Prime Minister's Office

Act on the protection of personal data (Data protection Act) [1]
Act no. 80 on the 7. June 2020

Chapter 1
Material scope, territorial scope etc.

Subject-matter and objectives

1. This Act lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

Material scope

2. This Act shall apply to the processing of personal data:
1) when the processing wholly or partly is by automated means, and
2) processing of personal data other than by automated means which form part of a filing system or are intended to form part of a filing system.

3. This Act shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.
(2) This Act shall not apply to the processing of personal data the by Parliament (Løgtingið) and institutions under the Parliament.
(3) Chapters 2-7 shall not apply to processing of personal data which takes place exclusively for artistic, literary or journalistic purposes. However Articles 41, 42 and 47 shall apply.
(4) Chapters 2-7 shall not apply to processing of personal data in information databases for journalistic purposes that exclusively include already published materials, provided the data are stored in the information database in the original version published. However Articles 41, 42 og 47 shall apply.

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

Territorial scope

5. This Act shall apply to the processing of personal data performed as part of activities carried out on behalf of:
1) a private data controller or data processor that is established on the

Faroe Islands, regardless of whether the processing takes place in the on the Faroe Islands, and

2) a public data controller or data processor that is established on the Faroe Islands and is within the home rule authority, regardless of whether the processing takes place in the on the Faroe Islands.

(2) This Act shall apply to the processing of the personal data of data subjects located on the Faroe Islands, carried out by a data controller or data processor that is not established on the Faroe Islands, if the processing activities are related to:

1) offering goods or services to such data subjects who are on the Faroe Islands, regardless of whether payment from the data subject is required, or
2) the monitoring of the behaviour of such data subjects insofar as their behaviour takes place on the Faroe Islands.

Definitions

6. For the purposes of this Act:

1) 'Personal data' means any information relating to an identified or identifiable natural person, the 'data subject'.
2) 'Processing' means any operation performed upon personal data, whether or not by automatic means, such as recording, organization, storage, adaptation, collection etc.
3) 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
4) 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
5) 'Filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
6) 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
7) 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
8) 'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
9) 'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules.
10) 'Consent of the data subject' means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the

processing of personal data relating to him or her.

11) ’Genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
12) ’Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
13) ’Data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
14) ’Foreign country’ means a country which is a member of the European Union (EU) or the European Economic Area (EEA).
15) ’Third country’ means a country which is not a member of the European Union (EU) or the European Economic Area (EEA).
16) ’Information society service’ shall mean any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Chapter 2
Principles and lawfullness of processing

Principles relating to processing of personal data

7. Personal data shall be:

1) Processed lawfully, fairly and in a transparent manner in relation to the data subject.
2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4) Accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational, including physical, measures.

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.

(3) Further processing for historical, statistical or scientific purposes shall not be considered to be incompatible with the purposes for which the data were collected if the disadvantages for the person whom the data relate are overridden by significant public interests.

Lawfulness of processing

8. Processing shall be lawful only if and to the extent that at least one of the following applies:

1) The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
2) Processing is necessary for the performance of a contract to which the

data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3) Processing is necessary for compliance with a legal obligation to which the controller is subject.
4) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights of the data subject which require protection of personal data.

(2) Subsection 6 of paragraph 1 shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for consent

9. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
(4) Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Conditions applicable to child's consent in relation to information society services

10. Where processing of personal data of a child, in relation to the offer of information society services directly to a child, is based on consent the processing of the personal data of the child shall be lawful provided the child is at least 13 years old.
(2) If the child is under the age of 13, the processing is only lawful if and to the extent that consent is given or approved by the holder of parental responsibility for the child. In consideration of available technology the controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Processing of sensitive personal data

11. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, data concerning criminal convictions and offences, material social problems and other purely private matters shall be prohibited.
(2) Processing of personal data covered by paragraph 1 is only allowed if and to the extent Articles 12-14 or Articles 18 and 19 apply.

12. Article 11 (1) shall not apply if one of the following applies:
1) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where law provides that the prohibition referred to in Article 11 (1) may not be lifted by the data subject.
2) Processing is based on law.
3) Processing is necessary for the purposes of carrying out the

obligations and exercising specific rights of the controller or of the data subject in the field of employment.

4) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
5) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
6) Processing relates to personal data which are manifestly made public by the data subject.
7) Processing is necessary for the establishment, exercise or defence of legal claims.
8) Processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or occupational medicine, for the assessment of the working capacity of the employee, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy.

(2) Processing of data covered by Article 11 (1) may also take place if processing is necessary for reasons of substantial public interest. The Data Protection Authority shall give its authorisation for this purpose if the processing is not carried out on behalf of a public authority. The Data Protection Authority may lay down more detailed terms for the processing.
(3) In consultation with the minister responsible for data protection, the competent minister may lay down more detailed rules regarding the processing of personal data covered by Article 11 (1). The rules shall provide sufficient guarantees for the rights of the data subject.

Processing of personal data relating to criminal convictions and offences

13. Personal data relating to criminal convictions and offences covered by Article 11 (1), may be processed on behalf of a public authority, if such processing is necessary for the performance of the tasks of the authority.
(2) Personal data relating to criminal convictions and offences may not be disclosed by the public authority. Disclosure may, however, take place where:

1) the data subject has given explicit consent to such disclosure,
2) disclosure takes place for the purpose of safeguarding private or public interests which clearly override the interests of secrecy,
3) disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority, or
4) disclosure is necessary for the performance of tasks for a public authority by a person or an enterprise.

(3) Private individuals or entities may process data about criminal convictions and offences if the data subject has given explicit consent. Processing may also take place if necessary for the purpose of safeguarding a legitimate interest and this interest clearly overrides the interests of the data subject.
(4) The data mentioned in paragraph 3 may not be disclosed without the explicit consent of the data subject. However, disclosure may take place without consent for the purpose of safeguarding public or private interests which clearly override the interests of secrecy.

(5) The processing of data in the cases regulated by paragraph 1-4 may otherwise take place if the conditions laid down in Article 12 are satisfied.

14. A complete register of criminal convictions may only be kept under the control of a public authority.

Processing which does not require identification

15. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Act.
(2) Where, in cases referred to in paragraph 1, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 26-31 shall not apply except where the data subject, for the purpose of exercising his or her rights under those sections, provides additional information enabling his or her identification.

Chapter 3
Specific processing situations

Processing of the national identification number

16. Public authorities may process data concerning identification numbers with a view to 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,
3) the conditions laid down in § 12 are satisfied, or
4) the processing is carried out solely for historical, scientific or statistical purposes.

(3) Paragraph 2, subsection 1-3 does 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.

Processing of personal data for the purpose of direct marketing

17. An enterprise may not disclose data concerning a consumer to another enterprise for the purpose of direct marketing or use such data on behalf of another enterprise for this purpose unless the consumer has given consent. Consent shall be obtained in accordance with the rules laid down in Article 6 of the Marketing Practices Act.
(2) However, the disclosure and use of data as mentioned in paragraph 1 may take place without consent in the case of general data on customers which form the basis for classification into customer categories, and if the conditions of Article 8 (1), subsection 6 are complied with.
(3) Data of the type mentioned in Article 11 (1) of this Act may not be disclosed or used pursuant to paragraph 2.

Processing of personal data for historical, statistical and scientific purposes

18. Sensitive data, cfr. Article 11 (1), may be processed if the processing is necessary for the purpose of historical, statistical or scientific purposes and the disadvantages for the person whom the data relate is overridden by significant public interests.
(2) The data covered by paragraph 1 may not subsequently be processed for other purposes. The same shall apply to processing of other data carried out solely for historical, statistical or scientific purposes.
(3) The data covered by paragraphs 1 and 2 may only be disclosed to a third party with prior authorisation from the Data Protection Authority. The Data Protection Authority may lay down terms for the disclosure.

