of the controller and of his representatives,
2) who has the day-to-day responsibility under the controller,
3) the purpose of the processing and its name,
4) the groups of data subjects and the categories of the data concerned,
5) the source of the personal data, and
6) if the personal data is disclosed, then to which groups or persons.

Access

19. If the data subject requests access the controller shall communicate to him in an intelligible form about:
1) the name and address of the controller and of his representatives,
2) who has the day-to-day responsibility under the controller,
3) the purpose of the processing and its name,
4) which personal data are being processed,
5) the source of the personal data,
6) if the personal data is disclosed, then to which groups or persons, and
7) the security measures in the processing, as long as access does not harm security.

(2) The data subject may request as accurate information cfr. Paragraph 1, as is necessary to enable the data subject to safeguard his interests.

Information to be provided when data is obtained from the data subject

20. Where the personal data are obtained from the data subject, the controller shall provide the data subject with the following information:
1) the name and address of the controller and of his representative,
2) the purposes of the processing and its name,
3) if the personal data is further disclosed, then to whom,
4) if providing information is obligatory, as well as the possible consequences of failure to provide the information, and
5) of other information necessary to enable the data subject to safeguard his interests in accordance with this Act, including the rules about access and rectification of data relating to the data subject.

(2) The provisions of Paragraph 1 shall not apply where the data subject already has the information mentioned in subsections 1 to 5.

Information to be provided when data is obtained from others than the data subject

21. When the personal data have been obtained from others than the data subject, the controller, who is collecting the data, shall

provide the data subject with information about which personal data is collected and, without delay provide the data subject with the information in Article 20 (1) subsections 1 to 5.
(2) The obligation to inform as laid down in Paragraph 1 shall not apply:

1) if the data subject already has the information referred to in Article 20 (1) subsections 1 to 5,
2) if collection is laid down by law,
3) if the provision of such information to the data subject proves impossible or would involve a disproportionate effort, in these cases the data subject shall be informed if reachable at the latest, when the personal data is being processed.

Derogation from the right to access and information

22. Article 18 and 19 on access and Article 20 (1) and Article 21 (1) on information shall not apply to personal data when:

1) if disclosed can endanger national security, defense or the relationship with other countries or organisations,
2) it should be kept secret because of the prevention, investigation, detection and prosecution of criminal offences,
3) it is not advisable to inform the data subject because of health issues or close relations to the data subject,
4) the data is covered by a binding obligation of secrecy set out in law,
5) the data is only in internal documents which have not been disclosed, or
6) if the data subject's interest in obtaining information is found to be overridden by vital public and private interest.

(2) When access is declined, this shall be reasoned with reference to the relevant provision.
(3) Data, which are processed on behalf of a public administrative authority in the course of its administrative procedures, may be exempted from the right of access under Article 26 to the same extent as under Articles 7-11 and 14 in the law on Public Access to Documents.
(4) The provisions in Article 18 shall not apply when personal data are processed solely for historic, scientific and statistic purposes and when personal data solely are stored as personal data as long as necessary according to the purpose of the processing.
(5) The Minister of Justice may lay down further rules concerning exceptions from the obligation of access and information and also other conditions concerning access to personal data.

How to inform

23. Communication in accordance with Chapter 6 shall be in writing, if requested. In cases where special care should be had for the data subject speak, the communication may be in the form of oral information about the contents of the data.

Respite

24. The controller shall reply to requests for access or other rights, cfr. Chapter 6 without undue delay and at the latest 4 weeks from receipt of the request.
(2) If in special cases it is not possible to reply within 4 weeks, the reply shall be available when possible. The controller shall inform the data subject of the reasons for the delay and when the decision can be expected.

Repetition

25. A data subject who has received a communication in accordance with Article 19 shall not be entitled to a new communication until 6 months after the last communication.
(2) If the data subject can prove that he has a specific interest to that effect, a deviation can be made.

Chapter 7
Other rights of the data subject

26. The data subject may at any time object to the processing of data relating to him.
(2) Where the objection under Paragraph 1 is justified, the processing may no longer involve those personal data.
27. The controller shall on his own, or at the request from the data subject, rectify, erase or block personal data, which are inaccurate or misleading or processed in violation of law or regulations.
(2) The controller shall on his own, or at the request of the data subject, notify the third party to whom the personal data has been disclosed of any rectification, erasure or blocking carried out in compliance with, cfr. Paragraph 1. However, this shall not apply if such notification proves impossible or involves a disproportionate effort.

28. The Minister of Justice may lay more detailed rules concerning how inaccurate or incomplete data shall be corrected.

29. The data subject may withdraw his consent.

30. The data subject may file a complaint to the Data Protection Authority concerning the processing of personal data relating to him.

