Chapter 3. Special commentary[1]

In addition to the 99 articles GDPR has 173 recitals. These recitals can compare to the commentary known in faroese law proposals. In the special commentary below there are references to the Articles and recitals in the GDPR that substatively correspond to the relevant article.

GDPR is attached to this proposal. GDPR is not a part of the law and will not be announced with the Act. However the articles and recitals of the GDPR are to be used in the interpretation of the Act. As explained under point 1.4.14 in the common commentary abovem this Act aims to a legal position on the Faroe Islands that is close to the legal position in the EU.

3.1. Comments to the specific articles

Chapter 1

Material scope, territorial scope etc.

Chapter 1 on Material scope, territorial scope etc. substatively correspond to Chapter 1 in GDPR.

See also recitals 1-14 in GDPR.

Subject-matter and objectives

Article 1
Article 1 substatively corresponds to article 1 in GDPR and sets out the objective of this Act.

It is proposed to broaden the objective somewhat compared to Article 1 of the current Act which sets out to provide the individual data protection.

The broadening entails that the objective of the Act is to set out rules on the protection of the individuals data, including protection of the individuals fundamental rights and freedoms, and to set out rules on the free movement of personal data.

It is therefore set out that the Act has two purposes. With these objectives the Act takes into account both the protection of the induvidual and the information society and the internationalization, including the importance for the individual and the society that personal data can be moved freely.

See also recital 14 in GDPR.

Material scope
The material scope proposed in this Act is the same as the scope in Article 2 of the GDPR and also within the limits set out in Articles 85 and 86 of the GDPR.

On material scope see also recitals 15-21.

Article 2

[1]This is an unauthorised English translation of the special commentary to the Draft Data Protection Act put forward in the Parliament on 21 December 2019. Subsequent changes made in the Parliament to Articles 4 (2), 36 (2), 43 (1) and (2) and Article 81 are not reflected in this version of the commentary.

It is proposed that the Act has the same broad material scope as the current Act, cfr. Article 3 of the current Act. This entails that the Act will apply to all processing of personal data. This means that the Act will cover processing which in whole or partly is by automatic means and other non-automatic processing of personal data, which is or are intended to be part of a filing system.

The reference to *automatic* processing is to be understood the same way as *electronic* processing in the current Act.

With this scope the Data Protection Act will – as is the case today – apply to all processing of personal data. This means that the Act applies horisontaly covering many different areas of law. See also point 1.4.1. of the common commontary above.

The broad scope entails that the Act also covers processing of personal data which takes place through video devices. The use of video devices is also covered by Act no 278 from 9 June 1982 on the prohibition of video surveillance in the private sector.

Article 3
As is the case with Article 3 (2) of the current Act, Article 3 (1) proposes that the new Act shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. This corresponds with Article 2 (2), litra c of the GDPR.

The reason for excluding this processing from the scope of the Act is that the need for data protection is not the same when the processing is for purely personal purposes.

The socalled household exemption entails that personal correspondance, an adressbook, an electronic family diary ect. As a staring point will not be covered by the Act.

Accoring to recialt 18 of GDPR also social networking can be covered by the exemption if the social networking is undertaken within the context of personal or household activity. This entails as a starting point that a person who has a private and closed profile on a social netword, e.g. Facebook, will not be covered by the Act when posting etc.

In *Paragraph 2* it is proposed that processing of personal data in the parlamentary work in the Parliament (Løgtingið) shall not be covered by this Act. This exemption covers the political preparations in the plenary and the parlamentary committees. The Act will still cover other work in the parliament, e.g. the administration.

The current Act applies to all work in the Parliament; although the Parliament to a certain extent is excempten from the obligation to notify. The reason for changing the scope is that the political discussions in the Parliament should be able to take place unobstructed and without unneccisary restrictions for the democraticly elected members of parliament.

In *Paragraphs 3 and 4* Article 6 in the current Act is proposed to continue. The Paragraphs balance the right to data protection and the freedom of speech, as laid down in Article 10 of the European Human Rights Convention. The paragraphs entail that processing of personal data which takes place exclusively for artistic, literary or journalistic purposes and the processing of personal data in information databases for journalistic purposes are excempted from the scope of the Act. However

even with the exemption Articles 41, 42 and 47 apply as well as Chapter 8, including Article 77 on compensation.

Article 4
Article 4 sets out – the same as Article 4 of the current Act – that 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.

The Data Protection Act will apply to all processing of personal data without regard to legal area. This means that the Act will apply horisontaly covering many different legal areas. See also point 1.4.1. of the common commentary.

The Data Protection Act does not exclude specific rules on the processing of personal data. When specific rules are made, the rules should always be within the framework set out by this Act. The means that the general principles always should be followed.

This entails also that is is possible in other legislation to specify the rules in the Data Protection Act – e.g. specify to which extent the principles are followed, set out a legal obligation, to specify how to fullfill the information obligation in specific areas etc. – ort o give the data subject a higher protection or better legal position than provided for in this Act, e.g. a broader information obligation or restriction on when data can be processed. However as a starting point is should not be deviated from the principles in Article 7 if this entails a worse legal position for the data subject.

If the data subject gets a better legal position is a case by case assessment. Article 4 therefore does not entail that it is not possible to make exemptions from the Data Protection Act if an overall assessment provides that the legal position of the data subject would become better.

It should be noted in this assessment that the Data Protection Act sets out rules on when personal data *can* be processed. Sector specific legislation often lays down rules on legal obligations to process personal data.

If deviations from the Data Protection Act are made in sector specific legislation, it should always be explained in the commentary why it is necessary to deviate and how this affects the data subject.

Territorial scope

Article 5
The proposal is based on Article 3 of the GDPR. The proposal mainly corresponds to Article 7 in the current Act.

Accorting to *Paragraph 1* the Act applies to the proccessing of personal data by a private or public data controller or data processor established on the Faroe Islands, regardless of whether the processing takes place in the on the Faroe Islands.

As is the case today, the Act will be restricted to only apply to public authorities under the home rule. This entails that the Act does not apply to public authorities under Danish rule, e.g. police and courts even though they are established on the Faroe Islands. See also point 1.4.12. and 1.4.13. in the common commentary above.

Compared to the current Act the word “established” is used in stead of “run business”. To be establish should be interpreted as it is in EU-law and coveres all effective and real exercise of activity through stable arrangements. The notion continues to be interpreted and the requirement is not hard to fulfill.

Whether a data controller or data processor is established in the Faroe Islands is a concrete assessment in each case.

Compared to the current Act the scope is broadend in order to cover also data processors who are established on the Faroe Islands even though the data controller is not established in the Faroe Islands.

In *Paragraph 2* the territorial scope is changed a little compared to the current Act. It is proposed that the Act – in addition to the scope in Paragraph 1 – also applies to prossessing of personal data about data subjects who are in the Faroe Islands, even when the processing is done by data controllers or processors who are not established in the Faroe Islands.

Paragraph 2 is not dependant on place of recidence. It is enough that the data subject is in the Faroe Islands.

Paragraph 2, *subsection 1*, covers the offering goods or services to data subjects who are on the Faroe Islands, regardless of whether payment from the data subject is required. This assessment should include whether the data controller or processor directly contacts data subjects in the Faroe Islands. It is not enough that the data controller or processor has a website which is accessible from the Faroe ISlands and that people in the Faroe Islands can write to a informed e-mail adress.

Paragraph 2, *subsection 2* covers the monitoring of the behaviour of data subjects insofar as their behaviour takes place on the Faroe Islands. This covers especially monitoring on the internet with the aim to profile a person in order to assess preferences etc.

See recitals 23 and 24 in the GDPR on how to interpret the scope.

The perpose of the change in the territorial scope is to ensure that the level of protection for each data subject in the Faroe Islands does not rely on whether the controller, processor or means of processing are on the Faroe Islands.

The main content of Article 7 (3) and (4) in the current Act on representitives is moved to Article 40 of this proposal. See special commentary to that Article.

See also recitals 22-25 in the GDPR.

Definitions

Article 6
It is proposed to have an article with definitions primarily based on Article 4 in the GDPR, although only definitions relevant in a faroese context are in the draft. Although not all definitions in GDPR

are in the draft Act, these defenition may be used in interpretations if relevant. See also recitals 26-37 in GDPR.

Many if the notions defined can also be found in Article 2 of the current Act. To the extent possible it has been chosen to use the same wordings. The assessment is that the new definitions in GDPR – al though being more detailed – do not in essence change current law. This entails that it will be possible to a certain extent to use pratice under the current law when interpreting the notions defined.

The following definitions are proposed:

No. 1: Personal Data
The definition of personal data – as is Article 2 (1) in the current Act – very broad and includes all information, which can be linked to a natural person.

The definition should be understood in accordance witg Article 4 (1) in GDPR and covers all information relating to an identified or identifiable natural person.

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

It is not a lot of information required in order for an individual to be directly or indirectly identified. Also information, which is conditioned on knowledge of national identification number, registrationnumer etc. are personal data.

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly. See also recital 26 in GDPR.

The Act covers only persons who are alive. Information on dead persons are only covered by the definition if the information can be linked to a living person, e.g. in information on a dead person disclose information on inheritable deceases.

The definition covers only natural persons and therefore not legal persons.

No. 2. Processing
It is proposed to use the same wording as Article 2 (2) in the current Act. Also this definition is broad and includes any processing of personal data.

In accordance with Article 4 (2) in GDPR the definition covers any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The reference to *automatic* processing in the definition is to be understood the same way as *electronic* processing in the current definition.

No. 3. Profiling
The definition is new and is based on Article 4 (4) in GDPR.

In recital 71 it is explained how this notion is to be understood. The defenition is of special importance – and should be read in conjunction with – Article 35 on automated individual decision-making including profiling. See the special commentary to Article 35.

No. 4. Pseudonymisation
The definition is new and is based on Article 4 (5) in GDPR.

When pseudonymisation is used in this proposal, it is often as an example of a security measure that the controller can apply. Pseudonymisation essentially means that it is not possible for unauthorized persons to identify a data subject without appling extra information. Pseudonymisation thereby increases the level of protection for the individual.

No. 5. Filing system
The definition is based on Article 4 (6) in GDPR. At the same time it is proposed to use the same wording as Article 2 (3) in the current Act with linguistic adjustments

There are no substative changes intended compared to the current Act and the definition should be read in conjunction with Article 2 (3) in the proposal, which entails that the Act – in addition to covering automatic processing – also covers non-automatic processing of personal data, which form part of a filing system or are intended to form part of a filing system.

No. 6. Controller
The definition is based on Article 4 (7) in GDPR.

This is a very important notion in data protection legislation. Except for minor linguistic changes it is the same definition as Article 2 (4) in the current Act.

The controller is the one which towards the data subject and others has responsibility for the processing, who is in control of the personal data and who decides how the data should be processed.

There can be more than one, who has the responsibility for the processing, and in such a case they are joint controllers. See also the special commentary to Article 39.

No. 7. Data processor
The definition is based on Article 4 (8) in GDPR.

Except for minor linguistic changes it is the same definition as Article 2 (5) in the current Act.

A processor does not process personal data for own purposes, but on behalf of the controller, who also has the responsibility towards the data subject.

No. 8. Third Party
The definition is based on Article 4 (10) in GDPR.

Except for minor linguistic changes it is the same definition as Article 2 (6) in the current Act.
No. 9. Recipient
The definition is based on Article 4 (9) in GDPR.

Except for minor linguistic changes it is the same definition as Article 2 (7) in the current Act.

The definition is of special relevance to the provisions in Chapter 4 on the rigths of the data subject, e.g. the controller is obliged to inform of recipients, cfr. Article 23 (1), subsection 5, as well as to inform recipients of rectifications etc. of personal data according to Article 30.

The provison on public authorities entails that authorities that receive personal data in order to reply specific inquiries shall not be regarded as recipients

This is especially relevant in the context of communication between authorities, when authority (A) in order to perform it's tasks, has the need for information from another authority (B). In the inquiry to authority B, authority A discloses personal data (e.g. name and birthday) in order to receive general information about a specific area or specific information on the data subject. In this example authority B would not be a recipient.

A *specific inquiry* can be e.g. an inquiry about an individual. These inquiries should always b ein writing and reasoned and should not cover a whole filing system etc. This covers also only inquiries, which are occasional.

See also recital 31 in GDPR.

No. 10. Concent of the data subject
The definition is based on Article 4 (11) in GDPR.

Personal data can be processed if the data subject has concented. Concent is the only basis for processing which is defined.

Consent from the data subject is also defined in Article 2 (8) in the current Act, but the new definition sets out more strict conditions for the data subject consent, as it is of importance that the data subjetk to the extent possible has control over his/her personal data and has a sufficient basis to assess a specific processing. The data subject consent is mentioned and decribed in severeal recitals in GDPR, e.g. recitals 32, 42 and 43.

A consent should fulfill these conditions:

As it is today a consent should be a *freely given indication*, which means that the consent should be given by the data subject him/her self or by someone who has power of attorney from the data subject, and that the consent should not be given under any form of compulsion from the controller, processor or anyone else.

According to Article 7 (4) in GDPR it should be – when assessing if the consent is freely given – taken utmost account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. If this is the case, it is probable that the consent is not freely given.

Recital 43 states that a consent is not freely given if there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given.

Also in this regard the proposal should be interpreted in accordance with GDPR.

It should be noted that recital 43 does not entail that public authorities are excluded from using consent as the basis for processing. If the information is necessary for the public authority and cannot be collected any other way, the public authority may subject to a concrete assessment use consent as a basis for processing. If in doubt the public auhtority can also assess whether other grounds of processing can be used, e.g. Article 8 (1), subsections 3 or 5.

When the consent should be an *indication* from the data subject, where the data subject by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, means that it is not possible to consent tacitly or indirectly.

The consent should also be *specific and unambigous* which means that no doubt shold be that the consent is given, to whom it is given and which processing the consent is given for.

Consent should also *informed* which means that the individual consenting should have gotten as much informtion that he or she is fully aware of what the consent covers, including the consequenses of consenting.

As is the case under the current Act there are no formal requirements applicable to the consent, which can therefore be given orally, in writing, electronicly etc. The burden of proof that the consent is given still remains with the controller who should ensure documentation. See also special commentary to Article 9 which lays down conditions for consent.

No. 11 and 12. Genetic data and biometric data
The definition is based on Article 4 (13) and (14) in GDPR.

It is new that genetic data and biometric data are defined. It is also new that these types of data specifically are regulated in the data protection Act.

According to Article 11 these data are considered sensitive which entails that processing as a starting point is forbidden. Please see special commentary to Article 11.

See also recitals 34 and 51.

No. 13. Data concering health
The definition is based on Article 4 (15) in GDPR.

The definition covers information on all current, future and past physical or mental health issues of a person, including information on abuse of medicine, drugs, narcotics, alchohol and other stimulants.

Data conserning health should be interpreted broadly and covers all matters relating to the physical or mental health status of the data subject.

As it is today, data concerning health are considered sensitive and processing as a starting point is forbidden. See also the special commentary to article 11. It is new that data concerning health is defined.

See also recital 35 in GDPR.

No. 14. Foreign country
It is proposed that the definition of foreign country is changed compared to the current Act. In the current Act "foreign country" covers all other countries than Faroe Islands, including Denmark and Greenland.

It is proposed that foreign country should mean a country which is a member of the European Union (EU) or the European Economic Area (EEA).

The reason for the change in the definition is that a different system is proposed compared to the one in the current Act, when it comes to transfer of personal data from the Faroe Islands to other countries.

The definition therefore is important for the rules on transfer of personal data to other countries, cfr. Chapter 6. Please see point 1.4.8. in the common commentary and the specific commentary to the provisions in Chapter 6.

No. 15. Third country
The definition should be read in conjunction with the definition of foreign country in Article 6 (14). Third country means a country which is not a member of the European Union (EU) or the European Economic Area (EEA).

Also this definition is important to the rules on transfer of personal data to third countries in Chapter 6. Please see point 1.4.8. in the common commentary and the specific commentary to the provisions in Chapter 6.

No. 16. Information society service
The definition is based on Article 4 (25) in GDPR.

The definition is new and is especially relevant when interpreting and using Articles 10 and 28 (1), subsection 6. The service being at a *distance* means that it is provided without the parties being simultaneously present.

By *electronic means* means that the service is sent initially and received at its destination by means of electronic equipment for the processing and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means

At *the individual request of a recipient of services* means that the service is provided through the transmission of data on individual request.

Information society services covers e.g. online games and social media, such as Faceboo, Snapchat and Instagram. Public digital services, such as Mín-boks (My-box), are usually not considered to be information society services covered by this definition.

Chapter 2
Principles and lawfullness of processing

Chapter 2 on principles and lawfullness of processing substatively correspond with Chapter 2 in GDPR.

Chapter 2 has the most fundamental and important rules on the processing of personal data.

Principles on the processing of personal data

Article 7
An article is proposed on the principles of processing of personal data which is based on Article 5 in GDPR and which also for the most part corresponds with Article 8 in the current Act.

When personal data is process it is a precondition that the principles in Article 7 are being followed.

Compared to the current Act, it is proposed that the principles in Paragraph 1 are formulated in more detailed. In headlines the principles are the following:

1) Lawfulness, fairness and transparency
2) Purpose limitation
3) Data minimisation
4) Accuracy
5) Storage limitation
6) Integrity and confidentiality

No. 1. Lawfulness, fairness and transparency
The proposal to provide that personal data should be processed lawfully and fairly essentially compares to current law, which provides that personal data should be processed lawfully and in accordance with good data protection practices. The requirement to process personal data in accordance with good practices is also covered by the new proposal, and this will continue to be a requirement which is to be detailed by the Data Protection Authority.

As something new it will be provided that personal data shoud be processed in a transparant way for the data subject. This is a part of the a main object of the revision of the data protection legislation that the data subject has more control over personal data about him/her and that the data subject knows what the personal data are used for.

In recital 39 it explained that the requirement entails e.g. that it should be transparent to the data subject that personal data concerning him/her are collected, used, consulted or otherwise processed

and that the principle also requires that any information relating to the processing of the personal data be easily accessible and easy to understand.

No. 2. Purpose limitation
The principle of purpose limitation is a fundamental rule in data protection legislation.

The principle of purpose limitation entails that personal data should be collected for specified, explicit and legitimate purposes and that collected personal data cannot freely be processed for other purposes, than those for which they were collected.

That the purpose should be specified and explicit means that the controller should have a clear purpose when the personal data are being collected. It is not enough to inform that the personal data are being collected for "administrative purposes" or "commercial purposes". The requirement also means that the controller cannot collect personal data that he or she does not need right now, but may need at a later time.

A legitimate purposes entails that an authority or a private company may collect personal data for the purpose of performance of a task which is within the authority's or company's scope of business.

A part of the purpose limitation principle is limiting further processing. Further processing is processing which comes after the original processing for with the personal data were collected.

Article 8 (1), subsection 2 in the current Act provides that further processing of personal data should be *compatable* with the original purpose. This wording is more strict than the previously applicable Danish legislation which provided that further processing to be *incompatible* with the original purpose (danish text: "*ikke [må] være uforenelig med disse formål"*).

When reading the commentary to the current Act it is not clear whether it was intentional that the faroese wording (*compatable with*) should be more strict compared to the Danish wording (*not incompatible with*). The different wordings have however led to different interpretations of the principle of purpose limitation on the Faroes and in Denmark.

It is proposed to change this part of the purpose limitation so that it be worded as in GDPR (and previously applicable Danish legislation). THis means that it is provided that the personal data can only be collected for specified, explicit and legitimate purposes and that the personal data not be further processed for purposes incompatible with these purposes.

The change in the wording entails that the requirement is slackend a little bit compared to the current wording. However this does not entail any disadvantages for the data subject.

Whether a further processing is incompatible with the original purpose is a case by case assessment.

Regardless of this limitation it will in most cases in pratice be possible to process personal data for other purposes than the one for with they were originally collected. However the purpose limitation principle sets out limits for this further processing. For example personal data may not be freely

disclosed between public auhtorities, even if this means that several auhtorities will have to collect the same personal data from each data subject.

Article 6 (4) in GDPR has example elements the controller should take into account when assessing whether a further processing is compatible with the original processing. The provision could be used as guidance in the assessment that is to be made according to Article 7 (1), subsection 2.

When the further processing is not based on the data subject's consent or on law GDPR provides that the controller should take into account, inter alia:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller
- the nature of the personal data, in particular whether sensitive data are processed
- the possible consequences of the intended further processing for data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Further processing should – in addition to fulfill the principles of processing – fulfill the other requirements in the proposes Act, including have a basis for processing.

Regarding further processing for historical, statistical or scientific purposes, please see the special commentary to Paragraph 3 below.

No. 3. Data minimisation
The provision corresponds with Article 8 (1), subsection 3 in the current Act and entails that the amount of personal data being processed should always be as little as possible to reach the purpose of the processing.

No. 4. Accuracy
With linguistic adjustments the provision corresponds with Article 8 (1), subsection 6 in the current Act and entails that the controllers should ensure that the personal data being processing is accurate and kept up to date.

With the reference in the second sentence that personal data which is *inaccurate* should be erased or rectified there is no intention to change pratice according to the current Act, which states that personal data which is *inaccurate or misleading* should be erased or rectified. Misleading is covered by inacurrate.

In the current Act it is provided that personal data is to be rectified or erased *without delay*, whereas the new Act provides that personal data is to be rectified or erased *at once*. This is a more strict requirement. How quickly this is will be laid down in pratice.

No. 5. Storage limitation
The proposed Article 7 (1), subsection 5, corresponds with Article 8 (1) subsection 5 of the current Act. The provision entails that personal data should not be stored longer than necessary.

To ensure that personal data are not stored longer than neccessary the controller should set out time limits for erasure or rules on review of the personal data with regular intervals to assess if and when the data should be deleted. See also recital 39 in GDPR.

In Article 5 (2) litra e in GDPR it is stated that personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the data subject. This means that personal data which are processed solely for these purposes may be stored longer than personal data processed for other purposes. This will also apply in the Faroe Islands.

