Act No. 410 of 27 April 2017 as amended by Act No. 503 of 23 May 2018 and Act No. 506 of 23 May 2018

The official version was published in 'Lovtidende' (the Law Gazette) on 29 April 2017. Only the Danish version of the text has legal validity.

Act on the processing of personal data by law enforcement authorities (the Law Enforcement Act)[1]

WE MARGRETHE THE SECOND, by the Grace of God, Queen of Denmark make known that: Folketinget (the Danish Parliament) has passed and We have granted Our Royal Assent to the following Act:

Chapter I

General provisions

Part 1

Scope of the Act

1.-*(1)* This Act shall apply to the processing of personal data by the Police, the Prosecution Service, including the Danish Military Prosecution Service, the Danish Prison and Probation Service, the Independent Police Complaints Authority, and the courts, when the processing is carried out, in full or in part, by the means of automatic data processing, and to any other non-automatic processing of personal data that is or is intended to be contained in a filing system, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(2) This Act shall not apply to the processing of personal data performed on behalf of or by the intelligence services of the Police and the Danish Defence.

(3) This Act shall not apply to the processing of personal data by virtue of Union legal acts that has entered into force on 6 of May 2016 or prior to this date, within the field of judicial cooperation in criminal matters and police cooperation, and that regulates the processing of personal data between Member States and the access of the designated authorities to EU-information systems.

2. Any rules governing the processing of personal data in other legislation that provides higher safeguards for the protection of the rights and freedoms of the data subject shall take precedence over the rules laid down in this Act.

Part 2

Definitions

3. For the purposes of this Act:

1) Personal data: Any information relating to an identified or identifiable natural person (data subject).

2) Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

3) Restriction of processing: The marking of stored personal data with the aim of limiting their processing in the future.

4) Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

5) Filing system: Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

6) Competent authority: Any public authority or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The competent authorities in Denmark are the Police, the Prosecution Service, including the Danish Military Prosecution Service, The Danish Prison and Probation Service, the Independent Police Complaints Authority, and the courts.

7) Controller: The competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data.

8) Processor: A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

9) Recipient: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed so that the recipient hereafter independently determines the purposes and means of the processing of the disclosed data, whether a third party or not. However, public authorities, which may receive personal data in the framework of a particular request, shall not be regarded as recipients.

10) Personal data breach: Any 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.

11) Genetic data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

12) Biometric data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

13) Data concerning health: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

14) International organization: An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Chapter II

Rules on processing of data

Part 3

Processing of data

4.-*(1)* Data must be processed in accordance with good practice and taking into account the nature of the data.

(2) Data must be collected for specified, explicit and legitimate purposes, comprised by section 1(1), and may not be further processed in a manner that is incompatible with those purposes, however see section 5.

(3) The processed data must be relevant, adequate and not excessive in relation to the purposes for which they are collected and/or further processed.

(4) The processed data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data, which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(5) The controller must use all reasonable measures to ensure that personal data are not transmitted or made available if the data are inaccurate, incomplete or not kept up to date. For this purpose, the controller shall insofar as this is possible verify the quality of the personal data before they are transmitted or made available. As far as possible in all transmissions of personal data, necessary information shall be added, enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of the personal data, and the extent to which they are up to date. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted.

(6) The data collected cannot be kept in a form which permits identification of data subjects longer than is necessary for the purposes for which they are processed.

(7) The data collected must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures, see section 27.

(8) The controller shall be responsible for and be able to demonstrate compliance with subsections (1) – (7).

5.-*(1)* Subsequent processing of data for any of the purposes set out in section 1(1), other than that for which the personal data were initially collected shall be permitted in so far as the controller is the same or another competent authority and the processing follows from laws and is necessary and proportionate to that other purpose.

(2) Pursuant to subsection (1), data may furthermore be processed for the purpose of archiving in the public interest or for the purpose of historical, statistical or scientific use.

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

6.-*(1)* Where personal data are transmitted, the transmitting, competent authority lays down and informs about special conditions for the processing of data. Special conditions cannot be laid down solely on the basis of transmission to a recipient in another Member State.

(2) The processing of data received from a competent authority must not violate the specific conditions laid down by the transmitting, competent authority.

7. The data controller shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

8. The data controller shall, where applicable and as far as possible, make a clear distinction between personal data of different categories of data subjects, such as:

1) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence,

2) persons convicted of a criminal offence,

3) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence, and

4) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in subsection (1) and (2).

9. Personal data shall only be processed when it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

10.-*(1)* Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation may not be processed.

(2) However, if the conditions laid down in this Act are met, data covered by subsection (1) may be processed where strictly necessary and where necessary for the reasons as referred to in section 1(1), including to protect the vital interests of the data subject or of another natural person, or where such processing relates to data which are manifestly made public by the data subject.

11.-*(1)* Decisions producing an adverse legal effect concerning the data subject or significantly affects him or her may be based solely on automated processing, including profiling.

(2) As regards decisions covered by subsection (1), appropriate safeguards must be provided for to ensure the legitimate interests of the data subject, including at least the right for the data subject to obtain human intervention on the part of the controller.