Legal information systems

19. Sensitive data, cfr. Article 11 (1), may be processed where the processing is carried out for the sole purpose of operating legal information systems of significant public importance and the processing is necessary for operating such systems.
(2) The data covered by paragraph 1 may not subsequently be processed for other purposes. The same shall apply to processing of other data carried out solely for the purpose of operating legal information systems.
(3) The minister responsible for data protection may lay down specific conditions concerning the processing operations mentioned in paragraph 1. The same shall apply to the data covered by Article 8 processed solely in connection with the operation of legal information systems.

Archiving personal data

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

Chapter 4

Rights of the data subject

Transparent information, communication and modalities for the exercise of the rights of the data subject

21. The controller shall ensure that any information to the data subject provided in accordance with this Act is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
(2) The controller shall facilitate the exercise of data subject rights under Articles 26-36 and shall not refuse to act on the request of the data subject for exercising his or her rights, unless the controller demonstrates that it is not in a position to identify the data subject, cfr. Article 15 (2).
(3) The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within 4 weeks of receipt of the request. That period may be extended by 8 weeks where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of any such extension within 4 weeks of receipt of the request, together with the reasons for the delay and any information on when the request will be answered.
(4) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within 4 weeks of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Data Protection Authority.
(5) Information provided under Articles 23 and 24 and any communication and any actions taken under Articles 26-36 and 49 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly

unfounded or excessive character of the request.

22. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
(2) Information may be given orally if the data subject documents his or her identity. Where the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Information to be provided where personal data are collected from the data subject

23. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
1) the identity and the contact details of the controller and, where applicable, of the controller's representative,
2) the contact details of the data protection officer,
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
4) where the processing is based on Article 8 (1) subsection 6, the legitimate interests pursued by the controller or by a third party,
5) the recipients or categories of recipients of the personal data, and
6) the fact that the controller intends to transfer personal data to a foreign country, a third country or international organisation and the existence or absence of an adequacy decision. If the transfer is based on Articles 61-64 the controller shall refer to the relevant legal basis.

(2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing:
1) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
2) the rigths in chapter 4,
3) the right to withdraw consent at any time, if the processing is based on consent,
4) the right to lodge a complaint with the Data Protection Authority,
5) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and of the possible consequences of failure to provide such data, and
6) the existence of automated decision-making, including at least the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
(4) Paragraphs 1-3 shall not apply where and insofar as the data subject already has the information.

Information to be provided where personal data have not been obtained from the data subject

24. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
1) the identity and the contact details of the controller and, where applicable, of the controller's representative,
2) the contact details of the data protection officer,

3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
4) the categories of personal data concerned,
5) the recipients or categories of recipients of the personal data, and
6) the fact that the controller intends to transfer personal data to a foreign country, a third country or international organisation and the existence or absence of an adequacy decision. If the transfer is based on Articles 61-64 the controller shall refer to the relevant legal basis.

(2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing:

1) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
2) where the processing is based on Article 8 (1) subsection 6, the legitimate interests pursued by the controller or by a third party,
3) the rigths in chapter 4,
4) the right to withdraw consent at any time, if the processing is based on consent,
5) the right to lodge a complaint with the Data Protection Authority,
6) from which source the personal data originate, and
7) the existence of automated decision-making, including at least the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

25. The controller shall provide the information referred to in Article 24, paragraphs 1 and 2:

1) within a reasonable period after obtaining the personal data, but at the latest within 4 weeks,
2) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject, or
3) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

(2) Article 24 shall not apply if:

1) the data subject already has the information,
2) the provision of such information proves impossible or would involve a disproportionate effort,
3) the provision of such information is likely to render impossible or seriously impair the achievement of the objectives of that processing,
4) obtaining or disclosure is expressly laid down by law to which the controller is subject, or
5) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law.

(3) In cases covered by paragraph 2, subsection 2 and 3 the controller shall take appropriate measures to protect the data subject's rights, including making the information publicly available.

Right of access by the data subject

26. If the data subject requests access, the controller shall confirm as to whether or not personal data concerning him or her are being processed, and, where that is the case, give access to the personal data. The controller shall also provide the following information:

1) the purposes of the processing,
2) the categories of personal data concerned,
3) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular

recipients in foreign countries, third countries or international organisations,
4) the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
5) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing,
6) the right to lodge a complaint with the Data Protection Authority,
7) where the personal data are not collected from the data subject, any available information as to their source, andthe existence of automated decision-making, including at least the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, cfr. Articles 61-64, the controller shall inform the data subject of the basis for the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee.