No. 6. Integrity and confidentiality
The provision in Article 7 (1) subsection 6 is about security of processing and is new as a part of the general principles of data processing. The provision entails an obligation for the controller to implement appropriate technical and organizational, including physical measures, in order to have an appropriate level of security.

The fact that security is an important part of data processing is not new compared to the current Act which has detailed rules on the security of processing e.g in Article 31 and Executive order on security in relation to processing. It is however new that security of processing is a part of the main principles among other things to remind controllers of the importance of security.

As it is today, it is the responsibility of the controller to ensure that the principles of data processing are followed. It is proposed that this is stated clearly in *Paragraph 2*. At the same time it is provided that the controller be able to demonstrate the the principles are followed. How the controller ensures that he or she is able to demonstrate compliance, is for the controller to assess. The controller should however in some way document that the principles are being followed.

In *Paragraph 3* it is provided that 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. The provision for the most part corresponds with Article 8 (2) in the current Act.

Paragraph 3 ensures that personal data which were not originally collected for these purposes, may be further processed for historical, statistical or scientific purposes. It is a precondition for this further processing is *solely* for the mentioned purposes and that the disadvantages for the person whom the data relate are overridden by significant public interests.

Paragraph 3 therefore sets out that the further procecssing is in line with the principle of purpose limitation. The assessment in each processing is therefore not if the processing is compatible or incompatible but rather whether there are significant public interests that override the disadvantages for the data subject.

Paragraph 3 is not a basis for processing. Therefore there should be a basis for the processing in Articles 8, 12 or 18.

Processing for historical, statistical or scientific purposes *and* other purposes, e.g. administrative or commercial purposes, is not covered by paragraph 3.

See also recitals 39 and 50 in GDPR.

Lawfullness of processing

Article 8
The Article is based on Article 6 in GDPR.

If the principles are complied with personal data can be processed provided that the is a basis for the processing.

It is proposed that Article 8 – as Article 9 in the current Act – covers processing of all personal data. If there is no other special basis for the processing, the basis should be found in Article 8.

One processing can have several bases.

There are six bases for processing in Article 8 (1):

1) Consent
2) Contract
3) Legal obligation
4) Protection of the vital interests of the data subject or of another natural person
5) Public interest or in the exercise of official authority
6) Legitimate interests

No. 1. Consent
As it is today, personal data about the data subject can be processed, if the data subject has given his/her consent. Consent should be interpreted in line with the definition in Article 6 (10). Plese see the special commentary to Article 6 (10).

Even though it is a precondition for a valid consent, cfr. Article 6 (10), it is explicitly stated in this Article that the consent should be given for one or more *specific* purposes. This is to ensure that the data subject know what he/she is consenting to.

On conditions for consent please see also the special commentary to Article 9.

Nr. 2. Contract
The provision corresponds with Article 9 (1), subsection 1 in the current Act with linguistic changes.

The provision entails that processing is legal, if the personal data about the data subject are necessary for the performance of a contract to which the data subject is party. This could be name and address, confirmations of orders ect.

It is a precondition that the the data subject is party to the contract, and therefore a contract between the controller and for example the data subject's employer cannot be a basis for processing.

The provision covers also processing prior to entering into a contract, e.g. registration in relation to an offer of financing.

No. 3. Legal obligation
The provision corresponds with Article 9 (1) subsection 2 in the current Act.

The provision entails that personal data can be processing if this is necessary for compliance with a legal obligation to which the controller is subject.

Legal obligation covers obligations in law, executive orders with basis in law, court rulings or decisions made by public administrative athorities. Also obligations following from international rules, e.g. conventions, are covered by the wording.

As a starting point legal obligations laid down in another country's legislation are not covered. Contractual obligations are not covered eighter.

No. 4. Protection of the vital interests of the data subject or of another natural person
The provision corresponds with Article 9 (1) subsection 3 in the current Act although it has been added that processing also can take place if the processing is necessary to protect the vital interests of another natural person.

Processing to protect the vital interests means that the processing should concern interests which have fundamental importance for the data subject or the other person. An example is that the data subject due to travel or illness is not able to give consent to a processing which can save the data subject substatial financial loss or other substatial damage.

No. 5. Public interest or in the exercise of official authority
The provision is a writing in one of Article 9 (1) subsections 4 and 5.

Public interest means that the interest shall be of common interest, which means that is should be of importance for a wide group of people. This can e.g. be processing with historical, scientific or statistical purpose. Also processing in legal information systems with the purpose of informing about legsislation, court decisions etc. can be covered. Also other processing can be in the public interest, e.g. registration of information within bigger private organisations, which have the interest of a wide group of people.

Even if a processing has a commercial purpose, if can also be in the public interest.

Personal data can also be processed if the processing is necessary for the exercise of official authority vested in the controller.

The provision covers all public authorities governmental and municipal and for the most part if the processing is in connection with decisions, such as decisions regarding social benefits or decisions about taxes. It is however not only processing in connection to specific decision which are covers. All administrative processing is covered.

The change of wording about the exercise of official authority so that there is no longer a referance to *"or a third party to whom the personal data are disclosed"* is not considered to be of importance compared to current law. The exercise of official authority may still be executed by a (private) third party to whom the personal data has been disclosed. Disclosing the information to the third party is often in the public interest.

No. 6. Legitimate interest
The provision corresponds with Article 9 (1), subsection 6 in the current Act with linguistic changes.

The provision entails that the controller or a third party may process personal data if this is necessary in order to pursue a legitimate interest and these interests are not overridden by the interests of the data subject. This is especially relevant if the data subject is a child.

The provision entails that there is a case by case assessment where the interests of the controller are to be weighed up against the data subject's interests.

The controller and the third party can exercise the legitimate interests of other persons. It is a precondition that the interests are legitimate to this person.

In Paragraph 2 it is proposed that it is not possible for public authorities to process personal data on the basis of Article 8 (1), subsection 6.

This is a change compared to the current Act, and the reason is that public auhorities should only process personal data on the basis of legislation, cfr. Article 8 (1) subsection 3, or in the exercise of of official authority, cfr. Article 8 (1), subsection 5, and not on the basis of a case by case assessment of legitemate interests. See also recital 47 in GDPR.

This change is not assessed to limit the processing of public authorities in pratice, as it is seldom that public authorities today process on the basis of legitimate interests.

See also recitals 40 and 41 and 44-49.

Conditions for consent

Article 9
The provision is based on Article 7 in GDPR. A similar provision is not in the current Act, although consent – as it is in this proposal – is defined.

Paragraph 1 provides 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.

The provision does not have any formal requirements and does therefore not require the consent to b ein writing. However the provision provides that it is completely clear that the burden of proof lays with the controller. It would therefore be sensible for the controller to document that the consent is given.

In Paragraph 2 it is proposed how to handle situations where the data subject's consent is given in the context of a written declaration which also concerns other matters

It these cases 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. This is to ensure that the data subject knows that he or she is consenting to the processing of personal data and what this processing is about. A declaration which constitutes an infringement of the conditions in this Act shall not be binding for the parties.

As it is today it is proposed in Paragraph 3 that the data subject shall have the right to withdraw his or her consent at any time. This does not affect the lawfulness of processing based on consent before its withdrawal.

A processing can have several bases for processing at the same time. If a processing is based on consent, but the processing from the start also can be based on another basis, the processing can continue with this other basis if the consent is withdrawn.

It is also possible to continue a processing if it at the time of the withdrawal is another (new) basis for the processing. See also Article 28 (1) subsection 2 in the proposal.

In Paragraph 4 there is a new requirement that the data subject prior to consenting should be informed of the right to withdraw the consent. It is also provided that it should be as easy to withdraw as to give consent

See also the special commentary to Article 6 (10) and recitals 42 and 43 in GDPR.

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

Article 10
The provision is based on Article 8 in GDPR.

This is a new provision concering the processing of personal data of children in relation to information society services.

The provision does not concern contractual law as such or the question when children or young people can legally act, e.g. when they can enter into agreements or make decision about their possessions. The provision is only applicable to processing of personal data and information society services.

Information society services is to be understood in line with the definition in Article 6 (16). Information society services covered by Article 10 are e.g. social media (Facebook, Snapchat etc. but also local school-intranets could be covered), online games and e-commerce of different sorts.

In Paragraph 1 it is proposed a processing of personal data of a child – in relation to the offer of information society services directly to a child – based on consent shall be lawful provided the child is at least 13 years old.

This entails that it will not be as it is today a case by case assessment if the child is mature enough to consent to a processing of personal data when it comes to information society services.

In Paragraph 2 it is provided that 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 Paragraph 2 it is also proposed that the controller – when the child is younger than 13 years of age – shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child. The controller should take into consideration available technology. If the controller has made sufficient efforts is a case by case assessment.

It is not specifically provided which efforts the controller should tak ein order to verify that consent is given or authorised by the holder of parental responsibility over the child. This will be specified in practice by the Data Protection Authority.

In Article 40 (2), litra g, in GDPR it is encouraged that the requirements for controllers in Article 8 be specified in socalled codes of conduct which associations and other bodies representing categories of controllers or processors may prepare. When these codes of conduct are prepared the Data Protection Authority may – to the extent relevant – include this in the work with specifying Article 10.

The provision in Article 10 is based on Article 8 in GDPR although the age mentioned in Article 8 in GDPR is 16 years. It is however possible for the EU Member States to set a lower age limit. It is proposed that the age limit be 13 years old which is the same as in Denmark.

The reason for proposing an age limit of 13 is that children in the Faroe Islands – as is the case in Denmark – are used to being on the internet and social media. The access to information and participation in online-activity has great societal and social importance for children, and gives them the possibility to have and hold on to friends, participate in online discussions, search for information for school, play games and listen to music etc. If the age limit is to high, this may lead to either exclusion from information society services because the parents will not consent, ort o children lying about their age.

Although the age limit in Article 10 is 13 years it should be noted that the Data Protection Act lays down general conditions for controllers and processors. The controller and processor should have a risk based approach to security of processing which means that the requirements for security of processing are especially strict when processing personal data about children. Please see point 1.4.2. in the general commentary.

According to recital 38 consent from the holder of parental responsibility over the child is not necessary – even if the child is below the age of 13 – in the context of preventive or counselling services offered directly to a child. This means that the child has the possibility to get counselling about alchohol abuse or mental problems without the consent from the holder of parental responsibility.

See also recital 38 in GDPR.

Processing of sensitive personal data

Article 11
The Aricle is for most part based on Article 9 (1) in GDPR.

It os proposed to list in Article 11 which personal data are to be considered sensitive. The starting point is that processing sensitive personal data is prohibited. The conditions for processing sensitive personal data are more strict than the conditions for processing other personal data, cfr. Article 8.

In *Paragraph 1* there is an exhaustive list of personal data which are considered sensitive.

It is proposed that the personal data listed in Article 2 (9) in the current Act as senstive, also in the new Act are to be considered sensitive. In addition also genetic data and biometric data are listed as sensitive.

It is noted that there is a lingusitic change as it in the current Act is stated that information on *colour and ethnic origin* is considered sensitive personal data. This is no doubt a translation of the words (Danish:) *racemæssig og etnisk baggrund* (in English *racial or ethnic origin*). It is considered more correct to change this to *racial or ethnic origin*.

Holding on to the categorization of sensitive data as it i sin the current Act entails that the provision is not identical with Article 9 in GDPR, as this Article does not cover *data concerning criminal convictions and offences, material social problems* and *other purely private matters*.

Becasue GDPR is a total harmonisation of data protection legislation in the EU, it is not possible for the EU-member stats to provide in national law that other personal data than data mentioned in Article 9 (1) shall be considered sensitive. Faroese legislation is not bound by this, and therefore it is proposed that also data concerning criminal convictions and offences, material social problems and other purely private matters as is the case today, shall be considered sensitive and covered by Article 11.

This entails a higher level of protection for the data subject than provided for in the EU – becasue the conditions for processing are more strict – without reducing the free flow of information notably. Therefore it is not considered that this will influence the faroese adequacy decision negatively, cfr. points 1.2.8 and 1.2.9 in the generel commentary.

Below you will find a description of sensitive personal data.

Personal data revealing **racial or ethnic origin** covers e.g. information on race and decent.

Information on nationality or name is normally not considered to be sensitive even if this information in some cases may reveal information on racial or ethnic origin.

Political opinions covers political convictions and points of view and covers more than just party political affiliation. If an association is considered political, a membership in this association may reveal political views of the members. This has to be a case by case assessment.

Religious beliefs covers information about the data subject's religion – no matter what this religion is. What is stated above about membership in a political association, is also applicable to membership in a religious association.

Philosophical beliefs covers different philosophical points of view.

Trade union membership covers membership in a trade union, while information that a person is not a member of a trade union is not covered by Article 11.

Genetic data covers 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.

Biometric data covers 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.

Data concerning health covers information on all current, future and past physical or mental health issues of a person, including information on abuse of medicine, drugs, narcotics, alchohol and other stimulants.

Data concering health is to be interpreted broadly and covers all data related to the physical or mental health of a natural person.

Information revealing that a person is sick or on sick leave without disclosing what kind of sickness the person suffers from is however as a starting point not covered by Article 11.

See also recital 35 in GDPR.

Information on a natural **person's sex life or sexual orientation** covers e.g. information on sexual activity and prefrerances and information on homosexuality.

Data concerning **criminal convictions and offences** is to be interpreted broadly and covers any law infringement which has or could result in punishment regardless of whether punishment has been imposed in the specific case. Also other consequences than punishment, such as deprivation of the right to operate an activity is covered.

Information that a person is or has been suspected of a criminal offence, is charged, accused or convicted of an offence is covered. However the provision is not to be understood in a way that it covers every notification to the police. For notifications to the police to be covered, they should in some way be substantiated.

Information on **material social problems** covers information such as serious disputes between married couples or between parents and children, information that a person has been in an accident with material personal or social consequences, information on lengthy unemployment or information that a person for a lengthy period has been on public welfare.

Information on **other purely private matters** covers separation, application for divorce, adoption and family disputes etc.

Information not covered directly by the above, but where the context discloses further information, e.g. if a data subject's address is in a mental health institution, then this information is also sensitive (in this case health information).

As a starting point processing of the mentioned personal data is prohibited. However in Paragraph 2 it is stated that processing can take place if the conditions in Articles 12-14 or 18-19 are complied with. A basis for processing should therefore be found in one of these articles.

Article 12
The provision in bases on Article 9 (2) in GDPR. A similar provision is in Article 10 in the current Act.

Article 12 provides when sensitive personal data covered by Article 11, can be processed.

In addition to a legal basis for the processing, processing of sensitive data should always comply with the general principles for processing in Article 7.

According to *Paragraph 1* sensitive personal data can be processed in the following cases:

1) Explicit consent
2) Authorised or laid down in law
3) Carrying out obligations and exercising specific rights in the field of employment
4) Protection of the vital interests of the data subject or of another natural person
5) Foundations, associations or any other not-for-profit body
6) Personal data which are manifestly made public by the data subject
7) Legal claims
8) Medical diagnosis etc.

No. 1. Explicit consent
It is proposed that the data subject – as is the case for regular personal data, cfr. Article 8 (1) subsection 1 – can consent to the processing of sensitive data.

When Paragraph 1, subsection 1 states that the data subject should give an explicit consent this does not – as a starting point – set out more strict conditions than to the consent required in Article 8 (1), subsection 1. Consent is defined in Article 6 (10) and should in all cases be *explicit* in order to be a legal basis for processing.

The reference in Paragraph 1, subsection 1 to the *explicit* consent of the data subject is however an extra reminder that in these cases there should not be any doubt that the data subject has consented to the processing.

If the law provides that the prohibition to process sensitive data may not be lifted by the data subject, the basis for processing in Article 12 (1) subsection 1 cannot be used.

No. 2. Authorised or laid down in law
It is proposed that it should still be possible to process sensitive personal data if this is authorised or laid down in law.

That the processing be authorised or laid down in law means that the processing should follow from legislation.

The legal basis entails that the Parliament and Government can decide and make it very clear that it is possible to process sensitive data for certain purposes.

While the Data Protection Act sets out when personal data *may* be processed, sectorspecific legislation often lays down that personal data *should* be processed for some specific purpose. It is important that appropriate measures are taken in order to protect the data subject in these cases. See also the special commentary to Article 4.

No. 3. Carrying out obligations and exercising specific rights in the field of employment
The provision is essentialy equivalent to Article 10 (1) subsection 8 in the current Act and entails that sensitive personal data can be processed if the processing is necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment.

Obligations and specific rights is to be understood broadly and includes all obligations and specific rights vested in the controller or of the data subject in the field of employment.

Obligations and specific rights can follow from legislation or collective agreements in the field of employment. It is therefore possible to process sensitive personal data if this is laid down in a collective agreement if the processing is necessary to comply with obligations and exercising specific rights in the field of employment.

No. 4. Protection of the vital interests of the data subject or of another natural person
The provision is equivalent to Article 10 (1) subsection 3 in the current Act and can be used if the data subject due to illness or other weakness, such as dementia, mental issues or unconsciousness is not able to consent to a processing.

The provision cannot be used if there is someone who is able to give consent on the part of the data subject. See the special commentary to Article 8 (1) subsection 4 about vital interests.

No. 5. Foundations, associations or any other not-for-profit body
The provision is essentialy equivalent to Article 10 (2) in the current Act and entails that foundations, associations or any other not-for-profit bodies under certain conditions can process sensitive personal data about members, previous members or persons who have regular contact with it in connection with its purposes.

The provision covers non-profit foundations and associations who have a public interest, e.g. an associations of people who have common interests or views in the field of religion, philisofy or politics. The provision also covers associations of patients, such as the Cancer Association, Aphasia Association and political youth associations or parties and trade unions.

The reference in the proposed provision that the f*oundations or associations should be non-profit will not entail a change in pratice.*

As it is today the personal data can only be processed within the association and only for a limited group of people. Personal data cannot be disclosed on the basis of this Article. Disclosing personal data should be on the basis of consent.

No. 6. Personal data which are manifestly made public by the data subject
There is not the same need for data protection if the data subject has made the sensitive personal data public and in these cases the personal data can be processed on the basis of Article 12 (1) subsection 6.

Information is made public if a broad group of people has come to know the information, e.g. if the information is rendered on television, radio, news papers, web sites etc. It is not enough that the controller knows that some personal data are intended to be disclosed to the public. The data subject shall himself/herself have taken steps to make the information public.

Disclosing information on social media, such as Facebook, Twitter or Instagram is also a publication coveres by Paragraph 1, subsection 6, if everyone can access the information. If the personal data are posted in a closed group where a limited number of people have access, the information is not made public.

No. 7. Legal claims
The provision is equvivalent to Article 10 (1) subsection 5 in the current Act.

Legal claims should be understood broadly and covers financial, legal etc. claims from the data subject, the controller or third parties.

Examples are processing of health information by social authorities in order to assess whether the data subject has the right to social benefits, or the processing of health information by insurance companies in order to assess whether the data subject has the right to compensation.

Also processing of personal data by public authorities in the exercise of official authority could be covered. For example when social authorities suspect incest or other sexual abuse of children and contact other authories such as hospital, police etc. in order to protect the children.

The provision also coveres processing of personal data if the processing is necessary in order for the controller to assess whether a claim can be made towards the data subject. The provision also covers processing necessary in order for legal claims of third parties to be established, exercised or defended, e.g. if courts are to process personal data of other data subjects than the parties to the case.

No. 8. Medical diagnosis etc.
With linguistic changes the provision is equivalent to Article 10 (7) in the current Act.

As it is under the current law the legal basis for processing is conditioned that the processing is by a health professional subject under law to the obligation of professional secrecy. The obligation of professional secrecy can be laid down in Chapter 9 in the Health Act and Articles 152 and 152a-f in the Criminal Code.

Processing subject to Article 12 does not require prior authorisation from the Data Protection Authority.

In *Paragraph 2* it is proposed to partially continue with Article 10 (3) in the current Act. The processing of sensitive personal data can therefore take place if processing is necessary for reasons of substantial public interest.

Compared to the provision in the current Act, it is proposed that only private controllers should require prior authorisation from the Data Protection Authority. Public authorities may therefore process on the basis of this provision without prior authorisation.

The provision is resuduary and has a narrow scope and can therefore only be used in exceptional cases. This applies to both public and private controllers.

In Paragraph 3 it is proposed that the competent minister in consultation with the minister responsible for data protection may lay down rules on the processing of sensitive personal data. These rules should provide sufficient guarantees for the rights and interests of the data subject.

The authority to lay down rules should only be used in special cases. The fact that the minister responsible for data protection is to be consulted entails a standardized practice.

The legal bases in Paragraphs 1 and 2 will be defined more narrowly in the case law of the Data Protection Authority. The Data Protection Authority will also provide guidelines where relevant.

It should be noted that in some areas there is already practice on consent which the Data Protection Authority should take into account in guidelines on consent. This is e.g. the case in the field of research, where the relevant authority (Vísindasiðsemisnevndin) approves the wording of consents to be used in research projects.

On sensitive personal data please see also recitals 51-56 in GDPR.

Processing of personal data relating to criminal convictions and offences

Article 13
The provision is based on Article 10 in GDPR.

It is proposed that data concerning criminal convictions and offences as is in the current Act are sensitive personal data. See special commentary to Article 11 (1) above. It is however new that there is a specific article on the processing of these data.

The starting point is that the basis for processing of personal data on data concerning criminal convictions and offences should be found in Article 13 which lays down more detailed conditions for processing.

In *Paragraph 1* it is proposed that personal data relating to criminal convictions and offences may be processed on behalf of a public authority, if such processing is necessary for the performance of the tasks of the authority.

In Paragraph 2 the conditions for disclosing personal data relating to criminal convictions and offences by public authorities are laid down. Paragraph 2 covers disclosing information to both other public authorities and private parties.
It is proposed in Paragraph 3 that private controllers in certain cases may process personal data relating to criminal convictions and offences. The starting point is that private controllers may only process this information if the data subject has given explicit consent. This legal basis may for instance be used in cases of hiring employees.