12. The competent authorities must put in place effective mechanisms to encourage confidential reporting of infringements of this Act to the supervisory authorities.

Chapter III

Rights of the data subject

Part 4

Information to be made available or given to the data subject

13.-*(1)* The controller shall make available to the data subject the following information:

1) The identity and the contact details of the controller.

2) The contact details and the function of the data protection officer in relation to the registered.

3) The purposes of the processing for which the personal data are intended.

4) The right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority.

5) The rights of the data subject pursuant to Parts 5 and 6 of the Act.

6) The right to let the competent supervisory authority exercise the rights of the data subject in relation to decisions by the competent authorities regarding failure, delay, restriction or denial pursuant to this Part and Part 5 and 6 of the Act, see section 40(1), para 10.

(2) The controller shall give the following information to the data subject, if necessary to enable the exercise of his or her rights:

1) The legal basis for the processing.

2) The period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period.

3) The categories of any recipients of personal data, including in third countries or international organisations.

4) Where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

14.-*(1)* The information pursuant to section 13(2) may be delayed, restricted or omitted if the data subject's interest in obtaining this information is found to be overridden in order to:

1) avoid obstructing official or legal inquiries, investigations or procedures;

2) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

3) protect public security;

4) protect national security;

5) protect the rights and freedoms of others.

(2) The Minister of Justice lays down specific rules on which categories of processing that fall under the points listed in subsection (1), and that the information to be provided to data subjects pursuant to section 13(2) may be delayed at an appropriate time, in so far as the provisions in subsection (1) allow for such a delay in a general scope.

Part 5

Rights of access by the data subject

15.-*(1)* If a data subject makes a request hereof, the data controller shall confirm as to whether or not personal data concerning him or her are being processed.

(2) If personal data about the data subject are being processed, access must be given to the personal data and a notice must be given containing the following information:

1) The purposes of and legal basis for the processing.

2) The categories of personal data concerned.

3) The recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations.

4) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

5) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

6) The right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority.

7) Communication of the personal data undergoing processing and of any available information as to their origin.

16.-*(1)* The right of access pursuant to section 15 may be delayed, restricted or denied if the data subject's interest in this information is found to be overridden by considerations of public interests referred to in section 14(1).

(2) A decision to delay, restrict or deny the data subject's right to access shall be notified to the data subject in writing and shall be accompanied by the reasons for the decision and an appeals guide. Furthermore, the decision must contain information on the right of the data subject to let the competent supervisory authority exercise the rights of the data subject, pursuant to section 40(1), para 10).

(3) Out of consideration to the purposes referred to in subsection (1), notification on the information referred to in subsection (2) may be omitted. If so, the data subject shall be notified that it can neither be confirmed nor denied whether personal data regarding the data subject are being processed. Such a notification must contain an appeals guide and information on the right of the data subject to let the competent supervisory authority exercise the rights of the data subject, pursuant to section 40(1), para 10).

(4) The Minister of Justice lays down specific rules as to which categories of processing that may fall under subsection (1), including exemptions from the right of access pursuant to section 15, insofar as the interests referred to in subsection (1) may normally be assumed to result in denying of such requests of access.

Part 6

Right to rectification, erasure and restriction of processing

17.-*(1)* Upon request from the data subject and without undue delay, the controller shall rectify data that proves to be inaccurate personal data relating to him or her. Similarly, the completetion of

incomplete personal data shall occur if possible without endangering the purpose of the processing. The controller shall notify the competent authority from where the inaccurate personal data stem of the rectification.

(2) Upon request from the data subject and without undue delay, the controller shall erase personal data that has been processed contrary to Part 3, or if required in order to comply with a legal obligation to which the controller is subject.

(3) Instead of erasure, the controller shall restrict the processing of personal data where:

1) The accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or

2) The personal data must be maintained for the purposes of evidence.

(4) Where processing is restricted pursuant to subsection (3), para 1), the controller shall inform the data subject before lifting the restriction of processing.

(5) A refusal of a request on rectification, erasure or restriction of procession shall be notified to the data subject in writing and shall be accompanied by the reasons for the decision and an appeals guide. Furthermore, the decision must contain information on the right of the data subject to let the competent supervisory authority exercise the rights of the data subject, pursuant to section 40(1), para 10). The provision of section 16(3) shall also apply.

(6) The controller shall notify the recipients about data that has been rectified, erased or processing has been restricted. The recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Part 7

General provisions

18.-*(1)* The data and notifications referred to in this Chapter must be made available or be given free of charge in a concise, intelligible and easily accessible form, using clear and plain language.

(2) The controller shall without undue delay and in writing respond to requests as referred to in this Chapter. If the request is not responded within four weeks from its reception, the controller shall inform the data subject about the reason for the delay and when a response is expected.

(3) The rules laid down in the Administration of Justice Act and the Administration of Military Justice Act regarding the right to information and access, rectification or erasure and limitation of processing of information in criminal cases, applies to the rights pursuant to this chapter.