Right to rectification

27. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

(2) The data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure

28. The controller shall on his or her own initiative or at the request of the data subject erase personal data concering the data subject without undue delay where one of the following grounds applies:
1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
2) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing,
3) the data subject objects to the processing and the conditions in Articles 32 and 33 are met,
4) the personal data have been unlawfully processed,
5) the personal data have to be erased for compliance with a legal obligation to which the controller is subject, or
6) the personal data have been collected in relation to the offer of information society services referred to in Article 10 (1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller shall take reasonable steps to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
1) for exercising the right of freedom of expression and information,
2) for compliance with a legal obligation which requires processing to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
3) for archiving purposes, historical, statistical or scientific purposes in so far as erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
4) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

29. If the data subject so requests the controller shall restrict the processing where one of the following applies:

1) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data,
2) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
3) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims, or
4) the data subject has objected to processing pursuant to Article 32 pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall only be processed:

1) with the data subject's consent,
2) for the establishment, exercise or defence of legal claims,
3) for the protection of the rights of another natural or legal person, or
4) for reasons of important public interest.

(3) If the processing is restricted pursuant to paragraph 1 the controller shall inform the data subject before the restriction of processing is lifted.

Notification obligation of the controller

30. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 27, 28 (1) or 29 (1) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Right to data portability

31. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller and have the right to transmit those data to another controller, where:

1) the processing is based on consent or on a contract, and
2) the processing is carried out by automated means.

(2) The personal data which the data subject receives pursuant to paragraph 1, shall be in a structured, commonly used and machine-readable format.

(3) Where technically feasible the data subject shall have the right to have the personal data transmitted directly from one controller to another.

Right to object

32. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Article 8 (1), subsection 5 or 6.

(2) The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

33. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing.

(2) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

34. At the latest at the time of the first communication with the data subject, the right referred to in Articles 32 and 33 shall

be explicitly brought to the attention of the data subject. The information shall be presented clearly and separately from any other information.

Automated individual decision-making, including profiling

35. The data subject shall not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision:

1) is necessary for entering into, or performance of, a contract between the data subject and a data controller,
2) is authorised by law to which the controller is subject, or
3) is based on the data subject's explicit consent.

(3) In the cases referred to in paragraph 2, subsection 1 and 3, the controller shall implement suitable measures to safeguard the data subject's rights.

(4) Decisions referred to in paragraph 2 shall not be based on sensitive personal data referred to in Article 11 (1), unless Article 12 (1) subsection 1 or Article 12 (2) apply and suitable measures to safeguard the data subject's rights are in place.

Restrictions

36. The provisions in Article 23 (1)-(3) and Article 24 on information, Article 26 on access and Article 48 on notification of data breaches 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 or the enforcement of criminal penalties, including the safeguarding against and the prevention of threats to public security,
3) it is not advisable to inform the data subject because of health issues or close relations to the data subject,
4) it is subject to secrecy or confidentiality pursuant to law, or
5) the data subject's interest in this information is found to be overridden by essential considerations of public or private interests.

(2) 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 2, 7-11 and 14 in the law on Public Access to Documents.

(3) The provisions in Articles 26, 27, 29 and 32 shall not apply when personal data are processed solely for historic, scientific and statistic purposes if the personal data is stored as personal data only as long as necessary according to the purpose of the processing and the exercise of such rights is likely to render impossible or seriously impair the achievement of the objectives of that processing.

(4) The minister responsible for data protection may lay down further derogations from the right to information and access and may lay down conditions when access is given.

Chapter 5
Controller and processor

Responsibility of the controller

37. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act.

Data protection by design and by default

38. The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles pursuant to this Act in an effective manner.
(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Joint controllers

39. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Act.