If the data subject has not consented to the processing of the data, processing may take place if necessary for the purpose of safeguarding a legitimate interest and this interest clearly overrides the interests of the data subject. This legal basis has a very narrow scope and can only be used in extraordinary cases. The legal basis can for example be used if a private company, e.g. a store, registers personal data in connection to theft for the purpose of filing a police rapport.

Paragraph 4 lists the conditions for private controllers disclosing personal data relating to criminal convictions and offences. This basis is – as is the basis for processing the data – very narrow.

In Paragraph it is proposed that processing of personal data relating to criminal convictions and offences may take place if the conditions in Article 12 are fulfilled. This is in order to make it clear that processing may take place if there is a legal basi sin Article 12, e.g. if the processing is authorised or laid down in law, cfr. Article 12 (1) subsection 2.

Article 14
The Article is eqivalent to Article 12 in the current Act and entails that a complete register of criminal convictions may only be kept under the control of a public authority.

This means that a private party must be under the control of a public authority to have such a register. The register must be complete in order to be covered by the provision. This means a register of all criminal convictions. Registers which only have personal data from some criminal convictions are not covered by this special provision.

Processing which does not require identification

Article 15
The Article is new and is based on Article 11 in GDPR

Paragraph 1 entails that the controller shall not be obliged to process more personal data than necessary for the sole purpose of complying with this Act. To a certain extent the provision clarifies the principle of dataminisation in Article 7 (1) subsection 4 of this proposal which can also be found in the current Act. The provision entails that a controller who processes personal data relating to a data subject without knowing the the identity of the data subject (even though he is processing personal data) 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, including the provisions on data subjects rights.

An example is a controller who receives an e-mail. The e-mailaddress is personal data but does not in every case entail that the controller knows who the sender or data subject is (for example runner1234@12345.fo). In these cases the controller has no obligation to collect further information

for the sole purpose of complying with this Act, including for the data subject to be able to use his or her rights.

This provision may be relevant for subscribtions for news letters of all sorts etc.

Paragraph 2 states that the controller if he or she 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.

This may be the case if the controller only processes information about an e-mail address, which is personal data but not enough to identify the data subject. In these cases the rules on data subject rights – appart for the obligation to inform – does not apply unless the data subject provides additional information enabling his or her identification.

See also recitals 57 and 64 in GDPR.

Chapter 3
Specific processing situations

Chapter 3 there are processing rules on specific processing situations. These are processing situations which in some way are not covered by the rules in Chapter 2 or where there is a need for special provisions in order to have a clear legal position.

Chapter 3 is based on Chapter 9 in GDPR which also has rules on specific processing situations where it in large part is left to the EU member states to lay down national rules as they see needed.

Processing of the national identification number
Processing of the national identification number has often been discussed since the National Registry with Act no. 86 from 1 June 1982 was tasked with giving people on the Faroe Islands a national identification number.

Since 1984 when the Public Registers Act and the Private Registers Act came into force and until the current Act on processing of Personal Data came into force in 2001 the national identification number was considered sensitive personal data. The conditions for processing were even more strict than processing of other sensitive personal data and the controller needed a legal basis in law in each case.

The strict rules on processing of the national identification number was one of the main reasons for the Registers Acts were revised and a new legislation came into force in 2001.

The national identification is not considered sensitive personal data in the current Act on processing of Personal Data and this will not change with the new Act.

Times have changes alot since everyone got a national identification number in the beginning of the 1980'ies. Both in regards of processing of personal data and the technical advances.

Processing of the national identification number now often takes place in digital solusions which have in common that they need to uniquly identify the user. The national identification number can

be used in these cases as the one information that can identify the user so that there is no doubt as to who the user is.

The fact that there is a system on the Faroe Islands which entails that everyone has a national identification number – which uniquly identifies every individual – allows for digital solutions using the national identification number as a basis for unique identification of the individual and thereby giving the individual access to information and services, e.g. on the internet.

In addition to making it easier for individuals to communicate with authorities and companies, e.g. banks, these solutions should ensure an appropriate level of protection which the personal identification number not in it self ensures.

Article 16
The provision corresponds with Article 11 in the current Act and lays down when public authorities and private controllers can process the national identification number. Even though the wording is the same as in the current Act the intention is that the Article be interpreted in the new context which is explained above.

According to Paragraph 1 public authorities may process data concerning identification numbers with a view to unique identification or as file numbers.

Name, address etc. can be used to identify an individual however it is always a risk that several people have the same name or live on the same address. The national identification number is unique for each individual and nobody has precisly the same number.

Public authories often use the national identification number as a key to other information about the individual.

Using the national identification number can make the administrative procedures easier and more efficient. At the same time the use gives the individual a more safe position as mistakes due to mixing people together are fewer.

A public authority can disclose the national identification number to a private controller if the private controller has a legal basis for the processing.

According to *Paragraph 2* private individuals and entities may process data concerning identification numbers if the conditions in Paragraph 2 subsections 1-4 are fulfilled. Compared with the current Act there is a little broadning of the scope.

According to Paragraph 2 *subsection 1* private controllers may process the national identification number if this this follows from law. This is to be understood as Acts by the Parliament or provisions laid down on the basis of these Acts.

If the processing follows from law is an overall assessment of the legislation. There can be cases where it is directly stated in a provision that the national identification number can be processed. There can however also be instances where processing of the national identification number is implied in a privision – or a system established by law – as a precondition. Also in these implied

cases the conclusion in a specific case may be that the processing follows from law, cfr. Paragraph 2 subsection 1.

According to Paragraph 2 *subsection 2* private controllers may process the national identification number if the data subject has given explicit consent.

As a new provision it is proposed in Paragraph 2 *subsection 3* that private controllers may process the national identification number if the conditions laid down in Article 12 are satisfied. The reason for this proposed change is that the national identification number is not considered sensitive personal data and therefore it should be possible to process the national identification number if the more strict conditions for processing of sensitive personal data are fulfilled.

According to Paragraph 2 *subsection 4* private controllers may process the national identification number if the processing is carried out solely for historical, scientific or statistical purposes.

The provisions in Paragraph 2 subsections 1-3 does not cover disclosing the national identification number. However in *Paragraph 3* it is provided in which specific cases private controllers can disclose the national identification number. The provision corresponds with a provision in the current Act.

According to Paragraph 3 *subsections 1 and 2* it is possible to disclose the national identification number if the disclosure follows from law or the data subject has given explicit consent to the disclosure. The law or consent should therefore explicitly refer to disclosure.

According to Paragraph 3 *subsections 3 and 4* it is possible for private controllers to disclose the national identification number disclosure if this is demanded by a public authority, or 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.

If a private controller is to disclose the national identification number the starting point is that the legal basis should be found in Paragraph 3 *subsections 1 or 2.* Paragraph 3 *subsections 3 and 4 are* resuduary with a narrow scope. Private controllers should however be able to disclose the national identification number if the disclosure is demanded by a public authority.

In *Paragraph 4* it is provided that Paragraphs 1-3 do not allow for publication of the identification number. Publication may only take place with the data subject's consent.

Apart from the change in Paragraph 2 subsection 3 the provision is continuation of current legislation.

Processing of personal data for the purpose of direct marketing

Article 17
Paragraph 1 partly corresponds with Article 9 (3) in the current Act.

According to Paragraph 1 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.

Private companies doing commercial business are covered by the provision. Private interest groups and associastions which are not doing commercial business are not covered. Member organisations of businesses that provide special offers for members and are a part of the business are also covered by the provision.

In Article 9 (3) in the current Act the notion marketing (Faroese: *marknaðarrøkt*) is used. It is proposed that this is changed to direct marketing (Faroese: *beinleiðis marknðarføring*). It is not further explained in the commentary to the current Act how this (*marknaðarrøkt*) is to be understood, however the assessment is that what is needed is rules on processing of personal data in connection with direct marketing (*beinleiðis marknðarføring*).

Direct marketing is marketing directed directly to a specific person.

The provision entails that a company which processed personal data with a specific purpose – the core activity of the company – cannot disclose personal data conserning the costumers to others in order for others to process the data for direct marketing. The company cannot process the data for direct marketing for another company.

In order for direct marketing to be allowed it is necessary that the data subject has consented to the processing. As a starting point is is necessary that the data subject consents to whom the personal data can be disclosed, which means that it is not possible to give a general consent to all disclosure.

In Paragraph 1 last sentence it is provided that Article 6 in the Marketing Act applies when optaining the consent. This reference entails that the company has to be ware of the conditions in Article 6 in the Marketing Act when the data subject is to give his or her consent.

According to Article 6 (1) in the Marketing Act it is not allowed in business to send out advertising or in other ways to to conduct marketing with electronic communication such as e-mails, texting (SMS, MMS) etc., by automatic callingsystems, telefax or telephone if the recipient has not asked for this beforehand. According to Article 6 (2) Paragraph 1 does not apply when a business in connection to sale of goods or services as been informed of the costumers e-mailaddress. In these cases it is allowed for businesses to market on the e-mailaddress own goods or services corresponding with the goods or services the costumer has bought. It is however a precondition that the costumer at any time has the possibility – without inconvenience and without charge – to oppose to this – both at the time of disclosing the e-mailsaddress and when receiving messages for the business.

In Paragraph 2 there is an exception from the provision in Paragraph 1. According to Paragraph 2 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.

This means that there are two conditions in order for the exception to apply.

Firstly it has to be general data on customers which form the basis for classification into customer categories.

General data on customers is information such as name, address, sex and age. Also information on whether the data subject owns a house, car, computer etc. are considered general data. It is not allowed on the basis of Paragraph 2 to disclose information which lead to disclosing sensitive information about the costumer, such as information on abuse, sickness and poor financial state. Paragraph 2 also does not allow for disclosing detailed costumer information or information on habits.

Secondly it is a precondition that the conditions in Article 8 (1) subsection 6 are complied with. This means that the 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.

It is therefore a case by case assessment. This assessment can in specific cases entail that personal data may not be disclosed. This can be the case if a company has informed it's customers that personal data will not be disclosed.

According to Paragraph 3 sensitive data, cfr. Article 11 (1), may not be disclosed or used pursuant to paragraph 2.

Article 17 should be read together with Article 33 which gives the data subject the right to object at any time to processing of personal data concerning him or her for direct marketing. Please see the special commentary to Article 33.

Processing of personal data for historical, statistical and scientific purposes

Article 18
A similar provision is in Article 10 (1) subsection 9 in the current Act.

There are several registers on the Faroe Islands that contain information on Faroes Islanders. This may be all Faroes Islanders or all Faroes Islanders that have been in contact with the healthcare system or social security services. Examples of such registers are Cosmic (central hospital register), the population register and the Cancer register. These registers can be important tools in research in public health, in statistic work etc.

Therefore the conditions for processing of sensitive personal data for historical, statistical and scientific purposes are laid down in a specific Article. The processing of personal data for these purposes can have significant public interest and therefore it is important that the legal basis is clear. This is to ensure that it is totally clear – for the data subject and the controller – when and to which extent processing for these purposes can take place.

Article 18 is a special legal basis for processing of sensitive data in registers for historical, statistical and scientific purposes, also called registerbased research. With research based on registers there can be shown connections between use of medicine and age, sickness and employment etc. The aim is to see general tendencies and not to conclude anything on each individual.

Note also that Article 18 covers processing of sensitive data. Legal basis for processing other personal data should be found in Article 8.

In Paragraph 1 it is laid down that 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.

Paragraph 1 covers processing *exclusively* for the mentioned purposes. If a processing has other purposes, such as journalistic purposes, the legal basi sin Article 18 cannot be used.

In generali t is proposed with this new Data Protection Act that the Data Protection Authority no longer gives prior authorisations to processing of sensitive data. This also applies to processing of sensitive data for historical, statistical or scientific purposes. It is therefore no longer the Data Protection Authority that assesses the public interests vis-à-vis the the disadvantages for the person whom the data relate. This assessment is for the controller.

The controller shall make a case by case assessment where the public interests are weighed vis-à-vis the the disadvantages for the person whom the data relate. The starting point for such an assessment for the controller's assessment can for example be a reasoned application for the person wanting to conduct statistical or scientific research in the data.

Instead of prior authorisation from the Data Protection Authority other safety measures follow from the proposed Act, such as the requirement to have a Data Protection Officer and to keep records. These requirements – which always apply to the public sector – in addition to the requirements to implement appropriate technical and organisational security measures will heighten the level of protection for the data subject. This is also the case when processing personal data for historical, statistical and scientific purposes.

As a starting point the case by case assessment to be made in each specific case will lead to it being possible for recognised institutions or researchers to conduct nation wide historical, statistical and scientific surveys if appropriate security measures are put in place, e.g. pseudonymisation or encryption of personal data.

The precondition that the public interest should be significant entails that not everyone can access the personal data for any and all purposes. It is required that the researchplan has a certain scientific level and that the objective will benefit the society as such.

Although prior authorosation from the Data Protection Authority is no longer needed, the controller can get guidedance – general or specific – from the Data Protection Authority when in doubt of whether the conditions for processing are fulfilled.

Paragraph 1 does not exclude the possibility to process personal data for historical, statistical and scientific purposes on another legal bases. For example processing can be based on consent from the data subject or based on law and in these cases these basis thke precedence.

It should be noted that the Act on Gene Research lays down special rules on gene research and has specific rules to protect the individual. The Act on Gene Research is still applicable and as a starting point takes presedence to the rules in this Act.

Article 18 (1) should be read in conjunction with Article 7 (3) which provides that 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.

This entails that it is possible to process personal data in registers etc. for scientific purposes even though the personal data were not collected for this purpose if it is assessed that the disadvantages for the person whom the data relate are overridden by significant public interests. See the special commentary to Article 7 (3) above.

According to Paragraph 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

This provision entails that it is not possible to process personal data which are processed in the context of a scientific research survey for other purposes than the survey which has given access the personal data. It is therefore not possible to take decisions or take concrete steps in regards to a data subject based on the research. The personal data are "locked" in the purpose for which they are processed. The same limitations are not in place if the processing is based on the consent from the data subject. Therefore it can be more sensible in certain cases to use consent as a legal basis.

Paragraph 3 provides that data covered by paragraphs 1 and 2 may only be disclosed to a third party with prior authorisation from the Data Protection Authority.

The provision covers disclosing personal data covered by Paragraph 1 and 2 to third parties. Third parties should be understood in line with the definition in Article 6 (8) and covers 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.

The Data Protection Authority may lay down terms for the disclosure. These terms should ensure that the personal data are processed *exclusively* for historical, statistical or scientific purposes and the appropriate security measures are in place.

Legal information systems

Article 19
With linguistic changes Article 19 corresonds with Article 13 in the current Act.

According to Paragraph 1 sensitive data 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.

Legal information systems are systems accessible to a broad scope of subscribers in order to ensure uniform practice. This means systems that have an outward aim. The systems may be accessible through the internet.

The purpose of the legal information systems is that decisions and judgements may be accessible to a lot of people. A legal information systems is for example publication of decisions or judgements on a webpage.
The fact that the system should be accessible for a broad scope of people means that everyone should have the possibility to access. This does however not mean that the access should be free of charge.

Internal legal information systems of authorities or companies – e.g. summary of decisions in order to ensure a uniform practicce – is not covered which means that the general rules apply to these systems.

The processing of the sensitive data should be necessary in order to operating the system. This entails that sensitive data should not be processed in a legal information system if the system can function and reach it's goals without the sensitive data.

Paragraph 2 corresponds with the proposed Article 18 (2). Please see the special commentary to that paragraph.

According to Paragraph 3 the minister 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.

Hereby it is ensured that the Minister may down rules that set as a conditions that e.g. name, address and other identifying information not be published in the legal information system.

Archiving personal data

Article 20
The Article corresponds with Article 14 in the current Act.

The Article ensures that it is clear that personal data coveres by this Act may be transferred to be archived. It is the legislation on Archives that lays down what should be archived and should be followed in these cases.

Article 20 does not lay down a requirement that information should be transferred to archives.

Article 20 applies to both public authorities and private companies.

The provision provides an assessment between the consideration to avoid unnecessary stowing of data on one hand and to preserve personal data for historic and scientific research purposes on the other hand.

The Data Protection Act regulates the daily and administrative use of personal data while the legislation on archives regulates the use in relation to research when the personal data are no longer necessary for administrative use. There is therefore no discrepancy between the two areas of law. The Data Protection Act has the starting point that the question on archiving should be assessed on the basis of the legislation on archives.

Article 20 is a general provision that ensures that personal data covered by the Data Protection Act may be transferred to an archive on the basis of the legislation on archives.

The general provision entails that sector specific provisions are not affected. Sector specific provisions on archiving of personal data – e.g. in the Act on Gene Research and Act on Autorisation – take precedence to the general provision in Article 20.

Article 20 therefore covers information processed on the basis of this Act and that are not coved by sector specific legislation that regulates the transfer of data to archives.

The provision is in line with the principle of storage limitation. Please see the special commentary to Article 7 (1) subsection 5.

Chapter 4
Rights of the data subject

Chapter 4 on the rights of the data subject corresponds with Chapter 3 in GDPR.

Similar provisions are in Chapters 6 and 7 in the current Act although the rights of the data subject are strengthened and in the most cases are also regulated in more detail.

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

Article 21
The provision is based on Article 12 in GDPR.

Article 21 holds general requirements on how the rights of data subjects should be understood, how they should be complied with and how the communication should be. There is not a similar Article in the current Act although the content for the most part corresponds with current practice.

In Paragraph 1 it is proposed that the controller should ensure that any information to the data subject is provided in such a way that the data subject understands the information.

The controller should in this case take into account who the recipient is, including if the information is given to a child. It is provided that the information be concise and transparent. The information should also be given in using a clear and plain language. The controller should have in place appropriate measures – organisational or technical – to ensure that the requirements are fulfilled.

According to Paragraph 2 the controller should facilitate the exercise of data subject rights. This provision entails that the controller is required to organize his or her functions in such a way that it is easy for the data subject to exercise his or her rights. This could for example be to make it possible to communicate electronically. It is also provided that the controllermay not refuse to act on the request of the data subject for exercising his or her rights.

Paragraphs 3 and 4 lay down requirements for the controller to provide information on action taken on a request to the data subject. This is to ensure that the data subject knows how far along the

request is and the reasons for prolonged processing time. The data subject should also be informed of the possibility of lodging a complaint with the Data Protection Authority.

The provisions to provide a reason etc. are not new requirements for public authorities. Public authorities are today covered by the requirement to provide reasons and guidance on lodging a complaint set out in the Public Administration Act. It is however new that it is a legal obligation for private controllers to provide reasons and give guidance on lodging a complaint.

There is no deadline for a complaint to be filed with the Data Protection Authority. The Data Protection Authority should therefore process all complaints. General administration legislation and practice may however in very special cases lead to the Data Protection Authority not processing a complaint in substance if the case is very old.

In Paragraph 5 it laid down that information provided to the data subject under Articles 23 and 24 and any communication and any actions taken under Articles 26-36 and 49 shall be provided free of charge unless the requests are manifestly unfounded or excessive.

Whether a request is manifestly unfounded or excessive is a case by case assessment where the controller may take into account the repetitive nature of the requests.

Article 25 in the current Act which entails that it as a starting point should pass 6 months between the requests for access by the data subject is not carried over into the new Act. See the special commentary to Article 26.

The burden of proof lays with the controller who should be able to prove that the requests are manifestly unfounded or excessive. The controller should therefore save documentation if a request for access is not granted. This could e.g. be by saving old requests.

The fee the controller may charge in relation to manifestly unfounded or excessive requests should be reasonable in relation to the administrative costs related to processing the request.

If the controller wishes to charge a fee, the controller should inform the data subject thereof prior to meeting the expenses.

Information provided to the data subject according to the information obligation in Articles 23-24 are not provided at the request of the data subject, and therefore Paragraph 5, 2. And 3. Sentence do not apply. The controller can therefore not on the basis of Paragraph 5 refrain from informing the data subject.

Article 22
The Article lays down how the controller should provide information to the data subject. As a starting point it is the data subject who decides which form of communication is to be used.

In Paragraph 1 it is provided that the information should be provided by electronic means if the request from the data subject is received electronically. The data subject can request to receive the information in another form.

According to Paragraph 2 the data subject may request for the tnformation to be given orally. In these cases the controller can request further information in order to confirm the identity of the data subject if there are doubts concerning the identity. If the controller requests further information does not prejudice Article 15.

According to Article 12 (7) in GDPR information to be provided to data subjects pursuant to Articles 13 and 14 (Articles 23 and 24 in this Act) may be provided in combination with standardised icons. These icons are not yet approved in the EU. When they are approved, they can also be used by controllers and processors in the Faroe Islands.

See also recitals 58, 59 and 64 in GDPR.

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

Article 23
The Article is based on Article 13 in GDPR. A similar provision is in Article 20 in the current Act.

As it is in the current Act it is distinguished between cases where the personal data are collected from the data subject (Article 23 in the proposal) and when personal data have not been obtained from the data subject (Articles 24-25 in the proposal).

The information obligation is very important as it entails that the data subject is informed that personal data are being processed, giving the data subject the possibility to assess the processing and whether other rights are to be used.

When the controller collects personal data from the data subject, the controller should provide the data subject with the information at the time of collection. This entails that the data subject can provide the personal data on an informed basis.

In Paragraph 1 it is laid down which information the controller should always provide to the data subject, when personal data are collected from the data subject. This is e.g. name and contact details of the controller.

According to Paragraph 1 subsection 3 the controller should provide the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

The requirement to inform the data subject of the purpose entails that the data subject be provided with sufficient information to understand why the data is being collected. How much information this coveres is a case by case assessment. However it is at least a requirement that the controller inform the data subject what the personal data are to be used for or are expected to be used for. The provision should be read in conjunction with Article 7 (1) subsection 2 on purpose limitation. Please see the special commentary to that Article above.

The fact that the controller should provide the data subject with the purpose of the processing is not new compared to the current Act. The requirement to give information of the legal basis is however new. The legal basis can be in Article 8 of this Act. Paragraph 1 Subsection 4 provides that if the processing is based on Article 8 (1) subsection 6, the data subject should be informed of the legitimate interests pursued by the controller or by a third party.