Chapter 8
Security

31. Controllers, who give processors, individuals, companies etc. performing work for the controller, access to data, shall ensure that personal data is processed only on instructions from the controller, and in accordance with Paragraphs 3 to 5 unless otherwise provided by law.
(2) The processing by way of a processor shall be governed by a written contract between the parties. This contract shall stipulate that the processor shall act only on instructions from the controller and that the rules laid down in Paragraphs 3 to 5 also apply to processing by way of a processor as to the controller.
(3) With appropriate technical and organizational security measures the controller and the processor shall provide that the processing of personal data satisfies the provisions laid down in this Act concerning secrecy, personal freedom and access, and shall implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act. Documentation of organizational security measures shall be available to employees of the controller and processor as well as to the Data Protection Authority. The controller is responsible for the upkeep of measures required by this Act.
(4) The controllers instruction shall not restrict journalistic freedom or impede the production of an artistic or literary product.
(5) The rules in Paragraphs 3 and 4 also apply to personal data, which are given to others than the processor, cfr. Paragraph 1.
(6) As regards personal data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions.
(7) The Minister of Justice may lay down more detailed rules concerning the security measures mentioned in Paragraph 3 and 5.

Chapter 9
Notifying the Data Protection Authority and permission to process.

The duty to notify

32. The controller or his representative shall notify the Data Protection Authority if:
1) the processing of personal data is by electronic means, and/or

2) the processing of personal data in a manual filing system.

(2) The notification shall given no more than 30 days prior to the processing. The Data Protection Authority shall in writing confirm the receipt.

(3) New notification shall be given to the Data Protection Authority if the processing changes and the change is outside the scope of the first notification.

(4) The Minister of Justice may lay down rules on exemptions of from the duty to notify. The Minister may exempt certain categories of processing or certain controllers, he may limit the obligation to notify or require permission. For such processing or controllers rules may be laid down to protect the data subject.

33. The provisions in Article 32 (1) to (3) and Article 34 shall not apply to processing with the aim to produce or upkeep a register which according to law is intended to provide information to the public, if the register is open to the public in general.

Notification

34. The notification shall include the following information:

1) the name and address of the controller, processor and of their representative, if any, and of who has the day to day responsibility of the processing,
2) the purpose of processing, its name and a general description of the processing,
3) the date of the beginning of the processing,
4) a description of the categories of data subjects and the categories of personal data relating to them,
5) where the data comes from, and who the data are to be disclosed, also if they are transferred, cfr. Article 35 (6), including put on the internet,
6) a general description of the measures taken to ensure security of processing,
7) the basis for the processing,
8) the date of erasure of the personal data.

(2) The Data Protection Authority decides, whether or not the notification is fulfilled. The Data Protection Authority may lay down more detailed rules concerning the content and the manner in which to notification.

Permission to process

35. Sensitive data, cfr. Article 2, subsection 9, may be processed only if permission is obtained from the Data Protection Authority.

(2) The Data Protection Authority may also demand permission to process of others personal data when the processing clearly violates important data protection interests. The Data Protection Authority shall in its decision take into consideration the kind of personal data, how many and how comprehensive these are and the aim of the processing.

(3) The controller is entitled to demand that the Data Protection Authority decides whether or not a processing requires permission to process.

(4) The Data Protection Authority may in the permission provide special provisions concerning the processing of personal data to limit the disadvantages for the data subject.

(5) In deciding whether to provide permission there shall be an assessment of whether the processing of personal data holds a disadvantage for the data subject even though conditions would be provided, cfr. Paragraph 4, or even though provisions provided in Chapters 2-7 in this Act are complied with, and the disadvantages still are overridden by the interests in the processing.

(6) The transfer of personal data to foreign countries, cfr. Articles 16 and 17, permission is required, even though the processing would not otherwise require permission.

(7) The Minister of Justice may lay down rules exempting certain categories of processing from the requirement of permission cfr. Paragraph 1. For such processing rules may be laid down to protect the data subject.

Chapter 10
Supervision

The Data Protection Authority

36. The Data Protection Authority shall act with complete independence in executing the functions entrusted to it. The Data Protection Authority, which consists of a Council and a Secretariat, is responsible for the supervision of all processing operations covered by this Act.
(2) The day-to-day business is attended to by the Secretariat, headed by a Director.
(3) The Council, which shall be set up by the Minister of Justice, is composed of a chairman, who shall be a lawyer, and of two other members. Substitutes may be appointed for the members of the Council. The members and their substitutes shall be appointed for a term of 4 years.
(4) The Council shall lay down its own rules of procedure and detailed rules on the division of work between the Council and the Secretariat.