Representatives of controllers or processors not established on the Faroe Islands

40. Where Article 5 (2) applies, the controller or the processor shall designate in writing a representative on the Faroe Islands.
(2) The obligation laid down in paragraph 1 shall not apply to:
1) processing which is occasional, does not include, on a large scale, processing of sensitive data, cfr. Article 11 (1), and is unlikely to result in a risk to the rights of natural persons, or
2) a public authority or body.

(3) The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor on all issues related to processing of personal data.

Processor

41. The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Act.
(2) Processing by a processor shall be governed by a contract that is binding and that sets out inter alia the subject-matter, the purpose of the processing and the obligations and rights of the controller. That contract shall stipulate, in particular, that the processor:
1) processes the personal data only on documented instructions from the controller, unless required to do so by law to which the processor is subject,
2) ensures that persons authorised to process the personal data are under an obligation of confidentiality,
3) respects the conditions referred to in Article 42 for engaging another processor,
4) takes all measures required pursuant to Article 46,
5) assists the controller for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter 4,
6) assists the controller in ensuring compliance with the obligations pursuant to Articles 46-52,
7) deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless law requires storage of the personal data,
8) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article, and
9) allows for and contributes to audits.

(3) The processor shall immediately inform the controller if, in its opinion, an instruction infringes applicable law.*(4)* Without prejudice to Articles 77-79, if a processor infringes this Act by determining the purposes and means of

processing, the processor shall be considered to be a controller in respect of that processing.

42. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
(2) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor.

43. The minister responsible for data protection may after having obtained the opinion of the supervisory autority approve standard contractual clauses for the matters referred to in Articles 41 (2) and 42 (2).
(2) The contract between the controller and processor may in full or in part be based on the standard contractual clauses approved by the minister responsible for data protection. The contract shall be in writing, including in electronic form.

Records of processing activities

44. Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
1) the name and contact details of the controller,
2) the purposes of the processing,
3) a description of the categories of data subjects and of the categories of personal data,
4) the categories of recipients including recipients in foreign countries, third countries or international organisations,
5) transfers of personal data to a foreign country, a third country or an international organisation,
6) the envisaged time limits for erasure of the different categories of data, and
7) a general description of the technical and organisational security measures referred to in Article 46 (1).

(2) Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller. These records shall contain:
1) the name and contact details of the processor and of each controller on behalf of which the processor is acting,
2) the categories of processing carried out,
3) transfers of personal data to a foreign country, a third country or an international organisation, and
4) a general description of the technical and organisational security measures referred to in Article 46 (1).

(3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form and shall be made available to the supervisory authority on request.
(4) Paragraphs 1-3 shall also apply to the representative of the controller or processor.

45. Article 44 shall not apply to an enterprise or an organisation employing fewer than 250 persons. Regardless of the first sentence, Article 44 shall apply if the processing:
1) is likely to result in a risk to the rights of data subjects,
2) the processing is not occasional, or
3) the processing includes sensitive personal data, cfr. Article 11 (1).

Security of processing

46. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing

as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These measures may include inter alia:

1) the pseudonymisation and encryption of personal data,
2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
(3) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by law.
(4) In consultation with the competent minister, the minister responsible for data protection may lay down rules to the effect that personal data which are processed in specified IT systems and kept for public administrative authorities, must be stored, in full or in part, exclusively on the Faroe Islands.

Notification of a personal data breach to the Data Protection Authority

47. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Authority. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
(2) Paragraph 1 shall not apply if the personal data breach is unlikely to result in a risk to the rights of natural persons.
(3) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
(4) The notification referred to in paragraph 1 shall at least:

1) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,
2) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained,
3) describe the likely consequences of the personal data breach, and
4) describe the measures taken or proposed to be taken by the controller to address the personal data breach.

(5) If it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
(6) The controller shall document any personal data breaches. That documentation shall enable the Data Protection Authority to verify compliance with this Article.

Communication of a personal data breach to the data subject

48. When the personal data breach is likely to result in a high risk to the rights of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information referred to in Article 47 (4), subsection 2-4.
(3) The communication to the data subject shall not be required if any of the following conditions are met:
1) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,
2) the controller has taken subsequent measures which ensure that the high risk to the rights of data subjects referred to in paragraph 1 is no longer likely to materialise, or
3) it would involve disproportionate effort.