According to Paragraph 1, subsection 5 information should be given on the recipients or categories of recipients of the personal data. Categories of recipients should be understood generally, e.g. as "other auhtorities" or "collaborations".
According to Paragraph 1 subsection 6 the controller should inform the data subject of the fact that the controller intends to transfer personal data to a foreign country, a third country or international organisation. Foreign country and third country should be understood as defined in Article 6 (14) and (15). The provision provides that the data subject always is informed of whether the personal data are transferred out of the Faroes even if there is not requirement for prior authorisation.

The data subject should be informed of the existence of an adequacy decision. If there is no such decision the data subject should be informed of the basis for transfer. This requirement entails – in addition to refering to the legal basis – that the controller should inform the data subject of how the data subject can get a copy of the contract etc. that is the basis for the transfer or where this contract etc. is accessible.

If information in a provision is not relevant, it is not required for the controller to inform thereof. It is for example not required to inform that the informtion will not be disclosed or that there is no data protection officer.

In Paragraph 2 it is proposed that the controller provides the data subject with further information necessary to ensure fair and transparent processing. The provision partly corresponds with Article 20 (1) subsection 5 in the current Act.

Paragraph 2 entails that the controller in each case should assess whether the information provided according to Paragraph 1 is sufficient or if the data subject should be given further information.

According to Paragraph 2 subsection 1 the controller should provide the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. This corresponds with the principle of storage limitation i Article 7 (1) subsection 5.

Paragraph 2 subsections 2-4 provides that information be given on the rights of the data subject according to this Act. Paragraph 2 subsection 5 provides that the controller should give information on 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.

Paragraph 2 subsection 6 provides that the controller should inform the data subject of the existence of automated decision-making. This covers e.f. decisions based on profiling cfr. Article 35. If these decisions occur the controlles should at least inform the data subject of meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Providing information on the logic involved does not entail providing information in detail of the processing. However it is crusial that the data subject is given enough information to be able to understand the assessments that underlie in the processing and how the automatic processing comes to a certain decision.

If it is a administrative decision, the information to be provided according to Paragraph 2, subsection 6, are to be provided in addition to the administrative requirement of giving a reason for a decision.

In Paragraph 3 it is proposed that the controller also has an obligation to inform if the controller intends to further process the personal data for a purpose other than that for which the personal data were collected. This is a broadening of the information requirement according to the current Act.

The application of Paragraph 3 depends on the purpose the data subject is informed of according to Paragraph 1 and what this purpose covers. The aim of the provision is to ensure that the data subject at all times knows to which purposes his or her personal data are processed. This also gives the data subject the possibility to use the rights provided in this Act.

It is a precondition for the further processing that the provisions in this Act are complied with, including the principles, especially purpose limitation, and the rules on lawfulness of processing

In Paragraph 4 it is provided that Paragraphs 1-3 do not apply where and insofar as the data subject already has the information. This also follows from the current Act. As the new Act lays down an obligation to provide more information than the current Act, it is likely that Paragraph 4 will be applicable in fewer cases.

See also recitals 60-62 in GDPR.

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

Article 24
The provision is based on parts of Article 14 in GDPR. A similar provision is in Article 21 in the current Act.

Article 24 provides for the obligation to inform when the controller obtains personal data from other sources than the data subject.

Information that should be provided according to Paragraph 1, subsections 1-3 and 5-6, is the same that should be provided according to Article 23 (1), subsections 1-3 and 5-6. Please see the special commentary to these provisions above.

According to Paragraph 1, subsection 4 the controller should provide information on the categories of personal data concerned. In substance there is a small change campared to the current Act as it is enough that the controller informs of the categories of personal data (for example *contactinformation* in stead of specific e-mailaddress, telephonenumer etc.).

Information to be provided in order to ensure fair and transparent processing according to Paragraph 2 subsections 1-5 and 7 is the same information to be provided according to Article 23 (1) or (2). Please see the special commentary to those provisions.

According to Paragraph 2 subsection 6 the controller should inform the data subject from which source the personal data originate. This includes information on whether the personal data came

from publicly accessible sources. Providing this information gives the data subject the possibility to assess the information, including their reliability.

Paragraph 3 is identical to Article 23 (4) on further processing. Please see the special commentary to that provision above.

Article 25

Article 25 is closely connected to Article 24 and provides for rules on how to comply with the obligation to provide for information when personal data have not been obtained from the data subject. Article 25 is based on parts of Article 14 in GDPR.

In Paragraph 1 it is provided when the information in Article 24 (1) and (2) should be provided to the data subject. According to the current Act the information should be provided without delay. This will be slightly changed with this proposal.

In Paragraph 1 subsection 1 it is proposed that the information should be provided within a reasonable period after obtaining the personal data, but at the latest within 4 weeks. Whether the information is provided within a reasonable period is a concrete assessment in each case having regard to the specific circumstances in which the personal data are processed.

In Paragraph 1 subsections 2 and 3 has more detailed rules on when the controller should inform the data subject when the personal data are to be used for communication with the data subject and when the personal data are to be disclosed.

In Paragraph 2 it is laid down when the obligation to inform does not apply. As when personal data are collected from the data subject, the obligation does not apply, cfr. Paragraph 2 subsection 1, if the data subject already possesses the information. Please see the special commentary to Article 23 (4).

According to Paragraph 2 subsection 2 the obligation does not apply if the provision of such information proves impossible or would involve a disproportionate effort. This is – with linguistic changes – the same as Article 21 (2) subsection 3, 1. sentence.

As is the case under the current Act, this is a concrete proportionality assessment. The controller should assess the importance of providing the information to the data subject in order for the data subject to use his or her rights on one hand and the burden of providing the information for the controller on the other hand. In this assessment the controller should take into account the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

Providing information to each data subject could be impossible or involve a disproportionate effort where processing is carried out for archiving purposes, scientific or historical purposes or statistical purposes.

Paragraph 2 subsection 3 provides that the obligation to provide information does not apply if the provision of such information is likely to render impossible or seriously impair the achievement of the objectives of that processing. This could cover e.g. the work carried out when an insurance company assesses how injuries occurs. The information should be provided as soon as the objectives have been reached.

According to Paragraph 2 subsections 4 and 5 the obligation does not apply if obtaining or disclosure is expressly laid down by law to which the controller is subject, or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law.

According to Paragraph 3 the controller should – in cases covered by paragraph 2, subsection 2 and 3 – take appropriate measures to protect the data subject's rights, including freedoms and legitimate interests. This could be by making the information publicly available on the controllers website. This way it is possible to generally get information on the purposes of the processing etc. and could ensure transparacy for the data subject and the public.

See also recitals 61 and 62 in GDPR.

Right of access by the data subject

Article 26
The Article is based on Article 15 in GDPR. Article 19 in the current Act has a similar content.

The aim of Article 26 on access is that the data subject has the possibility to get knowledge of which personal data about the data subject the controller is processing, why and on which basis. For example this gives the data subject the possibility to rectify personal data.

Paragraph 1 provides that if the data subject requests access, the controller shall confirm as to whether or not personal data concerning him or her are being processed. If this is the case the controller should give access to the personal data and provide the data subject with the information in Paragraph 1 subsections 1-8.

There are no formal requirements to the request for access which can be put forward both verbally and in writing. This entails that the controller cannot demand that the data subject puts in a request in writing. However the controller can request that the data subject clarifies the request i fit is unclear or if it can reduce the administative burden for the controller. The controller cannot refuse to reply if the data subject does not clarify the request.

Giving the data subject *access to the personal data* means that the controller can choose to give the data subject access to (or copies of) original documents, files, films from serveillance cameras etc. or to give access to copies of the information in new documents. It is however crusial that the data subject gets access to the information, making the data subject able to ensure that the personal data is correct and that the processing is lawfull.

Article 26 only gives the data subject access to information about himself or herself. Personal data concering other people should therefore be erased in the material the data subject gets access to.

The information the controller is to provide according to Paragraphs 1 and 2 – in addition to the personal data – is similar to the information to be provided according to Articles 23 and 24. Please see the special commentary to these provisions above.

According to Paragraph 3 the controller should provide a (written) copy of the personal data undergoing processing. The first copy is free of charge. This applies for both private and public

controllers. If the data subject requests any further copies, the controller may charge a reasonable fee.

As explained in the special commentary to Article 21 (5) above the fee the controller may charge should be reasonable in relation to the administrative costs related to processing the request.
The provision on reasonable fee covers the cases where the data subject requests several (physical) copies og the information and the administrative costs relating to this. The question of whether the controller can charge a fee for the processing of the request is regulated by Article 21 (5). See the special commentary above.

Article 25 in the current Act which provides that the data subject can get access to information every six months is not repeated in this proposal. In stead the controller should assess in each case if the request is manifestly unfounded or excessive, including due to its repetitative character, chr. Article 21 (5). Guidedance to this assessment can be found in recital 63 in GDPR where it is stated that the data subject should have the right to access easily and at reasonable intervals.

The current Act on Processing of Personal Data provides for public access to information in Article 18. This Article is not repeated in this proposal. The reason is that it is not assessed to be necessary for everyone to be able to get access to information according to the Data Protection Act. The Act on Public Access still applies, see below.

In the special commentary to Article 18 in the current Act it is explained that the aim of the article is situations were a person considers whether he or she will provide the controller with their personal data, including situations where a person considers to register as a member of an association. The overall assessment is that the Articles on information in Articles 23-25 in the proposal are sufficient and therefore there is no need for an Article equivalent to Article 18 in the current Act.

Public controllers should be aware of Article 4 (2) in the Act on Public Access when processing requests for access. When the controller receives a request for access from the data subject, the controller should assess which legal basis gives the data subject a better legal position. This assessment should be based on the amount of information to be given and not procedural rules, e.g. rules on payment for copies.

If the data subject has pointed to a certain legal basis and the authority assesses that the data subject can be provided with more information on another legal basis, e.g. the information to be provided according to Article 26 in this proposal, the authority should give guidance on this according to the general obligation to give guidance.

See also recital 63 in GDPR.

Right to rectification

Article 27
The Article is based on Article 16 in GDPR. Article 28 in the current Act has a similar content.

In Paragraph 1 it is proposed that the data subject shuld have the right to obtain rectification of inaccurate personal data concerning him or her. The data subject should contact the controller in

order to obtain rectification. However the controller should also on his or her own initiative rectify information if he or she becomes aware of inaccurate personal data.

Article 27 is a more detailed regulation of the principle of accuracy in Article 7 (1) subsection 4 which entails that personal data should be accurate ande kept up to date.
The personal data should be rectified without undue delay.

The controller does not have an unconditional obligation to rectify if the controller and data subject do not agree about the accuracy of the data.

This is especially relevant to data that cannot be objectively confirmed, such as age and name.

An example could be a dispute between the controller and data subject about who said what in a meeting and has become part of the minutes. A data subject can also disagree with an assessment by a professional, e.g. a teacher or a nurse, which has been documented in a file. The solution can in these cases be that it is noted that there is an agreement on whether the personal data is right ot wrong.

Paragraph 2 it is proposed that the data subject should have the right to have incomplete personal data completed, including by means of providing a supplementary statement. In the assessment of whether the data is incomplete the purposes of the processing should be taken into account.

Public authorities do usually not rectify directly in finished documents. Therefore a supplementary statement should be made in these cases, where it is clearly stated which personal data are inaccurate or incomplete. This applies to both objective information and subjective assessments.

See also recital 65 in GDPR.

Right to erasure

Article 28
The Article is based on Article 17 in GDPR. Article 27 in the current Act has a similar content.

The right to erasure in Article 17 in GDPR is also called the “right to be forgotten”. Although the provision for most part is a continuation of the current right to erasure, the purpose of the provision is to give data subjects better possibilities to erase personal data on the internet.

Paragraph 1 sets out when personal data should be erased – on the controllers own initiative or at the request of the data subject. Erasing data entails that the data should be erased everywhere, e.g. in all systems. As a starting point the obligation applies also to erasure of personal data in back-up systems etc. However this only applies if it is technicly possible to erase personal data from back-up systems.

According to Paragraph 1 subsection 1 personal data should be erased if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. This subsection is a more detailed regulation of the principles for processing in Article 7 (1) subsection 4 and 5 and builds on the fundamental rules that the controller should not keep personal data that he or she does not need.

According to Paragraph subsection 2 personal data should be erased if the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing. Please see the special commentary to Article 9 on conditions for consent.

The right to erasure in Paragraph 1 subsection 3 should be read in conjunction with the right to object in Articles 32 and 33. If the conditions in Articles 32 and 33 are met, the personal data should be erased.

If personal data have been unlawfully processed they should be erased according to Paragraph 1 subsection 4. The provision mirrors the principle in Article 7 (1) subsection 1 which lays down that personal data should be processed lawfully.

If the controller is subject to a legal obligation that requires that the personal data have to be erased, the controller should according to Paragraph 1 subsection 5 erase these data.

According to Paragraph 1 subsection 6 the controller should on his or her own initiative or at the request of the data subject delete personal data that have been collected in relation to the offer of information society services referred to in Article 10 (1). Please see the special commentary to Article 10. Paragraph 1 subsection 6 entails that it will be easier to erase personal dta which children and youth have provided information society services on the basis of consent. The reason is that it should be easier to erase personal data on the internet.

It is proposed to have a special notification obligation i Paragraph 2 in order to strengthen the data subjects control over own personal data that is being shared on the internet. The provision entails that a controller who has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller shall 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.

Controller should take reasonable steps to inform other controllers. It is a case by case assessment as to how much the controller should do to in these cases. In the assessment the controller can take account of available technology and the cost of implementation, including technical measures.

The special obligation to notify in Paragraph 2 is an addition to notification in Article 30. Please see the special commentary to Article 30.

In Paragraph 3 it is proposed to lay down when the right to erasure does not apply.

According to Paragraph 3 subsection 1 the right to erasure does not apply if the processing is necessary for exercising the right of freedom of expression and information. The provision entails a balancing between the right to data proctecion and the fundamental rights in the European Convention on Human Rights. See also point 2.8. in the general commentary.

In Paragraph 3 subsection 2 it is proposed that the right to erasure should not be applicable if the processing is necessary for compliance with a legal obligation 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. The provision mirrors the provisions in Article 8 (1) subsections 3 and 5

and entails that the right to erasure as a starting point does not apply when processing is based on these provisions.

The provisions also entails that the right to erasure in most cases cannot is not applicable to processing carried out by public authorities that proces personal data in the exercise of their tasks. As is the case for the right to rectification, it is usually not possible to rectify information in documents that have already been finalised. If information is inaccurate this should be documented rather than erased.

According to Paragraph 3 subsection 3 the right to erasure does not apply in processing is necessary 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

According to Paragraph 3 subsection 4 the right to erasure does not apply if the processing is necessary for the establishment, exercise or defence of legal claims. On how legal claims should be understood, please see the special commentary to Article 12 (1) subsection 7.

Common for the exceptions in Paragraph 3 is that the processing in all cases should be necessary. It is not sufficient that the processing lightens a burden for the controller.

See also recitals 65 and 66 in GDPR.

Right to restriction of processing

Article 29
The Article is based on Article 18 in GDPR. Article 27 in the current Act has a similar content.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

The wording restriction of processing is new compared to the current Act. The notion - limiting the future processing of personal data – is however not new and is in the current Act called *block*.

According to Article 27 in the current Act the controller should on his own, or at the request from the data subject block personal data, which are inaccurate or misleading or processed in violation of law or regulations.

It is proposed that the data subject in certain cases can demand that the controller restricts the processing of personal data.

According to Paragraph 1 subsection 1 the controller should restrict the processing of personal data if 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

According to Paragraph 1 subsection 2 the data subject can demand that the controller instead of ersasing personal data which is being processed unlawfully, restricts the processing. This provision can for example be used if the data subject intends to use the information as documentation in relation to compensation.

In Paragraph 1 subsection 3 it is proposed that the processing could be restricted if 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. On how legal claims should be understood, please see the special commentary to Article 12 (1) subsection 7.

According to Paragraph 1 subsection 4 the controller could restrict the processing while assessing whether the conditions in Article 32 on objection are fulfilled. If the conditions are fulfilled the controller cannot proces the personal data (which should then be deleted, cfr. Article 28 (1) subsection 3).

If the processing of personal data is restricted according to Paragraph 1 the controller can only store the personal data. If one of the conditions in Paragraph 2 subsections 1-4 are fulfilled the personal data may be processed.

According to Paragraph 3 the controller should inform the data subject before the restriction of processing is lifted.

The restriction of processing may be lifted when the conditions in Paragraph 1 are no longer fulfilled. This could for example be if the controller assesses that the conditions for objection in Article 32 are not fulfilled.

See also recital 67 in GDPR.

Notification obligation of the controller

Article 30
The Article is based on Article 19 in GDPR. Article 27 (2) in the current Act has a similar content.

The provision entails that the controller on his or her own initiative should communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed.

Recipient should be understood as defined in Article 6 (9).

The notification obligation of the controller entails that it is not necessary for the data subject to contact every controller etc. in cases where personal data should be erased.

The obligation to notify does not apply if it proves impossible or would involve a disproportionate effort. On how this should be understood please see the special commentary to Article 25 (2) subsection 2.

On request from the data subject the controller should inform the data subject about the recipients. This provision should be read in conjunction with Articles 23 and 24 on information to be given to the data subject when collecting personal data, e.g. information on recipients.

Right to data portability

Article 31

The Article is based on Article 20 in GDPR. There is no similar Article in the current Act.

The right to data portability is one of the new rights for the data subject which are included in the GDPR. This i sin line with one of the main goals of the GDPR which is to give the data subject more controll over his or her own personal data.
According to Paragraph 1 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. It should be possible without hindrance from the controller to transmit these data from one IT-system to another if this is technically feasible.

The right covers only data which the data subject has provided the controller and only if the processing is based on consent, cfr. Article 8 (1) subsection 1 or Article 12 (1) subsection 1 or on a contract, cfr. Article 8 (1) subsection 2, and if the processing is carried out by automated means.

This entails that the right to data portability does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In Paragraph 2 it is proposed that the personal data which the data subject receives pursuant to paragraph 1, should be in a structured, commonly used and machine-readable format. Exactly which format should be used is conditioned on which field of business the controller i son.

In any way possible it is advised to use open and documented standards such as JSON, XML, CSV etc. It is important that the personal data is disclosed in a way – if possible – for the data subject to understand the personal data and to use them again.

The right to data portability could be used if the data subject would like to get an offer for a service or wishes to change provider. It could cover personal data provided to banks, telephone companies or insurance companies in connection to offers etc.

Only covering data which the data subject has provided, entails that data which the controller has added on the basis of information provided by the data subject, should not be disclosed. This could be analysis or other processing of personal data on the basis of online activity of the data subject, e.g. personal suggestions of music based on music which the data subject has previously listened to or information related to an assessment of creditworthiness.

According to Paragraph 2 the data subject should have the right to have the personal data transmitted directly from one controller to another if this is technically feasible. This holds as a precondition that the controllers have interoperable formats or systems. The Article does however not lay down an obligation for the controllers to adopt or maintain processing systems which are technically compatible.

The data subject's right to data portability is without prejudice to the rights and freedoms of other data subjects. This entails that if personal data about other data subjects are transmitted – for example contact information of friends of the data subject when changing e-mail-address provider – the new controller does not have the right to use this information for own purposes, such as marketing.

See also recital 68 in GDPR.

Right to object
The right to object follows from Article 21 in GDPR. Article 26 in the current Act has a similar content.

The provisions proposed in Articles 32-34 are based on Article 21 in GDPR.

Article 32
In Paragraph 1 it is proposed that the data subject should have the right to object – on grounds relating to his or her particular situation – to otherwise lawful processing of personal data concerning him or her which is based on Article 8 (1), subsection 5 or 6. This includes profiling based on those provisions.

This means that the data subject can object to processing which 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 or
- 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.

The wording in Paragraph 1 entails that the possibility to object is slightly limited compared to the right in Article 26 in the current Act. The right to object in the current Act is not limited to a specific processing basis.

The proposal for Article 32 (1) means that the data subject cannot object to processing which takes place on the basis of consent (Article 8 (1) subsection 1 or Article 12 (1) subsection 1) or is necessary for compliance with a legal obligation to which the controller is subject (Article 8 (1) subsection 3).

However it is not assessed that this change – compared to the current Act – would lead to such significant disadvantages for the data subject that the Faroese legislation should differ from GDPR on this point.

As it is today the controller should on the basis of a case by case assessment conclude whether there is such a particular situation for the data subject that the processing should be stopped. The data subject should give reason for why he or she objects and why the processing should stop. The reasons should be important and have some significance before the processing is to be stopped.

If the controller assesses that the conditions for objection are not met, the controller should inform the data subject thereof and the reasons for the decision.

When a data subject has objected to a processing cfr. Paragraph 1 and the conditions are met, the controller according to Paragraph 2 should 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. This is also a case by case assessment.

See also recital 69 GDPR.

Article 33
In Article 33 there is proposed a special provision on objection in cases where personal data are processed for direct marketing purposes.

In Paragraph 1 it is proposed that the data subject in these cases should have the right to object at any time to processing of personal data concerning him or her. This includes profiling to the extent that it is related to such direct marketing.

The right to obejct to direct marketing in Article 33 (1) is broader than the general right to object in Article 32. The provision entails that the data subject has the right to object – at any time without regard to the legal basis – to procsseing, including profiling, for direct marketing purposes.

Direct marketing is marketing directed directly to a specific person.

In Paragraph 2 it is proposed that the controller should no longer process the data for direct marketing purposes if the data subject objects to processing for such purposes. An objection against direct marketing does therefore not mean that the controller should stop all processing of the data if the controller prosesses for other purposes as well.

See also recital 70 in GDPR.