Tasks

37. The Data Protection Authority shall:
1) on its own initiative or acting on a complaint from a data subject, see to that processing of personal data is carried out in compliance with the provisions of this Act and any rules issued by virtue of this Act,
2) treat notifications and applications concerning permission in compliance with the provisions of legislation,
3) provide for an organized general public list providing all notifications and permissions according to this Act,
4) give its opinion to proposed legislation concerning personal data,
5) examine where personal data are processed,
6) direct the private and public sector in cases of doubt and see to that personal data are processed in accordance with good practices,
7) watch closely and inform about the development concerning processing of personal data within this country and in other countries, and
8) submit an annual report.

Powers

38. The Data Protection Authority may order a controller to discontinue a processing operation, which infringes this Act, and to rectify, erase or block specific data undergoing such processing.
(2) The Data Protection Authority may prohibit a controller from using a specified procedure in connection with the processing of data it the Data Protection Authority finds that the procedure in question involves a considerable risk that data are processed in violation of this Act.
(3) The Data Protection Authority may order a controller to implement specific technical and organizational security measures to protect data to ensure that only processing which complies with this Act takes place, and to protect data against accidental or unlawful destruction or accidental loss, alteration, and disclosure to any unauthorized person, abuse or any other unlawful forms of processing.
(4) The Data Protection Authority may in special cases issue a prohibitory or mandatory injunction against data processors, cfr. Paragraphs 1 to 3.

Decisions and opinions

39. The Data Protection Authority shall take binding decisions in cases concerning Articles 9, 10, 11, 13, 15, 16 and 17, Articles 18 to 25, Articles 26, 27, 34, 35, 38 and 40.
(2) In other cases, the Data Protection Authority shall give opinions.
(3) The decisions of the Data Protection Authority may not be brought before any other administrative authority.

Access to personal data

40. The Data Protection Authority may demandall information of importance for its activities.
(2) The members and the staff of the Data Protection Authority shall at any time, without any court order, have access to all premises from where a personal data processing operation is carried out. This includes access to any location where personal data or technical means are being kept or used.

41. The Data Protection Authority shall submit an annual report on its activities. The report shall be made public.

42. The Data Protection Authority shall co-operate with others authorities in the Faroe Island and in foreign countries to the extent required to fulfill this Act.

Payment

43. The Minister of Justice may provide further rules concerning payment in connection with the submission of notifications and applications for permission under this Act.

Chapter 11
Liability and damages and criminal liability

Penalty

44. Unless a higher penalty must be imposed under other legislation, a person shall be liable to a fine or imprisonment for a term not exceeding four months if the following cases:
1) failure to notify, cfr. Article 32,
2) processing of personal data without permission, cfr. Article 35,
3) failure to comply with the requirements of the Data Protection Authority, cfr. Article 10 (3), Article 13 (3), Article 15 (1), Article 17 (2), Article 34 (2), Article 35, (4) and Article 38,
4) Processing contrary to conditions as referred to in Articles 8 to 13, Article 15, Article 16, Article 17, Article 32,
5) infringes Articles 23 to 25, Article 26, Article 27,
6) failure to inform the Data Protection Authority, cf. Article 7 (4), Articles 18 to 21, article 40.

(2) Any rules issued by virtue of this Act may stipulate punishment in the form of a fine or imprisonment for a term not exceeding four months.
(3) Companies etc. (legal persons) may incur criminal liability when infringing the rules of this Act.

45. Any person who carries on business, cfr. Article 9 (2) and (3), if convicted of a criminal offence may be deprived of the right to operate such activity in case the offence committed gives reason to suspect an imminent risk of abuse. In other respects, section 79 (3) and (4) of the Criminal Code shall apply.

Liability

46. The controller shall compensate any damage caused by the processing of personal data in violation of the provision of this Act unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of personal data.

Chapter 12
Final provisions, including commencement provisions

Entry into force

47. This Act shall enter into force on 1 January 2002 and at the same time the Private Registers Act, cf. Consolidation Act No. 107 of 15 November 1984 and the Public

Registers Act, Consolidation Act No 62 of 5 June 1984 shall be repealed.
(2) The members of the Register Council shall step in as members of the Data Protection Council until the Minister of Justice has appointed the members of the Data Protection Council.

48. Registers according to the Public Registers Act and the Private Registers Act shall no later than 6 month after the entry into force comply with the rules of this Act.
(2) The Data Protection Authority may in special cases lay down rules on prolonged period of adjustment mentioned in Paragraph 1, if considered necessary.