(4) If the controller has not already communicated the personal data breach to the data subject, the Data Protection Authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Data protection impact assessment

49. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

(2) A data protection impact assessment shall in particular be required in the case of:
1) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person,
2) processing on a large scale of sensitive personal data, cfr. Article 11 (1), or
3) a systematic monitoring of a publicly accessible area on a large scale.

(3) The Data Protection Authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.
(4) The Data Protection Authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

§ 50. The data protection impact assessment pursuant to Article 49 shall contain at least:
1) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller,
2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes,
3) an assessment of the risks to the rights of data subjects, and
4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act.

(2) If there is a change of the risk represented by processing operations the controller shall carry out a review to assess if processing is performed in accordance

with the data protection impact assessment.

51. The provisions in Articles 49 and 50 do not apply if a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of a law.

Prior consultation of the Data Protection Authority

52. The controller shall consult the Data Protection Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
(2) Where the Data Protection Authority is of the opinion that the intended processing would infringe this Act, the Data Protection Authority shall, within period of up to eight weeks, provide written advice to the controller or processor and may use any of its powers referred to in this Act. That period may be extended by six weeks, taking into account the complexity of the intended processing. The Data Protection Authority shall inform the controller or processor of any such extension within 4 weeks of receipt of the request for consultation together with the reasons for the delay.
(3) When consulting the Data Protection Authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

1) the respective responsibilities of the controller, joint controllers and processors involved in the processing,
2) the purposes and means of the intended processing,
3) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Act,
4) the contact details of the data protection officer,
5) the data protection impact assessment, and
6) any other information requested by the Data Protection Authority.

Designation of the data protection officer

53. The controller and the processor shall designate a data protection officer where:

1) the processing is carried out by a public authority or body,
2) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale, or
3) the core activities of the controller or the processor consist of processing on a large scale of sensitive data, cfr. Article 11 (1).

(2) A group of undertakings may appoint a single data protection officer.
(3) Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

54. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 58.
(2) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
(3) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Data Protection Authority.

Position of the data protection officer

55. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller and processor shall support the data protection officer in performing the tasks referred to in Article 58, in maintaining his or her expert knowledge and in giving access to personal data and processing operations.
(3) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.
(4) The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

56. The data protection officer shall directly report to the highest management level.
(2) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.

57. Data protection officers designated under Article 53 (1), subsection 2 and 3 may not without justification disclose or exploit data into which they have obtained insight in connection with the exercise of their duties as data protection officers.

Tasks of the data protection officer

§ 58. The data protection officer shall have at least the following tasks:
1) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Act,
2) to monitor compliance with this Act and other data protection provisions,
3) to provide advice where requested as regards the data protection impact assessment and monitor its performance,
4) to cooperate with the Data Protection Authority, and
5) to act as the contact point for the Data Protection Authority on issues relating to processing.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with the processing.

Chapter 6
Transfers of personal data to foreign countries, third countries or international organisations

Transfers of personal data to foreign countries

59. Transfers of personal data to foreign countries shall not require any specific prior authorisation.

Transfers to third countries etc. on the basis of an adequacy decision

60. A transfer of personal data to a third country or an international organisation may take place without any specific prior authorisation if the minister responsible for data protection has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.
(2) The minister responsible for data protection after assessing the adequacy of the level of protection and after an opinion is given by the Data Protection Authority, may decide that the third country etc. ensures an adequate level of protection.
(3) The Data Protection Authority shall, on an ongoing basis, monitor the level of protection in third countries etc., cfr. paragraph 2. If the Data Protection Authority is of the opinion that the level of protection is no longer adequate, it shall without undue delay notify the minister responsible for data protection.

Transfers subject to appropriate safeguards

61. In the absence of a decision pursuant to Article 60, a controller or processor may transfer personal data to a third country etc. only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for by:

1) a legally binding and enforceable instrument between public authorities or bodies, or
2) standard data protection clauses adopted by the minister responsible for data protection after receiving the opinion of the Data Protection Authority.

(3) Subject to the authorisation from the Data Protection Authority, the appropriate safeguards referred to in paragraph 1 may also be provided for in contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country etc.