Article 34
In Article 34 there is a special obligation to inform in regards to the right to object which entails that the controller at the time of the first communication with the data subject should bring the rights in Articles 32 and 33 explicitly to the attention of the data subject

The obligation to inform comes in addition to Article 23 and 24 which entail that the controller to the extent necessary to order to ensure fair and transparent processing, should inform the data subject of the rights in Chapter 4, sbrt. Article 23 (2) and 24 (2).

The obligation entails that the controller should bring the right explicitly to the attention of the data subject. This cannot be indirectly or tacitly. The information should be presented clearly and separately from any other information

Automated individual decision-making, including profiling

Article 35
The Article is based on Article 22 in GDPR. There is no similar Article in the current Act.

According to Paragraph 1 the data subject should not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her. The automated processing includes profiling which is defined in Article 6 (3).

The reference in Paragraph 1 to profiling entails that the data subject has the right not to be subject to a decision based solely on automated processing which uses 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.

The provision covers only processing which in some way evaluates personal aspects relating to the data subject. This is evident in recital 71 in GDPR and also in the title of the Article.

This entails that the Article is not applicable if there is no evaluation of personal aspects. This could for exampe be the case if the data subject wishes to withdraw money from an ATM. The automatic processing in these cases which may lead to a refusal because there is no coverage, is automatic processing based on facts – the fact that there is no money in the account – and is not an evaluation of personal aspects of the data subject.

Whether the decision produces legal effects concerning the data subject or similarly significantly affects him or her is a case by case assessment. Examples are decisions which lead to the cancellation of contracts, the data subject not getting social security, is refused access to a country or does not get access to an education. When assessing whether the decision significantly affects the data subject account should be takan to the specific situation the data subject is in.

The provision covers only decisions which are *solely* based on automatic processing. This means that if a person (e.g. a case worker) assesses the circumstances of a case and takes a decision which is partly based on automatic processing, then this decision is not covered by the provision. The person that takes part in the assessment has to have real influance on the decision and be able to change the conclusion in order to get out of the scope of the Article.

According to recital 71 in GDPR decisions producing legal effects concerning the data subject or similarly significantly affects the data subject should not concern a child. As a starting point this entails that automatic processing regarding children should not take place although the processing is not banned.

Controllers should therefore be extra careful when processing personal data regarding children if the processing is covered by Article 35.

To which extent automatic processing regarding children can take place will be further detailed by the Data Protection Authority.

Paragraph 2 lays down in which cases the prohibition in Paragraph 1 does not apply.

According to Paragraph 2 subsection 1 the prohibition does not apply if the processing is necessary for entering into, or performance of, a contract between the data subject and a data controller. This could be the case if the controller is a bank and automatically processes personal data regarding a costumer – age, income, employment and education – in order to assess how much money the bank can grant in loans.

According to Paragraph 2 subsection 2 automatic decisions can be taken when this is authorised by law to which the controller is subject. It is a precondition that the law lays down suitable measures to safeguard the data subject's rights, such as giving the data subject the right to contest the decision.

According to Paragraph 2 subsection 3 automatic decisions can be taken if based on the data subject's explicit consent.

According to Paragraph 3 the controller shall implement suitable measures to safeguard the data subject's rights in the cases referred to in paragraph 2, subsection 1 and 3. This means that the data subject should at least have the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

This means that the data subject who in the example above on the basis of automatic processing was granted a loan, should have the right to demand that the bank takes a new decision by human intervention.

There are fewer possibilities to part from the starting point in Paragraph 1 if the controller processes sensitive data. According to Paragraph 4 decisions referred to in paragraph 2 should not be based on sensitive personal data unless the data subject has given his or her explicit consent or the processing is necessary for reasons of substantial public interest and suitable measures to safeguard the data subject's rights are in place.

The suitable measures that should be in place could include the right to obtain human intervention on the part of the controller, the possibility for the data subject to express his or her point of view and to contest the decision, that the controller performs regular checks of the system and that the controller uses anonymousation and pseudonymisation to the extent possible.

See also recitals 71 og 72 in GDPR.

Restrictions

Article 36
The Article for most part corresponds with Article 22 in the current Act. The Article also corresponds with Article 23 in GDPR which gives the EU Member States the possibility to lay down restrictions in the rights of the data subject.

The provision entails restrictions to the obligation to inform in Article 23 and 24, the right of access in Ariticle 26 and the obligation to notify in Article 48.

In Paragraph 1 subsections 1-5 lists the interests which are assessed to precede the rights of the data subject and where information to the data subject according to Articles 23, 24, 26 and 48 therefore does not apply. A concrete assessment should be made in each individual case.

Restrictions could be made if a concrete assessment leads to the conclusion that the information if disclosed can endanger national security, defense or the relationship with other countries or organisations (no. 1), the information 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 (no. 2), it is not advisable to inform the data subject because of health issues or close relations to the data subject (no. 3), the information is subject to secrecy or confidentiality pursuant to law (no 4), or the data subject’s interest in this information is found to be overridden by essential considerations of public or private interests (no. 5).

According to Paragraph 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 7-11 and 14 in the law on Public Access to Documents. The provision alignes the possibility to restrict access according to both Acts (Data Protection Act and Act on Public Access to Documents).

In Paragraph 3 there is a special provision on restrictions when personal data are processed solely for history, 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. In these cases Articles 26, 27, 29 and 32 should not.

The aim of the provision is to ensure that scientific research based on the whole population or parts thereof can take place for the benefit of the society as a whole. If the conditions in Paragraph 3 are fulfilled the public interest overtake the interest of each individual.

Paragraph 4 repeats Article 22 (5) in the current Act and entails that the minister may lay down further derogations from the right to information and access and may lay down conditions when access is given. There are no rules laid down according to Article 22 (5) in the current Act.

See also recital 73 in GDPR.

Chapter 5
Controller and processor

The Chapter is based on Chapter 4 in GDPR. The current Act does not have an equvivalent Chapter although several provisions could be found in the current Act.

There are more Articles on controllers and processor in this proposal. The reason is to be found in the principles of acountability and the risk based approach, cfr. point 1.4.2. in the general commentary, which are the basis of the proposal and which have more detailed rules as a precondition.

Responsibility of the controller

Article 37
The Article is based on GDPR. There is no similar Article in the current Act.

Article 37 entails the overall statement that it is the controller who has the responsibility to ensure that the processing of personal data is performed in accordance with the Act. The responsibility of the controller is also laid down in Article 7 (2) in this proposal.

The controller should implement appropriate technical and organisational measures which correspond with the risk for the data subject posed by the processing.

Article 37 is an implementation of the risk based approach to data protection which the proposal is based on, that entails that the controller should make an assessment of the risks for the data subject posed by the processing when implementing security measures. The controller should in this

assessment take into account the nature, scope, context and purposes of processing. The controller should also take into account which kind of personal data he or she is processing (sensitive or non-sensitive) and who the personal data concern (e.g. personal data regarding children). See point 1.4.2. in the general commentary.
In addition to ensuring that the processing is performed in accordance with this Act, the controller should to be able to demonstrate that this is the case. The controller could do this by documenting the measures in some way. The controller should be able to demonstrate to the Data Protection Authority that the processing is in line with the Act.

The measures set in place should be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures could also include the implementation of appropriate data protection policies by the controller. This entails that the requirements the controller should fulfill are not static and that the controller should at all times assess the risk in the processing andi f the security measures are sufficient.

See also recital 74 in GDPR.

Data protection by design and by default

Article 38
The Article is based on Article 25 in GDPR. The Article is new compared to the current Act and entails that data protection should be made a natural part of IT-systems etc. when they are designed if they are to process personal data.

In Paragraph 1 it is laid down that the controller by design should ensure that processing is in line with the Act.

This entails that the controller – both at the time of the determination of the means for processing and at the time of the processing itself – should implement appropriate technical and organisational measures, which are designed to implement data protection principles pursuant to this Act, such as data minimisation, in an effective manner. This could include pseudonymisation as soon as possible. The provision entails a requirement to implement technical and organisational measures in a way that ensures processing in line with the Act.

Paragraph 1 does not apply for processing systems already in place at the entry into force of this Act. The provision does therefore not mean that systems that the controller already uses should be redesigned. The provision entails that the controller when determining of the means for processing, should include data protection measures. The provision also entails that the controller at the time of the processing itself also should be especially aware of data protection.

Data protection by design is based on a risk based approach to data protection. The controller should therefore when designing take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. The controller should in each case assess the risk posed by the processing in order to decide which measures are necessary and how this could be designed into processing systems.

See also point 1.4.2. in the general commentary.

According to Paragraph 2 the controller should 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.
The obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Paragraph 2 builds on the principle of data minimisation in Article 7 (1) subsection 3 and is an addition to the requirement in Paragraph 1. The provision entails that when a processing system or sevice etc. is set up (an online service or an app) the settings by default should ensure that personal data are processed, including shared, as little as possible.

Paragraph 2 does not entail an oblilgation to change or replace all current IT-systems when this Act enters into force. However i fit is possible to change setting without alot of work, then this should be done.

Data protection by design and by default will be explained in more detail by the Data Protection Authority in connection with guidance in concrete cases and in general guidelines, including written guidelines. The Data Protection Authority can – if considered relevant – use the written guidelines from the Danish Data Protection Authority in this work.

See also recital 78 in GDPR.

Joint controllers

Article 39
The Article is based on Article 26 in GDPR. The Article is new compared to the current Act however this will not lead to big changes in the current legal position.

Article 39 regards the situations where two or more controllers jointly determine the purposes and means of processing. In these cases they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Act. The Article is especially relevant for data subjects who wish to make use of the rights according to the Act and who always should know who is processing data and who is responsible for the processing.

According to the Article the controller should determine their respective responsibilities, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 23 and 24, and may also designate a contact point for data subjects. The reason why this should be agreed is that this should not affect the data subject negatively.

The arrangement referred to in the Article should duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects.

It should also be possible for the data subject to know the essence of the arrangement, which should be made available to the data subject, e.g. by giving the data subject access to the agreement.

Irrespective of the terms of the arrangement referred to in the Article, the data subject may exercise his or her rights under this Act in respect of and against each of the controllers.

See also recital 79 in GDPR.

Representatives of controllers or processors not established on the Faroe Islands

Article 40
The Article is based on Article 27 in GDPR. Similar privisions can be found in Article 7 (3) and (4) in the current Act.

Paragraph 1 entails that controllers or the processors who are not established on the Faroe ISlands, but who are covered by the Act, cfr. Article 5 (2) should designate in writing a representative on the Faroe Islands. This means that the starting point is that when personal data of data subject on the Faroe Islands is being processed a representatives for controllers or processor should be designated to whom the data subject can turn.

Please see the special commentary to Article 5 (2) on who is covered by the provision.

For the data subject this provision entails that the distance between the data subject and the controller or processor is short and that it is easier to communicate because the representative often will be Faroese or will have knowledge of Faroese and Faroese relations.

In Paragraph 2 there are laid down exceptions from the obligation in Paragraph 1.

According to Paragraph 2 subsection 1 the obligation does not apply to processing which is occasional, does not include, on a large scale, processing of sensitive data, and is unlikely to result in a risk to the rights, including freedoms, of natural persons.

Paragraph 2 subsection 1 is yet another example of the risk based approach. The provision entails that controllers and processors are not obliged to have representatives on the Faroe Islands if the risk posed to the data subject is small. See also point 1.4.2. in the general commentary.

If a processing is covered by the exception in Paragraph 2 subsection 1 is a case by case assessment. The assessment should include all three cumulative conditions.

The first condition is thatt the processing only is *occasional*.

Processing which is on a regular basis, e.g. collecting membership payment every three months, is not occasional if the data is stored between the payments. The reason is that even if the data is only "activily" processed every three months, the data is stored in between these processing situations, and storing data is also a form of processing of data.

The second condition is that the processing does not include, *on a large scale*, processing of sensitive data. Whether personal data on a large scale are being processed, is a concrete assessment taking into account for example the number of data subjects, the amount of data, how long the data

is to be processed, including if the processing is permanent, and the geografical scope of the processing.

The third condition is that it is unlikely that the processing would result in a risk to the rights of natural persons. Included in this assessment should be how the data is being processed, by which means and in which context.

According to Paragraph 2 subsection 2 the obligation to have a representative does not apply to a public authorities or bodies.

In Paragraph 3 the role of the representative is laid down. The representative should 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.

The fact that the controller or processor has a representative does not exclude the data subject from contacting the controller or the processor themselves.

It should also be noted that the designation of a representative does not exclude legal actions against the controller or the processor themselves in connection to consequences of processing of personal data.

See also recital 80 in GDPR.

Processor

Article 41
The Article is basen on Article 28 in GDPR. Similar provisions are in Article 31 in the current Act and in the Executive Order issued on the basis of Article 31 (7).

The Article defines the conditions when a controller uses a processor.

Paragraph 1 defines which processors the controller can use and lays down that the controller should 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

The provision sets out as a condition that the controller – in addition to ensuring that the processing by the controller is in line with the Act – should ensure that the processing that a processor carries out on behalf of the controller, is in line with the Act. This is without prejudice to Article 46 on security of processing which lays down an obligation for the processor to ensure an appropriate level of security.

How a controller should ensure that the processor provides sufficient guarantees is a case by case assessment based on the risk posed by the processing. In some cases it would be enough that the processor in writing certifies that appropriate technical and organisational measures are implemented, while in other cases it may be necessary to get a third party certification.

Paragraph 1 entails – in conjunction with Article 7 (2) on accountability – that the controller both prior to the processing and at the time of the processing itself has the obligation to continuously check that the processing of the processor is in line with the Act.

In practice the controller can use the contract, cfr. Paragraph 2, as a starting point for the continuous checks.

As is the case under the current Act Paragraph 2 lays down that processing by a processor should be governed by a contract or other legal act that is binding on the processor with regard to the controller. The contract should make clear the division of tasks, work and responsibility between the controller and the processor.

In Paragraph 2 subsections 1-9 it is detailed what the contract between the controller and the processor at least should contain. These are the boundaries the processor should work within.

According to Paragraph 2 subsection 1 the contract should stipulate the the processor only processes the personal data on instructions from the controller. This is in line with the general division of tasks between the parties, including the fact that it is the controller who decides the purposes of the processing, cfr. Article 6 (6).

The instructions from the controller should be documented. The requirement of documented instructions does not apply if the processor is required to process the data by law. In these cases the processor should inform the controller of that legal requirement before processing, unless that law prohibits such information.

According to Paragraph 2 subsection 2 the contract should ensure that persons authorised to process the personal data are under an obligation of confidentiality. This could be an obligation of confidentiality based on a contract between the parties or based on obligation of confidentiality laid down in law.

According to Paragraph 2 subsection 3 the contract should stipulate that the processor respects the conditions referred to in Article 42 for engaging another processor.

Paragraph 2 subsection 4 lays down that the contract should ensure that the processor takes all measures required pursuant to Article 46.

This provision entails that the controller and processor at the time on entering into a contract should make clear which security measures are necessary in order to fulfill the requirements in Article 46. This means that the controller and the processor should make an assessment of the risks posed by the procesing, cfr. Article 46, in order to ensure an appropriate level of security. These security measures could be described in the contract.

This does not entail that the controller in detail should decide how a processor implements technical security measures etc., but that the controller also assesses the risks and the appropriate level of security.

The continous checks the controller should have of the processor in order to ensure that the processor provides sufficient guarantees, cfr. Paragraph 1, can therefore be based on what is stated in the contract on which security measures should be in place.

In Paragraph 2 subsection 5 it should be stipulated in the contract that the processor should assist 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. This entails that the contract should describe how the processor to the extent possible - taking into account the nature of the processing – assists the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter 4.

According to Paragraph 2 subsection 6 the processor should assist the controller in ensuring compliance with the obligations pursuant to Articles 46-52. Account should be taken of the nature of processing and the information available to the processor.

In Paragraph 2 subsection 7 the contract should stipulate whether the processor – at the choice of the controller – should delete or return all the personal data to the controller after the end of the provision of services relating to processing, and should delete existing copies unless law requires storage of the personal data.

Finally according to Paragraph 2 subsection 8 and 9 it should also be stipulated in the contract that the processor should make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article, and allows for and contributes to audits, including audits by the controller or auditors on behalf of the controller.

According to Paragraph 3 the processor should immediately inform the controller if, in its opinion, an instruction infringes applicable law.

If a processor infringes this Act by determining the purposes and means of processing, the processor according to Paragraph 4 should be considered to be a controller in respect of that processing. It is provided that this is without prejudice to Articles 77-79. This entails that the processor could be punished or could be liable for compensation if the processor by determining the purposes of processing infringes the Act.

If a processor as described in Paragraph 4 goes from being a processor to being a controller, this entails that the “new” controller should fulfill all the conditions in the Act, including have a legal basis for the processing. If the new controller does not have a legal basis for the processing, the processing infringes the Act.

See also recitals 79 and 81 in GDPR.

Article 42
In Paragraph 1 it is laid down that the processor should not engage another processor without prior specific or general authorisation of the controller. The authorisation should be in writing.

In the case of general written authorisation, the processor should 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

The provision mirrors that it is the controller who should ensure that personal data is processed in line with the Act and that the controller therefore also should have the final word in deciding who processes the data.

In Paragraph 2 it is laid down that if 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. This is to ensure that the level of security is not lowered even if the processing takes place further away from the controller.

Article 43
In Paragraph 1 it is proposed that the minister after having obtained the opinion of the supervisory autority may lay down standard contractual clauses for the matters referred to in Articles 41 (2) and 42 (2).

In Paragraph 2 it is laid down that the contract between the controller and processor may in full or in part be based on the standard contractual clauses layed down by the minister responsible for data protection. It is also laid down that the contract between the controller and processor should be in writing, including in electronic form.

Also the provision on the processor and the relation to the controller is to be detailed by the Data Protection Authority. To the extent relevant the Data Protection Authority may use the guidelines issued by the Danish Data Protection Authority on the subject and the contract-template the Danish Data Protection Authority has issued may also be used as inspiration for this work.

Records of processing activities

Article 44
The Article is bases on Article 30 in GDPR. No similar Article i sin the current Act. However Article 4 (1) in the Executive Order on security in relation to processing of personal data lays down that in connection to a assessment of risks there should be records of the types of personal data being processed.

The provision entails that the controller and processor should keep records of processings.

The requirement of records replaces the obligation to notify the Data Protection Authority of processing. The reason for not continuing the obligation to notify and replacing this with an obligation to keep records, is in line with the principle of accountability which GDPR is based on. See point 1.4.2. in the general commentary.

In Paragraph 1 it is laid down that the controller should maintain a record of all *processing activities* under its responsibility. The obligation applies to all controllers regardless of whether a processor is used or not.

In the records the controller should keep the information listed in Paragraph 1 subsections 1-7. This entails that the record should contain the name and contact details of the controller (no. 1), the purposes of the processing (no. 2), a description of the categories of data subjects and of the categories of personal data (for example *contactinformation* rather than the actual e-mailadress,

phonenumber etc.) (no. 3), the categories of recipients including recipients in foreign countries, third countries or international organisations (no. 4), transfers of personal data to a foreign country, a third country or an international organisation (no. 5), the envisaged time limits for erasure of the different categories of data (no. 6), and a general description of the technical and organisational security measures put in place (no. 7).

In Paragraph 2 it is proposed that also the processor should keep records. However these records should cover all *categories of processing activities* carried out on behalf of a controller. The obligation for the processor is more leniant than the obligation for the controllers whose records should cover all *processing activities.*

The processors records are not as extensive as the controllers records. The information to be kept is the name and contact details (no. 1), the categories of processing carried out (no. 2), transfers of personal data to a foreign country, a third country or an international organisation (no. 3), and a general description of the technical and organisational security measures put in place (no. 4).

Only relevant information should be kept. This means that it is not necessary to keep in the records that the information is not transferred etc.

It is for the controller and processor to decide how the records are kept. However in Paragraph 3 it is stipulated that the records should be in writing, including in electronic form and that they should be made available to the supervisory authority on request.

The advantage of keeping records – in addition to ensuring that the controller and processor at all times know which data is being processed and to which purposes etc. – is that the supervision is made easier for the Data Protection Authority. With the records the Data Protection Authority can quicly get an overview of which processing is taking place etc. Records will therefore be an important part of the supervision by the Data Protection Authority.

According to Paragraph 4 the obligation to keep records should also apply to the representative of the controller or processor. This means in relation to Paragraph 1 subsection 1 and Paragraph 2 subsection 1 that name and contact details should include representives and Data Protection Officers.

Article 45
In Article 45 exceptions from the obligation to keep records is laid down.

It is proposed that the obligation should not apply to enterprises or organisations employing fewer than 250 persons. This entails that small and medium size enterprices as a starting point are not covered by the obligation.

Employees are people who the enterprice at any time has employed.

Enterprices coveres in these cases also organisations etc. Public authorities are however not covered by the exception. The obligation to keep records will therefore always apply to public records.

Although the exception seems wide this is not the case. It is laid down that the exception should nop apply in three instances. The conditions are not cumulative and the obligation therefore applies if one (or more) of the provisions are fulfilled.

According to subsection 1 the exception does not apply if the processing is likely to result in a risk to the rights of data subjects. It is not a precontion that there should be a big risk, only that there is a risk. This is a case by case assessment. Please see the special commentary to Article 40 (2) and piont 1.4.2. in the general commentary.

According to subsection 2 the obligation also applies if the processing is not occasional. Please see the special commentary to Article 40 (2) on the assessment of whether a processing is occasional.

According to subsection 3 it is provided that the exception does not apply if the processing includes sensitive personal data, cfr. Article 11 (1).

Article 45 entails that if an enterprice has fewer than 250 employees but conducts a processing that poses a risk (no. 1) or includes sensitive personal data (no. 3) the enterprice as an obligation to keep records according to Paragraph 1 (it the enterprice is the controller).

In these cases the obligation coveres the processing which poses a risk or covers sensitive data. Other processing by the enterprice is not covered. It is therefore the processing and not the enterprice as such that is covered by the obligation.

It is proposed that this Act has the same limit for the exception – 250 employees – as GDPR. This limit has been chosen even though there probably are only few enterprices in the Faroe Islands which have more than 250 employees.

The reason for not lowering the limit is that small and medium enterprices on the Faroe Islands should be covered by the same obligations as equivalent enterprices in the EU. If the limit on the Faroe Islands was set to be 50, 100 or 200 employees then this would entail that enterprices on the Faroes Islands would be covered by the obligation to keep records even though similar enterprices in the EU were not covered.

See also recital 82 in GDPR.

Security of processing

Article 46
The Article is based on Article 32 in GDPR. Similar provision can be found in Article 31 in the current Act and in the Executive order on security in relation to processing issued on the basis of Article 31.

As is the case for other provisions in this proposal, the Article on security is based on a risk based approach to data protection. This means that when assessing which level of security should b ein place account should be taken to the risks posed by the processing. This entails that the bigger the risks, the higher the requirements to the security measures.

In Paragraph 1 it is laid down that the controller and processor in the assessment should take 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.

This is a case by case assessment.

Please see point 1.4.2. in the general commentary regarding accountability and risk based approach.

Paragraph 1 lists examples of security measures which the controller or processor can put in place. Please note that these are examples and that it is for the controller or processor to assess whether one or more of the mentioned measures should be put in place or if other measures are more compatible with the processing which is to take place.

According to Paragraph 1 subsection 1 the measures could include the pseudonymisation and encryption of personal data.

Pseudonymisation should be understood in line with the definition in Article 6 (4).

Pseudonimised personal data is still considered personal data and therefore covered by the Act.

If personal data is anonomised in a way that the data subject no longer can be idenitfied and this is not reversible, the data is no longer covered by the Act.

Encryption – as well as pseudonymisation – of personal data entails that unauthorised persons do not understand the information because additional information is necessary in order to make the data intelligible.

Although encryption is an example of a security measure and not a requirement, it will still be advisable – as laid down in Article 11 (3) of the Executive order on security in relation to processing – that personal data which are transmitted electronically are encripted if confidentiality is required.

According to Paragraph 1 subsection 2 the security measures could cover the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The fact that the controller on an ongoing basis should ensure appropriate security measures demonstrates that the level of data protection is not static but can change over time and that the security measures therefore should be assessed continuously.

Integrity entails that is should be possible to check if the processing systems are correct, reliable and complete.

Availability entails that the processing system sand services should alwats be available to approved users, e.g. by ensuring a well-functioning back-up system.

Resilience entails technical and organisational resilience in processing systems and services, e.g. preventing detrimental insidences.

According to Paragraph 1 subsection 3 the security measures can also cover the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

This entails that the controller or processor should have an emergency preparedness which ensures that it is possible to access personal data in case of incidents such as fire, hacking or ransomware.

According to Paragraph 1 subsection 4 the security measures could cover a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
This entails that the controller and processor at a regula basis test, assess and evaluate firewalls, encriptions, acessibility control etc.

In Paragraph 2 it is laid down that essential for deciding the level on security is the risk presented by the processing. There is also guidance for the controller and processor in what to include in this assessment. In assessing the appropriate level of security account should 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.

In point 1.4.2. of the general commentary on accounability and risk based approach there are further examples of security measures that can be put in place to counter the risks presented by the processing. It is essential that the controller and processor make an overall assessment of the processing, the circumstances surrounding the processing and the risks for the data subject.

With this proposal the current Executive order on security in relation to processing will be repealed. However the content of the Executive order is for the most part in line with the new Article on security of processing in this Act. The current Executive order and practice according to the Executive order may therefore be used as inspiration when fulfilling the requirements in this Article – both for controllers and processors and for the Data Protection Authority when issuing new guidelines on security of processing.

As a part of security of processing it is laid down in Paragraph 3 that the controller and processor should 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. This covers both organisational and tecnical measures.

In Paragraph 4 there is a possibilty for the the minister responsible to 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.

While the provisions in Paragraph 1-3 regard the security of processing, Paragraph 4 primarily regards the protection of national security etc. The main aim of the provision is therefore not to protect individual data but to protect personal data which are of importance to national security etc.

The provision in Paragraph 4 replaces and renews the socalled war-provision in Article 31 (6) in the current Act. The Article in the current Act entails that 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.

The war-provision in the current Act therefore entails that systems should have a “red botton” which ensure that personal data could be destroyed in case the Faroe Islands were to be occupied.

Paragraph 4 does not include a requirement for a “red botton”. The provision instead entails that certain IT-systems are to be kept on the Faroe Islands and in that way ensures Faroese jurisdiction and accessibility for Faroese authorities to these IT-systems.

According to Paragraph 4 it is the minister responsible for data protection that should lay down the rules in consultation with the competent ministers. This entails that it is possible to ensure an uniform practice. This also entails that it is a requirement for the competent ministers when accuiring new systems or updating existing systems to contact the minister responsible for data protection in order to assess whether the system is covered by Article 46 (4).

When assessing whether the system is coverd account should be taken to whether the system geografically covers the whole country, which data is to be processed and the amount of data as well as the significance of the system for the society as a whole.

Paragraph 4 replaces Article 31 (6) in the current Act and applies to aquisition of IT-systems after the entry into force of this Act. This covers also tender and outsourcing of current IT-systems.

This entails that current systems covered by Article 31 (6) in the current Act will not be covered by the new provision unless the system is put out to tender.

See also recitals 28, 75-77, 83 and 87 in GDPR.

Notification of a personal data breach to the Data Protection Authority

Article 47
The Article is based on Article 33 in GDPR. A similar obligation which entails a notification of breaches to the Data Protection Authority can be found in Article 6 (3) in the Executive Order on security in relation to processing although the obligation is not as broad as the proposed Article in this Act.

According to Paragraph 1 the controller should notify personal data breaches to the Data Protection Authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Examples of personal data breaches could be:

- Unauthorised access to personal data
- The controller’s employee changes or erases personal data by a mistake

- The controller's employee on purpose or by mistake discloses information about one costumer to another costumer or
- The controller's server is hacked and the hacker gets access to personal data.

The controller should notify the Data Protection Authority *after* having become aware of the breach. This means that the breach has to have occured in order for the obligation to apply. A suspicion that a breach might have occured is not enough. If the controller has such a suspiction he is however obligated to investigate in order to stop a possible breach. In the assessment of whether a breach has occured account could be taken of whether the information to be provided to the Data Protection Authority cfr. Paragraph 4 is available.

The controller should without undue delay notify the Data Protection Authority. This means that the controller should notify as soon as it is possible. The controller should not wait until the 72 hours have passed if he or she has accessible information at an earlier time.

There are not many cases where it will not be possible for the controller to notify a breach within 72 hours after having become aware of the breach, cfr. Paragraph 5 about providing the information in phases. In those cases the controller should however be able to give reasons for the delay, cfr. Paragraph 1, second entence.

According to Paragraph 2 the controller should not notify the Data Protection Authority of the breach if it is unlikely that the breach would result in a risk to the rights and freedoms of natural persons. It is a concrete assessment to be made by the controller whether the breach is covered by Paragraph 2. It should however be fairly certain that the breach will not result in risks for the data subject.

The controller has the burden of proof in order to assertain that it is unlikely that the breach would result in a risk. The controller should be able to explain and state the reasons if the Data Protection Authority has another opinion.

A breach may not lead to risks for the data subject if the controller has rectified the breach quickly and has applied relevant security measures. An example could be that the controller has quickly deleted personal data from a website and has documentation that noone has accessed the website while the information was accessible. Another example could be that the controller has deleted necessary personal data but these data are still accessible in the back-up system.

According to Paragraph 3 the processor without undue delay after becoming aware of a personal data breach should notify the controller. The processor's obligation to notify is applicable in all cases – also in cases where the processor assesses it to be unlikely that the breach would result in a risk. This assessment therefore lies with the controller. When a processor has notified the controller, the controller should assess whether Paragraph 2 is applicable.

Paragraph 4 lists the information to be included in the notification from the controller to the Data Protection Authority.

The notification should 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 (no. 1), communicate the name and contact details of

the data protection officer or other contact point where more information can be obtained (no. 2), describe the likely consequences of the personal data breach (no. 3), and describe the measures taken or proposed to be taken by the controller to address the personal data breach (no. 4).

It is intended that the Data Protection Authority issues guidelines on the obligation to notify which in more detail explains the provision including which breaches should be notified.

If it is not possible to provide the information at the same time, the information may be provided in phases, cfr. Paragraph 5.

According to Paragraph 6 the controller should document any personal data breaches. The documentation be used when the the Data Protection Authority verifies compliance with this Article.

The obligation to document applies to *all* breaches. This means that also breaches that are not notified to the Data Protection Authority because they do not represent a risk to the data subject should be documented. This will enable the Data Protection Authority during an inspection to see which breaches have occured and how they have been handled.

According to plan, it will be possible to notify breaches electronically, e.g. via the Data Protection Authority's website.

See also recitals 85, 87 and 88.

Communication of a personal data breach to the data subject

Article 48
The Article is based on Article 34 in GDPR. There is no similar Article in the current Act.

Paragraph 1 entails that the controller when the personal data breach is likely to result in a high risk to the rights of natural persons – in addition to notifying the Data Protection Authority – should communicate the personal data breach to the data subject without undue delay.

In relation to the risk assessment please see point 1.4.2. in the general commentary.

The proposed Articles 47 and 48 entail that there are cases where the breach should be notified to the Data Protection Authority but not the data subject because the risk threshold is different. According to Article 47 the threshold is *a risk* and according to Article 48 the threshold is *high risk*. The reason is to not unnecessarily alarm the data subject.

According to Paragraph 2 the communication to the data subject referred to in paragraph 1 should 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. The reason for expressly laying down that the communication should be in a clear and plain language is that it might worry the data subject when receiving this information and therefore it is important to handle this in a rational way.

Paragraph 3 lays down exceptions of the obligation to communicate to the data subject. According to Paragraph 3 subsection 1 communication to the data subject is not required if 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.

Covered by this exception is for example a situation where a controller has lost a memory stick containing personal data but where the personal data are encrypted in such a way that it is not possible for unauthorised persons to break the encryption.

According to Paragraph 3 subsection 2 communication to the data subject is not required if the controller has taken subsequent measures which ensure that the high risk to the rights of data subjects is no longer likely to materialise.

Covered by this exception is for example if a controller updates IT-systems in a way that by mistake gives access to personal data via the internet. The controller becomes aware of the mistake and immediately closes unauthorised access. At the same time the controller initiates an investigation which shows that in the periode when the system was accessible only authorised persons visited the website.

According to Paragraph 3 subsection 3 communication to the data subject is not required if it would involve disproportionate effort. This requires a contrete proportionality assessment. The controller should assess the importance to the data subject to receive the information on one hand and the work required by the controller on the other hand. If it would involve disproportionate effort to communicate to each data subject, the controller should communicate publically, e.g. by press release, information on the website etc.

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

See also recital 86 in GDPR.

Data protection impact assessment

Article 49
The Article is based on Article 35 in GDPR. There is no similar Article in the current Act.

The Article entails that there in certain cases a data protection impact assessment should be carried out prior to the processing. A data protection impact assessment entails that the controller prior to the processing assesses the risks presented by the processing. This is to the extent possible protect the personal data of the data subject.

Paragraph 1 lays down that where *a type* of processing – 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. The Article is based on the risk based approach to data protection. See also point 1.4.2. in the general commentary.

According to Paragraph 1 the controller should make a concrete assessment of a processing operation and the risks posed by this processing. According to Paragraph 1 the obligation is especially relevant when using new technologies.

"New technologies" coveres for example the use of biometric data, including iris-scans, or communication with public auhtorities using apps. The technologi should objectivly be new. The fact that a controller uses a technology for the first time is not covered if the technology has been used by others.
It is however not a precondition that the technology is new in order for the provision to apply. If the technology is not new the controller should assess on a case by case basis if a data protection impact assessment should be carried out.

A data protection impact assessment may address a set of similar processing operations that present similar high risks.

Paragraph 2 lists three examples of processing operations which require a data protection impact assessment. Paragraph 2 is not exhaustive.

According to Paragraph 2 a data protection impact assessment is required in the case of 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 (no. 1), processing on a large scale of sensitive personal data, cfr. Article 11 (1) (no. 2), or a systematic monitoring of a publicly accessible area on a large scale (no. 3).

Paragraph 2 should be read in conjunction with recital 91 in GDPR which describes when a data protection impact assessment should be carried out. Generally it can be stated that the examples in Paragraph 2 in conjunction with Paragraph 1 and recital 91 entail that the scope of the Article is narrow and that the controller therefore in most cases is not required to carry out a data protection impact assessment.

The Data Protection Authority will provide guidelines etc. on the requirement to carry out a data protection impact assessment in more detail, including providing guidance on when a data protection impact assessment should be carried out.

In Paragraphs 3 and 4 it is laid down that the Data Protection Authority should establish and make public lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and the kind of processing operations for which no data protection impact assessment is required. The lists will not be exhaustive.

Article 50
Article 50 lays down what a data protection impact assessment should contain.

Paragraph 1 entails that the data protection impact assessment should contain at least a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller (no. 1), an assessment of the necessity and proportionality of the processing operations in relation to the purposes (no. 2), an assessment of the risks to the rights of data subjects (no. 3), and 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 (no. 4).

Paragraph 1 subsection 1 entails that there should be a systematic description of the envisaged processing operations which cover personal data. The personal data should be clearly described and defined. The impact assessment should also include a decription of the purposes of the processing, including the legitimate interest pursued by the controller.

The purpose of paragraph 1 subsection 2 is to ensure that only personal data which is necessary to the processing are being processed and thereby preventing unnecessary dataaccumulation by the controller.

According to Paragraph 1 subsection 3 the impact assessment should contain an assessment of the risks to the rights of data subjects. This means that the rights of the data subject should be weighed in the assessment of a envisaged processing operation.

Paragraph 1 subsection 4 should be read in conjunction with subsection 3 because the measures set in place should counter the risk posed by the processing.

The controller could seek the views of data subjects on the intended processing, if the controller finds this appropriate. If the controller choses to seek the views of data subjects this should be without prejudice to the protection of commercial or public interests or the security of processing operations.

According to Paragraph 2 the controller should carry out a review if there is a change of the risk represented by processing operations to assess if processing is performed in accordance with the data protection impact assessment. This entails an obligation for the controller to continuously ensure that the processing is in accordance with the impact assessment.

Article 51
In Article 51 it is laid down that there is no need for a data protection impact assessment if such an assessment has already been carried out as part of a general impact assessment in the context of the adoption of a law

This entails that the general assessment that has be made when adopting legislation is sufficient.

On data protection impact assessments (Articles 49-51) see also recitals 75-77, 84, 89-93 and 95 in GDPR.

Prior consultation of the Data Protection Authority

Article 52

The Article is based on Article 36 in GDPR. The Article is closely linked to the provisions on data protection impact assessments and therefore there is no similar Article in the current Act although consultation with the Data Protection Authority – in connection to authorisations or consultations – is a part of the current legislation.

Paragraph 1 entails that 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 the controller should consult the Data Protection Authority prior to processing.

The obligation to prior consultation therefore only applies in cases where the impact assessment indicates that the processing would result in a high risk for the data subjects and where the controller cannot mitigate this risk and choses to continue with the processing.

If the impact assessment indicates that the processing would result in a high risk for the data subjects the controller could change the processing or set out security measures to ensure that the risk will not be high. This would entail that there will be no obligation to consult with the Data Protection Authority.

Paragraph 2 lays down time limits for the Data Protection Authority in cases where the Data Protection Authority is of the opinion that the intended processing – in which the Data Protection Authority has been consulted – would infringe this Act, because the controller has not identified or mitigated the risk sufficiently. It is laid down that the Data Protection Authority within these time limits should provide written advice to the controller or processor and may use any of its powers referred to in this Act.

There is not an obligation for the Data Protection Authority to provide written advice if the Data Protection Authority assesses that the processing is in line with the Act. The Data Protection Authority should however in all cases comply with general administrative law and the conditions provided therein.

If the Data Protection Authority does not give advise within the time limits set out this does not entail that the Data Protection Authority will be excluded from using its powers referred to in this Act in regards of that processing. No reply from the Data Protection Authority should therefore not be understood as a general authorisation or seal of approval o fall aspects of the processing operation put before the Data Protection Authority. It will still be the controller – and not the Data Protection Authority – that is responsible for ensuring that the processing operation at all times is in line with the Act, cfr. also point 1.4.2. in the general commentary.

Paragraph 3 lays down which information the controller should provide the Data Protection Authority when consulting pursuant Paragraph 1. This is information that gives the Data Protection Authority the possibility to assess the processing. The controller should for example provide the purposes of the intended processing (no. 2), security measures (no. 3) and the data protection impact assessment (no. 5).

See also recitals 94-96 in GDPR.

Designation of the data protection officer

Article 53
The Article is based on Article 37 in GDPR. There is no similar Article in the current Act.

The data protection officer is a new character in Faroese data protection legislation. The data protection officer (DPO) is among other things tasked with guiding the controller on all issues

regarding data protection and is thereby a part of ensuring that personal data is processed in a secure manner.

Article 53 lays down in which cases DPO's should be designated.

According to Paragraph 1 subsection 1 the controller and the processor should designate a data protection officer where the processing is carried out by a public authority or body. Public auhtority or body should be understood in line with Article 1 (1) in the Act on Public Administration. Paragraph 1 subsection 2 and 3 lays down in which cases private entities should designate a DPO.

According to Paragraph 1 subsection 2 a DPO should be designated when 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.

According to Paragraph 1 subsection 3 a DPO should be designated when the core activities of the controller or the processor consist of processing on a large scale of sensitive data, cfr. Article 11 (1).

In order for a private entity to be covered by the obligation to designate a DPO three conditions should be fulfilled.

In Paragraph 1 subsection 2 and 3 include two common conditions. In both provisions it is laid down that the processing of personal data is the *core activity* of the controller or processor and that the processing is on *a large scale*.

The first condition of *core activity* entails that the processing of personal data should be the main activity of the entity and not only a "side-activity".

This entails that although an entity processes personal data on a regular basis this does not always mean that the condition of core activity is fulfilled. For example as a starting point it is not a core activity when an entity in connection with costumerrelations, sale or employment matters processes personal data. However it is a core activity if the controller or processor offer a product which entails the processing of personal data.

Examples of entities whos core activity is processing of personal data are entities who offer hosting of personal data, including providers of market surveys. Also in cases where the product is inseparably intertwined with the processing of personal data this could be a core activity. This could be insurance companies, who offer insurance on the basis of collected personal data. Also for providers of telecommunications and internet processing of personal data is a core activity.

The second condition of personal data being processed on *a large scale* is a case by case assessment.

In recital 91 in GDPR it is stated that processing on a large scale covers in particular large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk. It is further stated that the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer

Covered by the notion *on a large scale* is for example processing of personal data in a hospital. As a starting point also processing of data on costumers of insurance companies or banks should be considered being on *a large scale.* The same applies to providers of telecommunications and internet.

In conclusion the assessment of whether a processing is on a large scale should be based on the amount of information, the number of data subjects and the time in which the personal data is to be processed. Also the geografical scope can be included in the assessment.

In addition to the common conditions that the processing should be a core activity and be on a large scale there is also a third condition which should be fulfilled before an entity has the obligation to designate a DPO.

The third condition is that the processing operations require regular and systematic monitoring of data subjects (Paragraph 1 subsection 2) or consist of processing on a large scale of sensitive data, cfr. Article 11 (1) (Paragraph 1 subsection 3).

Processing operations which require regular and systematic monitoring of data subjects coveres for example tracking of behavior on the internet, including tracking which enables the profiling of a data subject with the aim of analysing or predicting aspects concerning behavior, personal preferences and interests. Regular and systematic monitoring can also take place outside the internet. Covered are also providers of telecommunications and internet and associated services, the monitoring of fitness- and health information on portable devices, profiling for riskassessments (e.g. for bankloans or insurance), loyalty programs etc.

In order to be covered by Paragraph 1 subsection 3 processing should cover sensitive data, cfr. Article 11 (1).

If the three conditions are fulfilled a private entity should designate a DPO.

Paragraph 1 lays down in which cases controllers and processors are obliged to designate a DPO. It is however possible to designate a DPO in other cases as well.

If a controller or processor choses to designate a DPO the rules in Article 54-58 should be complied with. The reason is that if an employee has the tasks and the responsiblities of a DPO then the employee should have the same protection. The employer can therefore not have the benefits without also being covered by the obligations.

According to Paragraph 2 a group of undertakings may appoint a single DPO and according to Paragraph 3 public authorities or bodies may designate a single DPO for several such authorities or bodies, taking account of their organisational structure and size.
Explicitly providing that group of undertakings or public authorities can share a single DPO does not entail that a shared DPO is excluded in other cases. It is possible for other organisations to have a single DPO. It is also possible for municipalities to have a single DPO.

It is however a fundamental condition for the designation of a shared DPO that the DPO can perform his or her tasks according to the Act in sufficiant manner, including that this does not result in a conflict of interests.

See also recitals 24, 91 and 97 in GDPR.

Article 54
Article 54 lays down qualifications to be fulfilled by the DPOs.
According to Paragraph 1 the DPO should be designated on the basis of professional qualities. This includes in particular expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in this Act.

This entails that the person who is designated should at least have an education and experiences that qualify the person to assess whether processing and intended processing is in line with the Act. The person should also be qualified to fulfil the tasks referred to in Article 58.

In order to fulfill these conditions the starting point is that the person should have legal qualifications in regards to data protection and also has experiences in this field. On which level these qualifications should be depends on the processing of personal data, including amount of data, sensitivity and complexity. It is not a requirement that the DPO is a lawyer (university degree). This will be for the controller or processor to asses. In some cases it might be sensible that the DPO has a technical education or certain technical abilities.

According to Paragraph 2 the DPO may be a staff member of the controller or processor, or may fulfil the tasks on the basis of a service contract (as a consultant).

The proposal does not entail that the controller or processor should hire new employees. The tasks of the DPO may be fulfilled by current employees in addition to other tasks, cfr. special commentary to Article 55.