Derogations for specific situations

62. If Articles 60 or 61 do not apply transfer of personal data to a third country etc. shall take place only on one of the following conditions:

1) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards,
2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request,
3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person,
4) the transfer is necessary for important reasons of public interest,
5) the transfer is necessary for the establishment, exercise or defence of legal claims,
6) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent, or
7) the transfer is made from a register which according to law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid in law for consultation are fulfilled in the particular case.

(2) A transfer pursuant to paragraph 1, subsection 7 shall not involve the entirety of the personal data contained in the register.

63. If Articles 60 or 61 do not apply and non of the derogations in Article 62 apply transfer of personal data to a third country etc. shall take place only if the transfer:

1) is not repetitive,
2) concerns only a limited number of data subjects,
3) is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights of the data subject, and
4) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

(2) The controller shall inform the Data Protection Authority of the transfer. The controller shall also inform the data subject of the transfer pursuant paragraph 1 and on the compelling legitimate interests pursued.

64. Article 62 (1), subsection 1-3 and Article 63 shall not apply to activities carried out by public authorities in the exercise of their public powers.
(2) The controller or processor shall document the assessment as well as the suitable safeguards referred to in Article 63 (1), subsection 4, in the records referred to in Article 44.

Prohibition of transfer of sensitive data

65. If a decision has not been adopted concerning the adequacy of the level of protection pursuant to Article 61, the Data Protection Authority may in exceptional cases prohibit, restrict, or suspend the transfer to a third country etc. of sensitive data, cfr. Article 11 (1).

Chapter 7
Data Protection Authority

Organisational structure

66. The Data Protection Authority is an independant authority and shall act with complete independence in exercising its tasks and powers.
(2) The Data Protection Authority, which consists of a Council and a Secretariat, is responsible for monitoring processing of personal data in accordance with this Act.
(3) The day-to-day business is attended to by the Secretariat, headed by a Director.
(4) The Council shall determine its own rules of procedure and the specific rules governing the distribution of work between the Council and the Secretariat.

67. The Minister responsible for data protection shall appoint the Data Protection Council, consisting of a chairman who must be a lawyer, and of four additional members. Two of the members are nominated by the Accociation of Municipalities and the Faroe Employer's Association recpectively.
(2) Substitutes are also to be appointed for the members. The members and the substitutes shall be appointed for a term of four years. Reappointment may take place two times. The appointment of the chairman, the members and their substitutes shall be based on their professional qualifications.

Tasks

68. The Data Protection Authority shall inter alia:
1) on its own initiative or acting on a complaint from a data subject, ensure that the processing of personal data is in compliance with this Act,
2) promote public awareness in relation to data protection,
3) advise the government (Landsstýrið), the parliament (Løgtingið) and other institutions and bodies on legislative and administrative measures relating to the protection of personal data,
4) promote the awareness of controllers and processors of their obligations under this Act,
5) conduct investigations where personal data is being processed,
6) monitor and inform of relevant developments regaring data protection on the Faroe Islands and abroad, and
7) draw up and make public an annual report on its activities.

69. The Data Protection Authority shall co-operate with others authorities in the Faroe Islands and abroad, if relevant.

Powers

70. The Data Protection Authority shall have the power to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Act and to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Act.

(2) The Data Protection Authority shall have the power to order the controller or processor to discontinue processing operations and have the power to order the controller or processor to rectify or erase personal data or restrict processing of personal data.
(3) The Data Protection Authority shall have the power to order the controller or processor to bring processing operations into compliance with this Act within a specified period.
(4) The Data Protection Authority shall have the power to order the controller or processor to implement technical and organisational, including physical, security measures to ensure that only processing in compliance with this Act takes place, and to ensure that personal data is not unlawfully destructed, lost or restricted and that the personal data is not disclosed to unauthorised persons or otherwise unlawfully processed.

71. The Data Protection Authority may demand being given all information of importance for its activities.
(2) The members and leading staff of the Data Protection Authority shall at any time against appropriate proof of identity and 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.

Decisions of the Data Protection Authority etc.

72. The decisions of the Data Protection Authority may not be brought before any other administrative authority.

73. The Data Protection Authority may publish its statements and decisions. Decisions which are made public shall be anonymised and be made unrecognisable to the extent possible. Such publication shall also be subject to Article 36 of this Act.

74. The opinion of the Data Protection Authority shall be obtained when Acts, Executive Orders, Circulars or similar general regulations of importance regarding the processing of personal data are being drafted.

75. The minister responsible for data protection may lay down rules prescribing that communication to the Data Protection Authority must be transmitted by digital means, including rules on the use of specified IT systems, special digital formats and digital signatures, etc.

Chapter 8
Remedies, liability and penalties

The right to lodge a complaint

76. Every data subject shall have the right to lodge a complaint with the Data Protection Authority about the processing of personal data relating to him or her.

Compensation

77. The controller or processor shall compensate any damage caused by an unlawful processing activity or any other processing contrary to the provisions of this law, unless it is established that such damage could not have been averted through the diligence and care required when processing of personal data.

Penalty

78. 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 six months if that person infringes the provisions on:
1) the data controller's and the data processor's obligations under Articles

10, 15, 38-42, 43, (2), 2. sentence, 44, 46-50, 52 (1) and (3), 53, 55 or 58,
2) the fundamental principles of processing set out in Articles 7 (1) and (2), 8, 9 (1), (2) and (4), 11, 12 (1) and (2), 13-14, 16-17, 18 or 19 (1) and (2),
3) the rights of data subjects under Articles 9 (3), 21 and 22, 23(1)-(3), 24, 25 (1) or 26 and 27, 28(1) and (2) or 29-35,
4) the transfer of personal data to third countries etc. under Articles 60-63, 64 (2) or 65.
5) prevents the Data Protection Authority from gaining information or access under Article 71,
6) fails to comply with terms or an order from the Data Protection Authority given under Articles 12 (2), 18 (3), 19 (3) or 70 (1)-(4),
7) fails to comply with the Data Protection Authority's decisions under the law in other respects or sets aside the Data Protection Authority's terms of authorisation according to the law.

(2) Anyone who violates Article 57 shall be punished with a fine unless a higher penalty must be imposed according to other legislation.
(3) Penalties in the form of a fine may be prescribed by rules issued in pursuance of this Act.
(4) Companies etc. (legal persons) may incur criminal liability according to the rules of Part 5 of the Criminal Code.
(5) The period of limitation for infringement of this Act or rules issued in pursuance of this Act is five years.

Fixed penalty notices

79. Where an infringement of this law or rules issued in pursuance of this Act is estimated not to result in a penalty higher than a fine, the Data Protection Authority may indicate by a fixed penalty notice that the case may be settled without legal proceedings, if the party who committed the infringement admits to being guilty of the infringement and declares acceptance of a fine indicated in the fixed penalty notice within a specified time limit.
(2) The rules of the Administration of Justice Act on the requirements for the content of an indictment and on the right of an accused to remain silent shall also apply to a fixed penalty notice.
(3) Where a fine is accepted, any further prosecution shall be discontinued.

80. Anyone who operates or is engaged in the activity referred to in Article 19 or stores personal data as a private data processor may if convicted of a criminal offence 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.

Chapter 9
Entry into force

81. This Act shall enter into force on 1 January 2021 and at the same time Act no. 73 of 8 May 2001 on the processing of personal data shall be repealed, cfr. paragraph 2.
(2) Article 67 enters into force on 1 July 2020 and at the same time Article 36 (3) in Act no. 73 of 8 May 2001 on the processing of personal data shall be repealed.
(3) Authorisations given by the Data Protection Authority under Act no. 73 of 8 May 2001 on the processing of personal data shall be valid until 1 January 2022.
(4) Data processing contracts in accordance with Article 31 (2) Act no. 73 of 8 May 2001 on the processing of personal data, entered in to prior to the entry into force of this Act, shall be in line with this Act on 1 January 2022 at the latest.

[1] This is an unauthorised English translation. The original version which has been published in the Official Law Journal of the Faroe Islands is the only legally valid version.