According to Paragraph 3 the controller or processor should publish the contact details of the DPO and communicate them to the Data Protection Authority. This is to ensure tranparency and to ensure that data subjects always know – or easily can find out – who the DPO is and where they can turn.

Position of the data protection officer

Article 55
The Article is bases on Article 38 in GDPR. There is no similar Article in the current Act.

In Paragraph 1 it is laid down that the controller and processor should ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. This can be ensured by having fixed internal procedures etc. on all questions regarding data protection.
The provision ensures that the DPO is properly involved in all questions regarding compliance with this Act and other rules on data protection, including internal policies.

Providing that the DPO should be involved in a *timely manner* entails that the DPO should have the time to familiarize with the case and give comments etc. *prior* to initiating the processing.

According to Paragraph 2 the controller and processor should support the data protection officer in performing the tasks referred to in this Act.

This entails that the DPO should have the time to take care of the tasks and that enough money is set aside to perform these tasks. How much time, effort and money should be set aside for this task is a concrete assessment, which should be based on the size of the company or authority, which processing operations take place, the complexity of the processing and the risks presented by the processing.

The controller and processor should also support the DPO in maintaining his or her expert knowledge. This can be with appropriate possibilities of training. The controller and processor should also give the DPO access to personal data and processing operations because this is necessary in order for the DPO to fulfill his or her tasks.

It is important that the DPO can function with independance. The importance of the independance is reflected in recital 97 in GDPR.

As a part of the DPO independance it is laid down in Paragraph 3 that the controller and processor should ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. It is also laid down that the DPO should not be dismissed or penalised by the controller or the processor for performing his tasks.

The fact that DPOs should not be dismissed or penalised by the controller or the processor for performing their tasks provides the DPOs with a special security that other employees do not have and entails that the employers managerial rights are reduced. The protection provided for DPOs resembles the protection provided for staff representatives in the performance of representative tasks. This protection is provided in order to ensure that the DPOs can fulfill their tasks in a way to better the level of data protection.

The provision does not provide an unconditional protection against dismissal. DPOs may therefore be – like other employees – dismissed if they do not fulfill their (other) tasks or if they do not comply with the work contract.

As explained in the special commentary to Article 54 the proposal does not entail that the controller or processor should hire new staff for the DPO position. In most cases there will not be a full time position but can be compared to staff representatives or safety representatives.

In Paragraph 4 it expressly laid down that the DPO may fulfil other tasks and duties. This entails that an employee of the controller or processor may fulfill the tasks as DPO in addition to other work.

Paragraph 4 also lays down that the controller or processor should ensure that any such (other) tasks and duties do not result in a conflict of interests which would entail that the DPO cannot fulfill the tasks with complete independance. This entails that the DPO cannot at the same time have the responsibility that the processing is in line with the Act. This is the responsibility that usually is placed with the IT-manager who can therefore not at the same time be the DPO.

Article 56
As a part of the DPO independance it is laid down in Paragraph 1 that the DPO should report directly to the highest management level of the controller or processor. The DPO can report on a regular basis or on a case by case basis as the company or authority see fit.

What the highest management level is depends on the structure of the controller or processor.

In private companies who have a board of directors or a manegement, it is the director who takes care of the day to day business that is the highest management level although it is structurally the board of directors who have the top power in the company.

For public authorities it is the highest administrative management. In minicipalities the DPOs report to the councilors without prior discussions in a certain committee.

According to Paragraph 2 data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.

Article 57
The Article lays down a special obligation of secrecy for DPOs designated under Article 53 (1), subsection 2 and 3. It is laid down that these DPOs may not without justification disclose or exploit data into which they have obtained insight in connection with the exercise of their duties as DPOs.

DPO designated by public authorities are covered by the obligation of secrecy which applies to all public employees in Articles 152 and 152a-152f in the Criminal Code.

Tasks of the data protection officer

Article 58
The Article is based on Article 39 in GDPR. There is no similar Article in the current Act.

While Articles 55-57 in more general terms lay down the role of the DPO, Article 58 more specifically lays down which tasks the DPO *at least* should have. DPO may have more tasks than the ones mentioned. It is however important to ensure that the DPOs have the competances and the ability to take care o fall the tasks and do it in a way that does not infringe Articles 54-57.

According to Paragraph 1 the DPO should at least inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Act (no. 1), monitor compliance with this Act and other data protection provisions (no. 2), provide advice where requested as regards the data protection impact assessment and monitor its performance (no. 3), cooperate with the Data Protection Authority (no. 4), and act as the contact point for the Data Protection Authority on issues relating to processing (no. 5).

It should be noted that even though the DPO should monitor compliance with this Act, it is not the responsibility of the DPO to ensure that processing is in compliance with the Act. The responsibility still lays with the controller, cfr. Article 7 (2) and Article 37 and the special commentary to these Articles. If the DPO becomes aware of processing which is not in compliance with the Act, he or she should inform the highest level of manegement, cfr. Article 56.

According to Paragraph 2 the DPO in the performance of his or her tasks should have due regard to the risk associated with the processing taking into account the nature, scope, context and purposes of processing. See also point 1.4.2. in the general commentary.

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

The Chapter is in large based on Chapter 5 in GDPR. Adjustments have be made for the provisions to be adapted to the Faroe Islands which are not members of the EU.

Chapter 5 in the current Act contains rules on the transfer of personal data to foreign countries. Some changes are proposed, cfr. point 1.4.8. in the general commentary and the special commentary below. The most prominent change is that it is proposed to distinguish between foreign countries and third countries when personal data is to be transferred from the Faroe Islands.

The rules on transfer of personal data from the Faroe Islands are to ensure that the level of protection provided by this Act is not lowered. The starting point is therefore that personal data can only be transferred to countries that have – at least – the same level of protection. This entails as a starting point that the rules laid down in this Act should also be fulfilled when personal data are transferred onwards from the country to which they were transferred from the Faroe Islands.

The rules on transfer should also ensure that data can be moved freely when the level of protection is adequate. This i sin line with the aim of the proposed Act, cfr. Article 1.

When personal data are transferred from the Faroe Islands this should hava a legal basis in Chapter 6 in this Act in addition to fulfilling the other rules laid down in this Act, including the rules on lawfulness of processing.

Transfers of personal data to foreign countries

Article 59
In Article 59 it is proposed that transfer of personal data to foreign countries should not require any specific prior authorisation. Foreign countries means countries which are a member of the European Union (EU) or the European Economic Area (EEA), cfr. Article 6 (14).

The reason for proposing that these transfers should not require any specific prior authorisation is that the level of protection in these countries is assessed to be high and to provide data subjects on the Faroe Islands an adequate level of protection.

The provision entails that if the conditions for processing of personal data in this Act are complied with, including lawfulness of processing, the personal data can be transferred to foreign countries without prior authorisation from the Data Protection Authority. It is however laid down in the provisions on notification to the data subject and access that the data subject should be informed of the transfer. This entails that the data subject always knowns if personal data relating to him or her are transferred from the Faroe Islands.

It should also be noted that personal data *from* the EU can be transferred to safe third countries[2] without prior authorisation. Personal data can therefore now – and also in the future if the Faroe Islands continue to be a safe third country – be transferred from the EU to the Faroe Islands without prior authorisation from the relevant Data Protection Authority.

This change compared to the current Act lightens the administrative burden for especially private companies which communicate with EU-countries and which will no longer be obliged to notify the Data Protection Authority of the transfer or get prior authorisation (for sensitive data).

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

Article 60
The Article is based on Article 45 in GDPR. A similar provision can be found in Article 16 in the current Act.

When personal data are to be tranferred to third countries – this means countries which is not a member of the European Union (EU) or the European Economic Area (EEA), cfr. Article 6 (15) – a legal basis should be found in Articles 60-63.

The starting point is that basis for the transfer should be found in Article 60. If a legal basis cannot be found in Article 60, then Article 61 may be applicable. If a legal basis cannot be found in Article 61, then Article 62 may be applicable etc.

If there is no legal basis applicable in the mentioned Articles, the personal data cannot be transferred. In addition to a legal basis for the transfer, the controller should comply with the other provisions in this Act, including lawfulness of processing.

In Paragraph 1 it is laid down that a transfer of personal data to a third country or an international organisation may take place without any specific prior authorisation if the minister 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.

The third countries etc. subject to the decisions by the minister are called *safe third countries*. Compared to the current Act it is expressly laid down that the minister – in addition to deciding that a whole country ensures an adequate level of protection – may decide that a territory or one or more specified sectors within a third country or international organisations ensure an adequate level of protection.

As explained in point 1.2.3. in the general commentary a transfer of personal data to safe third countries under the current Act should be notified to the Data Protection Authority or require prior authorisation from the Data Protection Authority.

With the proposal for Article 60 this will be changed. If the minister has decided that a third country, a territory or one or more specified sectors within that third country or international organisations is safe, then the transfer of data does not require notifiacation or prior authorisation.

[2] Safe third countries: Third countries which have received an adequacy-decision from the Commission

According to Paragraph 2 the minister 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.

It is proposed that the minister – as the case is today – in an executive order lays down which countries ensure an adequate level of protection.

In Article 45 in GDPR in details lays down what the European Commission should take into account when deciding whether the level of protection in a third country is adequate. Article 45 in the GDPR is based on case law from the Court of Justice of the European Union. It is proposed that the minister should take into account the same issues when assessing the level of protection. This way pratice will be the same on the Faroe Islands and in the EU.

When assessing the adequacy of the level of protection, the minister should take account of the following elements:

1) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
2) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Faroe Islands; and
3) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

It is proposed that when the European Commission has decided that a third country etc. ensures an adequate level of protection, the minister may take that decision into account in the assessment of whether the level of protection is adequate in a particular third country. This will entail that the safe third countries as a starting point will be the same countries and that companies on the Faroe Islands therefore will have the same basis for their business as companies in the EU.

According to Paragraph 3 the Data Protection Authority should, on an ongoing basis, monitor the level of protection in third countries etc. It is important that the Data Protection Authority monitors whether changes are in the third country which will entail that the adequacy decision should be amended. Also in these cases it will be relevant to monitor developments in the EU.

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.

When the minister receives a notification from the Data Protection Authority he or she should as quicly as possible decide whether changes should be made. The minister may in these cases decide that an adequacy decision be amended, e.g. not cover a whole country. The minister may also decide whether the amendment should be temporary or permanent.

It the minister repeals an adequacy decision all transfer to that country should stop. Transfer to that country may take place if the conditions in Articles 61-64 are fulfilled.
See also recitals 103-107 in GDPR.

Transfers subject to appropriate safeguards

Article 61
The Article is based on Article 46 in GDPR. A similar provision can be found in Article 17 (2) in the current Act.

The Article lays down when personal data may be transferred to third countries etc. that have not received an adequacy decision.

According to Paragraph 1 a controller or processor may – in the absence of an adequacy decision – 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.

The aim of the provision is to make sure that the controller or processor put in place measures to ensure that rules on data protection are followed, that enforcable data subject rights are accessible as well as effective legal remedies, including administrative remedies, are accessible on the Faroe Islands or in the third country.

The appropriate safeguards should amend the fact that the minister has not decided that the country has an adequate level of protection and that the country therefore as a staring point does not provide for appropriate protection.

Paragraph 2 lists how the controller or processor should provide for the appropriate safeguards.

According to Paragraph 2 subsection 1 the appropriate safeguards referred to in paragraph 1 may be provided for a legally binding and enforceable instrument between public authorities or bodies.

It is a requirement for the use of Paragraph 2 subsection 1 that the parties are public auhtories in the Faroe Islands and in the third country, that the instrument – an agreement regarding taxes, a memorandum etc. – is legally binding for the parties and that the instrument is enforcable.

In this instrument data subject rights and effective legal remedies should be ensured.

According to Paragraph 2 subsection 2 the appropriate safeguards may be provided for by a standard data protection clauses adopted by the minister responsible for data protection after receiving the opinion of the Data Protection Authority.

Eqivalent provisions in GDPR lay down that the European Commission or the Data Protection Authorities in the Member States may adopt standard data protection clauses.

The standard data protection clauses adopted by the minister after receiving the opinion of the Data Protection Authority may be based on data protection clauses adopted on EU-level.

It is important that the minister adoptes these data protection clauses in good time prior to the entry into force of this Act in order for the controllers to be able to adjust to the new rules.
The data protection clauses may be part of a broader contract betweem the parties. It is also possible for the parties to agree to more security measures etc. than provided for in the standard data protection clauses.

It the parties change the standard clauses it entails that it is no longer standard data protection clauses adopted by the minister, cfr. Paragraph 2 subsection 2 and the agreed clauses may therefore as a starting point not be the basis for transfer without (a new) prior authorisation.

If standard data protection clauses adopted by the minister are used when personal data are transferred to third countries, the controller or processor does not need prior specific authorisation.

According to Paragraph 3 the appropriate safeguards may also be provided for in other contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country etc. subject to the authorisation from the Data Protection Authority.

Thereby it is possible for the parties to enter into agreements not based on standard contractual clauses, but this also entails that clauses are subject to prior authorisation by the Data Protection Authority. This may be a time consuming process as the Data Protection Authority has to be sure that the provisions provide for appropriate safeguards.

See also recitals 108-109 in GDPR.

Derogations for specific situations

Article 62
The Article is based on Article 49 in GDPR. A similar provision can be found in Article 17 in the current Act.

It is laid down when transfer is specific situations can take place when there is no legal basis in Article 60 or in Article 61. If the conditions in Paragraph 1 are fulfilled transfer can take place in specific situations.

Please note that Article 62 is derogations for specific situations. This entails that this Article may not be used for regular and repeated transfers of data to third countries. Article 62 contains derogations and therefore has a narrow scope.

According to Paragraph 1 subsection 1 transfer may take place if 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 as the conditions in Articles 60 and 61 are not fulfilled.

Informing the data subject of the possible risks entails that the data subject consents on an informed basis.

Transfer may also take place if 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 (no. 2), if 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 (no. 3), if the transfer is necessary for important reasons of public interest (no. 4), or if 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 (no. 6).

According to Paragraph 1 subsection 5 a transfer may take place if the transfer is necessary for the establishment, exercise or defence of legal claims. Please see the special commentary to Article 12 (1) subsection 7 on how this should be interpreted.

On legal claim in regard to transfers to third countries it should be especially noted that a legal claim as a starting point can not be based on a judgment of a court or tribunal and any decision of an administrative authority of a third country. Decisions etc. by foreign authorities may only be enforced on the Faroe Islands if based on an agreement between the Faroe Islands and the third country on mutual legal assistance.

According to Paragraph 1 subsection 7 a transfer may take place if 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.

According to Paragraph 2 a transfer pursuant to paragraph 1, subsection 7 should not involve the entirety of the personal data contained in the register.

Paragraph 1 subsection 2 and Paragraph 2 entail that personal data from the population register may be transferred to a third country if the data subject requests this because the data subject has moved to a third country. However the whole population register may not be transferred to a third country on the basis of Paragraph 1 subsection 7.

Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

See also recitals 108-109 in GDPR.

Article 63
If there is no legal basis for the transfer in Articles 60-62 there is a last possiblity in Article 63. The Article may only be used as a derogation and there is no other legal basis for the transfer. The scope of the Article is even more narrow than Article 62.

According to Paragraph 1 a transfer may only take place – if there is no legal basi sin Articles 60-62 – if the transfer of personal data to a third country etc. is not repetitive (no. 1), i fit concerns only a

limited number of data subjects (no. 2), if 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 (no. 3), and if 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 (no. 4).

The conditions are cumulative.
When applying this Article 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.

See also recitals 111-115 in GDPR.

Article 64
According to Paragraph 1 Article 62 (1), subsection 1-3 and Article 63 should not apply to activities carried out by public authorities in the exercise of their public powers.

The reason is that public authorities as a starting point should have a legal basis in public law and should not perform tasks their tasks on the basis of private law.

According to Paragraph 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

Article 65
The Article is based on Article 49 (5) in GDPR.

It is laid down that the Data Protection Authority in exceptional cases may prohibit, restrict, or suspend the transfer to a third country etc. of sensitive data if a decision has not been adopted concerning the adequacy of the level of protection.

The provision applies is specific cases which entails a narrow scope. It should be an exceptional situation which leads to the decision by the Data Protection Authority. The Data Protection Authority should always follow the rule of proportionality and take the least extensive decision that reaches the aim.

The decision by the Data Protection Authority may be based on unstability in the third country due to military coup or serious natural disaster.
The Danish Data Protection Authority has a similar possibility to take these decisions. Since the Danish Act entered into force it has not been used.

The Data Protection Authority should inform publically when taking decisions according to Article 65 and should also inform of the reason for the decision and for how long the decision will apply. The Data Protection Authority should should follow the situation closely and regularly assess whether the decision should be repealed.

Chapter 7
Data Protection Authority

Chapter 7 is based on Chapter 6 in GDPR.

The proposal for Chapter 7 on the Data Protection Authority also to a large extent continues the rules laid down in Chapter 10 in the current Act.

Organisational structure

Article 66
The provision lays down the organisational structure of the Data Protection Authority and is to a large extent based on Article 36 of the current Act.

Paragraph 1 lays down that the Data Protection Authority is an independant authority and should act with complete independence in exercising its tasks and powers. This is a requirement of functional independance.

The Data Protection Authority is a part of the public administration. This entails that the Act on Public Administration, Act on Public Access and other administrative laws apply to the functions of the Data Protection Authority.

The aim of laying down that the Data Protection Authority is an independant authority and should act with complete independence is ensuring an effective and reliable authority. The independence should be interpreted on the basis of this aim.

The Data Protection Authority is an independant authority means that the Data Protection Authority should not be an intertwined part of another (bigger) authority when performing tasks as a supervisory authority. This entails for example that the Data Protection Authority should not be a division in a bigger institution. It is important that the Data Protection Authority *as such* is independant.

The provision does however not entail that the Data Protection Authority could not structurally be part of a certain purview, e.g. be an authority hierarchically under a ministry and thereby a minister. The provision does also not entail that the authority cannot have housing with other authorities if the Data Protection Authority has it's own offices etc.

The Data Protection Authority structurally being part of a certain purview entails that it is the minister that ensures that the appropriation on the Budget Act is sufficient in order for the Data Protection Authority to function fully. This can be based on the opinion of the Data Protection Authority and does not influence the independance of the Data Protection Authority.

The Data Protection Authority should *act with complete independence in exercising its tasks and powers* which means that the decisions taken by the Data Protection Authority may not be brought before any other administrative authority and that the minister responsible for data protection may not give orders on how decisions should be made or on how supervisory tasks should be conducted. This is usually something a minister is empowered to do.

The requirement of independence of the Data Protection Authority is primarily independence from other parts of the executive branch, e.g. Government and ministries. When performing supervisory tasks the Data Protection Authority should therefore be professionally independant of the Government and ministries which therefore may not give orders in concrete cases or in general matters on the administration of this Act.

The requirement of independence entails that there is no other authority supervising the supervisory tasks of the Data Protection Authority. However other authorities are not excluded from supervising the Data Protection Authority's finances or whether the Data Protection Authority complies with rules applicable to public authorities. On this matter the Data Protection Authority is as other public authorities and therefore under the supervision of the Ombudsman and the National Auditor.

Decisons by the Data Protection Authority can also be put before the courts on the basis of the common rules in the Administration of Justice Act.

In addition to applying to the Data Protection Authority as such, the requirements of independance also apply to the director and the members of the Council who should remain free from external influence, whether direct or indirect, and should neither seek nor take instructions from anybody.

According to Paragraph 2 the Data Protection Authority, should consist of a Council and a Secretariat. It is also laid down that the Data Protection Authority is responsible for monitoring processing of personal data in accordance with this Act.

The provision should be read in conjunction with the rules on material and territorial scope in Chapter 1. The Data Protection Act has a wide scope and applies horisontally covering many different areas of law. This entails that the Data Protection Authority supervises in all these areas, which can be very different, however having in common that the rules on data protection should be complied with.

It is considered sensible to have the same structure as today with a Council and a Secretariat. It is however a precondition that the Council has a more prominant role and the work of the Council is more transparant.

It is the Council which in all cases of doubts determines how the Act should be interpreted and how case law in a certain area should be, while the Secretariat gathers information etc.

All matters of principle and matters of great importance should be put to the Council.

The Council and a Secretariat are *one* authority. Therefore decision taken by the Secretariat – on the basis of practice or guidelines from the Council – may not be brought before the Council.

According to Paragraph 3 the day-to-day business is attended to by the Secretariat, headed by a Director.

On the independance of the Director, please see above under Paragraph 1. In addition to this the common rules on incompetance in the Public Administration Act also apply to the Data Protection Authority, including the Secretariat.

Paragraph 3 should be read in conjunction with Paragraph 2 which entails that it is the Council which lays down how the Act should be interpreted while the Sectretariat handles the cases in the day to day business.

The day-to-day business coveres all the tasks listed in Article 68. The Data Protection Authority should when performing its tasks follow the common rules applicable to the public administration. In Paragraph 4 it is laid dowm that the Council should determine its own rules of procedure and the specific rules governing the distribution of work between the Council and the Secretariat.

It is thereby proposed that the Council should deside on its own how the work of the Council should be organised. The rules of procedure should contain rules on quorum, on how the meetings should be held etc.

The Council should meet on a regular basi sand at least every second month. The Council could be – in addition to examining concrete and general questions on data protection – also be informed of the dayly business of the Secretariat.

The Council should also lay down rules coverning the distribution of work between the Council and the Secretariat which means that the Council could decide that certain cases should be handled only by the Secretariat.

As described above all matters of principle and matters of great importance should be brought before the Council. Other cases may be handled by the Secretariat on the basis of guidelines that can be taken from the decisions made by the Council.

In order to ensure transparancy for the data subject the rules of procedure should be made public. It is also proposed that decisions etc. from the Data Protection Authority as a starting point should be made public, cfr. Article 73 and the special commentary to this Article.

Article 67
In Article 67 (1) it is laid down that the minister should appoint the Data Protection Council. When appointing the Council the minister should strive for independance and expertice.

Compared to the current Act it is proposed that two more members should be part of the Council which will have 5 in stead of 3 members. The reason is a wish for a broader representation which entails that more points of view are present in the interpretation of the Act and laying down practice. With more focus on information and promoting public awareness etc. it is considered sensible to have the municipalities and the private sector represented in the Council.

It is still a requirement that the chairman must be a lawyer, which means that the person should have a university degree in law (cand.jur). The reason is that data protection legislation is complicated and therefore at least one member should be a lawyer.

In addition to a law degree the minister should take into account whether the person has knowlegde of data protection legislation. This can be through work or training.

There is no specific educational requirement for the other members of the Council.

It is however proposed that the minister when appointing members should take into account that at least one member should have some kind of technical education or expertice. In addition to being a complicated legal area, data protection is also closely connected to technical solutions etc. Therefore it is necessary that this expertice is present in the Council.

The minister should also strive for that one of the members of the Council has knowledge of research and processing of personal data in this regard.

In addition to the members which the minister appoints without nomination, the minister should appoint two of the members on the nomination by the Accociation of Municipalities and the Faroe Employer's Association recpectively.

It is not laid down which education etc. these members should have. However it is important that these members – who represent the municipalities and the private sector – have knowledge of the area which they represent in addition to knowledge of data protection legislation.

Although the Council consists of 5 permanent members the Council is not excluded from laying down in the rules of procedure that in concrete cases a person with certain expertice can participate in the meeting. These persons can participate in the meetings in order to give the Council information and do not have voting rights.

According to Paragraph 2 the minister also appoints substitutes for the members. The Accociation of Municipalities and the Faroe Employer's Association should also nominate substitutes.

The members and the substitutes are appointed for a term of four years. Reappointment may take place two times.

The requirements of independance also apply to the members of the Council who should also remain free from external influence, whether direct or indirect, and should neither seek nor take instructions from anybody, cfr. the special commentary to Article 66 above. The common rules on incompetance in the Public Administration Act also apply.

The minister will appoint a new Council upon the entry into force of this Act. The current members will be a part of the Council until new members are appointed under this Act.

In Paragraph 2, 3. sentence it is laid down that the appointment of the chairman, the members and their substitutes should be based on their professional qualifications.

Tasks

Article 68
The Article is based on Article 57 in GDPR. The Article corresponds with Article 37 in the current Act.

Article 68 lays down the tasks of the Data Protection Authority. The list is not exhaustive. The Act has specific tasks for the Data Protection Authority in some Articles, e.g. Article 61 (2) subsection 2.

According to Article 68 (1) the Data Protection Authority should 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. It is the supervisory task of the Data Protection Authority which is laid down in this provision.

According to Article 68 (2) it is explicitly laid down that the Data Protection Authority should promote public awareness in relation to data protection. It is very important that it is a prioritized task for the relevant authority to promote public awareness. This can be done in general information campaigns, seminars and other ways. Also written guidelines on the Data Protection Act are an important part of this work. Awarenessraising helps highten the level of security and gives data subjects better protection.

The Data Protection Authority should also advise the government (Landsstýrið), the parliament (Løgtingið) and other institutions and bodies on legislative and administrative measures relating to the protection of personal data (no. 3) and promote the awareness of controllers and processors of their obligations under this Act (no. 4). This can be in both concrete matters and general guidelines.

According to Article 68 (5) the Data Protection Authority should conduct investigations where personal data is being processed. This includes investigations of processing by private companies and public authorities, including whether the processing is in line with the Act. The investigations may be conducted ex officio and may include supervisoriy visits.

According to Article 68 (6) the Data Protection Authority should monitor and inform of relevant developments regaring data protection on the Faroe Islands and abroad. This is a continuation of the current provision. The obligation to monitor developments under the new Act will be even more important in the future as the Act is based on EU-legislation and to the extent possible should be interpreted in line with the relevant EU-legislation.

The Data Protection Authority should also according to Article 68 (7) draw up and make public an annual report on its activities. The annual report is an important part of ensuring transparancy in the area.

See also recitals 123 and 132 in GDPR.

Article 69
The Article repeats Article 42 in the current Act. The provision does not correspond with an eqvivalent Article in GDPR. However it is an important part of GDPR that the supervisory authorities in the EU-member states co-operate with each other.

According to Article 69 the Data Protection Authority should co-operate with others authorities in the Faroe Islands and abroad, if relevant. Cooperation should be with both Faroese and Danish authorities on the Faroe Islands in addition to supervisory authorities in other countries. The cooperation can be in concrete cases as well as general issues.

Powers

Article 70
The Article is based on Article 58 in GDPR. The provision to a large extent corresponds with Article 38 in the current Act.

Article 58 devides the powers into three different kind of powers:

1) Investigative powers.
2) Corrective powers.
3) Authorisation and advisory powers.

Although Article 70 is not devided the same way as Article 58 in GDPR, the Data Protection Authority's powers correspond with the powers provided for eqvialent authorities in EU-member states.

It is always the Data Protection Authority that in each specific case decides how a concrete case should be handled and which power to use. The Data Protection Authority works on the basis of the general principle of proportionality which entails that the least intrusive power which can meet the goal should be used.

According to Paragraph 1 the Data Protection Authority can 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.

The provision gives the Data Protection Authority the possibility to issue warnings to controllers or processors prior to processing. It is in all cases the controller who has the responsibility of the processing and a warning does not entail that processing may not go ahead. It is rather an extra possiblity for the Data Protection Authority to make sure that everything is in order.

Paragraph 1 also gives the Data Protection Authority the possibility to issue reprimands after processing has taken place. This may be used in cases where processing which was not in line with the Act has taken place and has stopped again and it is not considered necessary to implement other measures.

Paragraph 2 repeats Article 38 (1) in the current Act and entails that the Data Protection Authority can order the controller or processor to discontinue processing operations and can also order the controller or processor to rectify or erase personal data or restrict processing of personal data. The provision entails tha the Data Protection Authority can ban certain processings and can order the controller or processor to rectify personal data.

According to Paragraph 3 the Data Protection Authority can order the controller or processor to bring processing operations into compliance with this Act within a specified period.

The specified period should be a case by case assessment based on thethe severity of the infringment of the Act and the extent of the changes the controller or processor have to implement in order to ensure that processing is in line with the Act.

Paragraph 4 repeats the current provision and entails that the Data Protection Authority can order the controller or processor to implement technical and organisational 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.

Article 71
The provision repeats Article 40 in the current Act.
Article 71 (1) and (2) are crusial for the Data Protection Authority's ability to supervise.

It is necessary in order for the Data Protection Authority to make decisions on an informed basis that the Data Protection Authority has access to all relevant information and may access premises. The Data Protection Authority can demand information etc. from both public and private parties.

According to Paragraph 1 the Data Protection Authority may demand being given all information of importance for its activities.

Paragraph 1 has not been changed compared to the current Act and the obligation for the controller and processor to provide information should still be administered in compliance with the prohibition on self-incrimination in Article 6 in the European Convention on Human Rights.

As a starting point Article 6 in the European Convention on Human Rights entails that a person is not obliged to give information if the person is suspected of a criminal offence which may lead to punishment.

It the Data Protection Authority is investigating a case, e.g. on the basis of a complaint, in order to assess whether there has been an infringement, and *before* anyone is suspected of an infringement which may lead to punishment, Article 6 in the European Convention on Human Rights does not apply.

Paragraph 2 gives the members and leading staff of the Data Protection Authority access to all premises of the controllers and processors.

The provision entails that the Data Protection Authority without any court order can access relevant premises. This could be the regular work place, storage buildings, technical warehouses and home work places. The members and leading staff should when accessing the premises have the possiblity to monitor processing and to look things up in filing systems.
The Data Protection Authority can on the basis of Paragraph 2 get access to premises both announced and unannounced supervisory visits. Usually the Data Protection Authority announces a supervisory visit 2-3 weeks prior to the visit.

The power to get access to premises without a court order is a quite radical power which should be used with caution and respect. This entails that as a starting point it should be the members of the Council or leading staff who are in charge of the investigation on location.

Decisions of the Data Protection Authority etc.

Article 72
The Article corresponds with Article 39 (3) in the current Act.

Article 72 entails that decisions of the Data Protection Authority may not be brought before any other administrative authority. The provision helps give the Data Protection Authority sufficient independance, cfr. also the special commentary to Article 66.

The provision coveres administrative decisions. Covered are concrete decisions in complaints regarding infringements of the processing provisions or the infringements of data subject rights. Opinions by the Data Protection Authority, guidelines etc. is not covered by this provisions as these are not administrative decisions.

The fact that the decisions by the Data Protection Authority may not be brought before another administative authority is without prejudice to the right of the individual to bring cases before the courts on the basis of the rules in the Administration of Justice Act.

Article 73
In Article 73 it is laid down that 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. The provision is new compared to the current Act although this a possibility that the Data Protection Authority is assessed to have already.

Article 73 does not contain an obligation for the Data Protection Authority to make public decisions and statements. However it is very important for the transparency in the data protection field that the Data Protection Authority to the extent possible publishes decisions and statements and this is the reason for the provision.

The publishing by the Data Protection Authority of decisions and statements is also very important for controllers and processors who are to comply with the Act. It will be an important instrument for those covered by the Act – and who have the responsiblity to ensure compliance with the Act – that they are able to get information on the practice of the Data Protection Authority and on how the Act is being interpreted in concrete cases and in general issues.

Covered by the provisions are decisions in concrete cases which in some way have public interest, e.g. because a matter of principle has been discussed in the Council. Also statements on general issues, e.g. investigations of processing of personal data in a certain branch of business or on how a certain provision is to be interpreted, should be made public.

The Data Protection Authority can make decisions etc. public on the Data Protection Authority website. Decisions which are made public should be anonymised and be made unrecognisable to the extent possible. The reason is that the aim is not to name and shame certain businesses and authorities but to make it easier for controllers and others to comply with the Act in accordance with the practice of the Data Protection Authority.

The publication should also be subject to Article 36 of this Act.

Article 74
The Article provides for an obligation to obtain the opinion of the Data Protection Authority when rules regarding the processing of personal data are being drafted. The opinion should be optain before the rules enter into force.

The provision does not provide for an obligation to obtain the opinion of the Data Protection Authority prior to public hearing. The Data Protection Authority can offer it's opinion at the same time as other parties.

It is probably already pratice that rules are sent to the Data Protection Authority to retreive an opinion as this follows from the government procedures for drafting legislation provided by the Prime Minister's Office.

Artice 75
According to Article 75 the minister 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.

Under the current Act it is not possible for the Data Protection Authority to require that communication with the Data Protection Authority is in a digital form. The provision will lighten the administrative burden of the Data Protection Authority.

Chapter 8
Remedies, liability and penalties

Chapter 8 is based on Articles 77-80, 82 and 84 in Chapter 8 in GDPR.

GDPR provides for general rules and to a large extent leaves it to the EU-member states to lay down more detailed rules in national legislation. The provisions provided for in this Chapter for the most part repeat current legislation and the assessment is that these rules are within the scope of the flexibility of GDPR.

The right to lodge a complaint

Article 76
The Article is based on Article 77 in GDPR and corresponds with Article 30 in the current Act.

It is laid down that 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. This applies to both public and private sector.
The Data Protection Authority should process the complaint, cfr. Article 68 (1) and can use its powers, cfr. Article 70. The Data Protection Authority should follow the general rules applicable to public authorities.

If the complaint is in regard to sector specific legislation the Data Protection Authority can contact the relevant authority in order to have a common understanding of the rules.

The data subject can logde a complaint on his own, but can also be represented by others according to the rules in the Public Administration Act on representation.

In addition to lodging a complaint with the Data Protection Authority the data subject can bring the question whether a controller or processor has infringed the Act before the courts. This is according to the common rules in the Administration of Justice Act.

According til Article 78 in GDPR the EU-member states should provide the data subject effective judicial remedy against a supervisory authority. This is not explicitly laid down in Article 76. However it is always possible for data subject – according to the common rules in the Administration of Justice Act – to bring decisions etc. from the Data Protection Authority to the courts. It is a precondition that the rules in the Administration of Justice Act are fulfilled.

See also recitals 141-143 and 145 in GDPR.

Compensation

Article 77
The Article is based on Article 82 in GDPR. The Article corresponds with Article 46 in the current Act.

As it is today it is proposed that there be culpa liability with reverse burden of proof (presumption of liability). This entails that the controller – or processor – should compensate damages which occur because unlawful processing takes place. Damages should not be paid if the controller/processor can prove that such damage could not have been averted through the diligence and care required when processing of personal data.

The general conditions for compensation should also be fulfilled, including the conditions of causality and foreseeability.

Article 77 coveres both material and non-material damages but it will as a starting point still be a requirement that the data subject has had some kind of financial loss.

If several controllers or one controller and one processor are responsible for the damage, each controller or processor shall be held liable in accordance with the common rules on compensation. IT also follows from these common rules that the data subject can claim full compensation from one controller or processor. Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors.

Compared to the current Act the data subject can claim compensation from the processor. Because it as a starting point always will be the controller who is responsible for the processing, a processor can only be liable for the damage caused by processing where he or she has not complied with obligations of this Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

See also recitals 146 and 147 in GDPR.

Penalty

Article 78
The Article is based on Article 84 in GDPR. The Article corresponds with Article 44 in the current Act.

Paragraph 1 provides that unless a higher penalty can 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 in this Act.

The reason for a imprisonment term of not exceeding six months (compared to 4 months in the current Act) is to align the imprisonment term with the term in Article 264 d in the Criminal Code. According to Article 264 d in the Criminal Code a person can be imprisoned for up til six months if he or she in an unauthorised way discloses messages or pictures which reveal personal matters concering a person or in any other way reveals circumstances about the person which should not be made public.

These infringements can be compared and should therefore be punished in the same way.

In line with Article 19 in the Criminal Code the provison covers both intentional and negligent infringements of the Acts.

It is proposed that infringements of the Act – both intentional and negligent – as a starting point should be punished with fines and that the punishment only in special cases is imprisonment. This might be the case if sentitive data on a large scale intentionally have been made public.

It should be noted that it is not a precondision that all infringments should be fined (or punished with imprisonment). The concrete circumstances in a case can lead to the Data Protection Authority – in stead of reporting the case to the police or issuing a fixed penaly notice – gives a warning or an order. Please see recital 148 in GDPR.

In regards of the size of the fine, this will be for the courts to decide in each specific case.

Article 83 (2) in GDPR lists circumstances which should be taken into account when supervisory authorities decide the size of the fine. This is e.g. the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage suffered by data subjects, duration of the infringement etc. These circumstances should also be taken into account when punishment is set in concrete criminal cases on the Faroe Islands. In addition Chapter 10 in the Criminal Code applies.

It is proposed that the size of fines will be considerably higher compared to the current situation. It is proposed that the level of fines on the Faroe Islands as a starting point should follow the developments in Denmark if there are on special circumstances which can lead to a different level. It should be noted that following the developments in Denmark does not necessarily mean in all cases that the size of the fine should be exactly the same. The size of the society and businesses should be taken into account.

The size of businesses and the benefits gained by the infringements should also be taken into account when deciding the level of the fine. It is not the aim of raising the size of fines that the fines get so high that the businesses go bankrupt if this Act is infringed.

It is important that the rules on data protection are taken seriously and raising the level of the fines is an important part of underlining the seriousness.

On the level of fines please see also point 1.4.10 in the general commentary.

Paragraph 1 subsections 1-7 lists the provisions where infringement can lead to punsihment. The articles listed are the same as the ones listed in the current Act.
It should be noted that the person that can be punsihed under Paragraph 1 as a starting point is the one responsible for the processing which is the controller. The controllers have obligations according to the Act that others cannot be punished for infringing. The Act however also holds obligations applicable for processors. If these obligations are not met, the processors can also be punished.

DPOs do not have the responsibility for the processing or the responsibility of ensuring that the processing is in line with the Act. The DPOs give advise and can therefore as a starting point not be punished according to this Act. Controllers and processors can however be punished if they do not have a DPO when this is required according to this Act.

According to Paragraph 2 violations of Article 57 shall be punished with a fine unless a higher penalty must be imposed according to other legislation. According to Article 57 DPOs 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.

This entails that infringment of Article 57 cannot be punished with imprisonment according to this Act.

According to Paragraph 3 penalties in the form of a fine may be prescribed by rules issued in pursuance of this Act.

Paragraph 4 provides that companies etc. (legal persons) may incur criminal liability according to the rules of Part 5 of the Criminal Code.

For public authorities Article 27 (2) in the Criminal Code applies. According to this Article public auhtorities may not be punished for infringements committed in their exercise of official authority. According to Article 27 (2) public authorities may only be punished in the exercise of activity that corresponds to or can be considered equal to activity carried through by private entities.

This is not changed with the proposal. THis entails that public authorities cannot be punished for infringements of this Act if the processing is part of their exercise of official authority, e.g .when the authority takes a decision.

According to Paragraph 5 the period of limitation for infringement of this Act or rules issued in pursuance of this Act is five years. This parts from the general rule in the Criminal Code which provides a periode of limitation of 2 years.

The reason for the prolonged period of limination is that it was the assessment of the Danish Police in 2018 when GDPR came into force that infringements of the Data PRotection Act may be extencive and complicated and go on for a long period. Therefore the period of limination should be 5 years.

The circumstances on the Faroe Islands are the same and therefore it is proposed that the period of limination for infringement of this Act should be 5 years.

See also recitals 149-152 in GDPR.

Fixed penalty notices

Article 79

The Article is partly based on Article 83 in GDPR. There is no similar Article in the current Act. The posiblity for the Data Protection Authority to issue fixed penalty notices is therefore new.

It is proposed that if the Data Protection Authority assesses that an infringement of this Act or rules issued in pursuance of this Act should be punished with a fine, the Data Protection Authority according to Paragraph 1 may issue a fixed penalty notice. It is precondition that 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, which may be prolonged.

A fixed penalty notice is a criminal justice decision and the condition for using this type of decision are strict. The reason is that fixed penalty notices differ from the way criminal cases usually are processed. As a starting point criminal cases are invesigated by the police. If there is a basis for further processing the cases is handed to the procecution service which decides if criminal charges should be brought. If criminal charges are brought the courts decide if a party is guilty and fixes the penalty.

The Administration of Justice Act has extensive rules on procedures in criminal cases which provide legal certainty for the individual. One of the main rules is that it is the courts that issue penalties. However the Administration of Justice Act in some cases allows for the procecution service to issue fixed penalty notices.

Article 79 allows the Data Protection Authority to issues fixed penalty notices. This deviates from the general principle that the police, procecution service and courts handle criminal cases. The advantage is that it will be the authority that on a day to day basis works with the Act and therefore has the expertice in the area that under certain conditions can conclude cases that will not lead to higher penalties than fines.

On reasons of legal certainty fixed penalty notices can only be used in special cases. It is a precondition that the case is suited to be concluded in this manner. This entails that the infringements should be *similar*, *simple* and without *evidentiary doubts*.

Suitable cases could for example be negligent publication of personal data on a website or infringement of the obligation to notify data subjects.

In addition to only being used i certain cases it is a precondition that 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.

Before the Data Protection Authority can issue fixed penalty notices, the courts should lay down the level of the fines to be used. This entails that the first cases of infringements of the specific Articles should be brought before the courts which decides the size of the fines for each infringement. This

means that the Data Protection Authority to begin with has to report the cases to the police and that the procecution service brings the cases to court. When the size of the fines is laid down by the courts, the Data Protection Authority can use this size of fines in fixed penalty notices in other cases.
It is precondition that the question of whether a case should lead to a fixed penalty notice should be discussed in the Council in each specific case.

According to Paragraph 2 the rules of the Administration of Justice Act on the requirements for the content of an indictment should also apply to a fixed penalty notice.

This is to ensure that a party that accepts a fixed penalty notice is informed in a sufficiant manner and knows what acceptance means.

It is also laid down that the rules of the Administration of Justice Act on the right of an accused to remain silent should also apply in these cases. If the party wishes to remain silent or does not declare acceptance of a fine, the case should be given to the police.

Paragraph 3 provides that where a fine is accepted, any further prosecution will be discontinued. This entails that the party cannot later be charged for the same infringement and that the same infringement may not be brought before the courts.

See also point 1.4.9. in the general commentary and the special commentary to Article 78.

Deprivation of right to run a business

Article 80
The Article is partly based on Article 84 in GDPR. With certain modifications the Article repeats Article 45 in the current Act.

It is laid down that 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.

Article 80 supplements Article 79 in the Criminal Code on deprivation of rights. Article 80 ensures that deprivation can take place in these cases. The assessment to be made is similar to the assessment that courts already make according to Article 79 (1) and (2) in the Criminal Code.

Article 79 (3) and (4) of the Criminal Code shall apply.

See also recitals 149-152 in GDPR.

Chapter 9
Entry into force

Chapter 9 holds only one Article. The Article is on the entry into force.

Entry into force

Article 81
It is proposed that this Act enters into force on 1 January 2021. At the same time Act no. 73 of 8 May 2001 on the processing of personal data will be repealed. Also executive orders issued on the basis of the Act from 2001 will be repealed at the same time.

This entails that all processing of personal data, which takes place from 1 January 2021 should fulfill the conditions of this Act. Controllers and others should therefore – prior to the entry into force – assess whether processing that is ongoing is in line with the new Act or if certain changes should be made.

Please note that this assessment may lead to the conclusion that the conditions are already fulfilled as the new Act on many points continues current legislation.

As explained in the special commentary to Article 38 on data protection by design and default the new Act does not entail that controllers and others should make investments in new systems in order to comply with the provision. It is however a precondition that the systems – as is the case today - should comply with the general conditions of the Act, e.g. the principles in Article 7.

According to Paragraph 2 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.

This provision entails that controllers and others which may have acted on an authorisation from the Data Protection Authority are given a longer period of adjustment. This only applies to processing that is already ongoing when the Act enters into force and which the Data Protection Authority has authorised.

Paragraph 3 provides that 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. This gives controllers and processors a longer period to get contracts in line with the Act.