(4) The Minister of Justice lays down specific rules regarding processing of requests pursuant to this Chapter and the processing of complaints, including that decisions may not be brought before any other administrative authority.

19. The data controller may refuse to comply with manifestly unfounded or excessively repetitive requests which are made pursuant to the provisions in this Part.

Chapter IV

Obligations of the controller and processor

Part 8

Obligations of the controller

20.-*(1)* The controller shall implement and if necessary review and update the appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with this Act. Where proportionate in relation to the processing activities, the controller must also implement the appropriate data protection policies.

(2) The measures referred to in subsection (1) includes data protection by design and by default.

21. Where two or more controllers jointly determine the purposes and means of processing, they shall be considered as joint controllers. Joint controllers shall establish an arrangement for assignment of responsibility for processing complying with this Act, in particular as regards the exercise of the rights of the data subject pursuant to Chapter 3. The arrangement shall include the designation of a single contact point. A special contact point may be designated, functioning as a single contact point for data subjects when exercising their rights.

Part 9

Obligations of the processor etc.

22.-*(1)* If a controller hands over the processing of data to a processor, the controller must ensure that the processor may take the technical and organisational measures as referred to in sections 20 and 24, and ensure compliance.

(2) The processing by a processor must be in accordance with law or a written contract between the processor and the controller. The law or the contract must set out the subject-matter and duration of the processing, the nature and the purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller. In particular, the law or the contract shall stipulate that the processor:

1) Acts only on instructions from the controller,

2) Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,

3) Assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights,

4) At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless the legislation requires storage of the personal data,

5) Makes available to the controller all information necessary to demonstrate compliance with this provision,

6) Complies with the conditions referred to in paragraphs 1)-5) and subsection (3) with a view to engaging another processor.

(3) A processor's handing over of processing to another processor shall happen according to a general or specific written contract with the controller. If the handing over happens according to a general contract, the processor must inform the controller within 14 days prior to when the data was handed over.

(4) Any person acting under the authority of the controller or the processor and which has access to personal data can only process such data pursuant to instructions from the controller, unless required to do so by other legislation.

Part 10

Records of processing activities and logging

23.-*(1)* The controller must maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

1) The name and contact details of the controller and, where applicable, the joint controller and the data protection officer,

2) The purposes of the processing,

3) The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations,

4) A description of the categories of data subject and of the categories of personal data,

5) Where applicable, the use of profiling,

6) Where applicable, the categories of transfers of personal data to a third country or an international organization,

7) The legal basis for the processing operation, including transfers, for which the personal data are intended,

8) Where possible, the envisaged time limits for erasure of the different categories of personal data, and

9) Where possible, a general description of the technical and organisational security measures referred to in section 27.

(2) The processor must maintain a record of all categories of processing activities carried out on behalf of a controller. That record shall contain all of the following information:

1) The name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer,

2) The categories of processing carried out on behalf of each controller,

3) Where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organization, and

4) Where possible, a general description of the technical and organisational security measures referred to in section 27.

24.-*(1)* Logs must be kept for the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure.

(2) The Minister of Justice lays down specific rules as to which automated processing systems introduced before 6 of May 2016 that are covered by subsection (1).

Part 11

Data protection impact assessment and consultation of the supervisory authority

25.-*(1)* Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

26.-*(1)* The controller or the processor shall consult the supervisory authority prior to processing of personal data which will form part of a new filing system to be created, where:

1) A data protection impact assessment as provided for in section 25 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, or

2) The type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of the data subjects.

(2) Where the supervisory authority is of the opinion that the intended processing would infringe the provisions adopted pursuant to this Act, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority may provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller. The supervisory authority may use any of its powers pursuant to Part 20 of the Act. That period may be extended by a month, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

(3) The supervisory authorities establish a list of the processing operations, which are subject to prior consultation pursuant to subsection (1).

Chapter V

Security of personal data

Part 12

Security of processing

27.-*(1)* The controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in section 10.

(2) In respect of automated processing, the controller or processor shall, following an evaluation of the risks, implement measures designed to:

1) Deny unauthorised persons access to processing equipment used for processing (‘equipment access control’),

2) Prevent the unauthorised reading, copying, modification or removal of data media (‘data media control’),

3) Prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (‘storage control’),

4) Prevent the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’),

5) Ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control'),

6) Ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control'),

7) Ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control'),

8) Prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control'),

9) Ensure that installed systems may, in the case of interruption, be restored ('recovery'), and

10) Ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

(3) In consultation with the competent minister, the Minister of Justice may lay down rules to the effect that personal data which are processed in specified IT systems and kept for public administrative authorities, must be stored, in full or in part, exclusively in Denmark.

(4) The Minister of Justice lays down specific rules regarding the measures mentioned in subsections (1) and (2).

Part 13

Personal data breach

28.-*(1)* In the case of a personal data breach, the controller shall notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(3) The notification referred to in subsection (1) shall at least:

1) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

2) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained,

3) describe the likely consequences of the personal data breach,

4) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide the information referred to in subsection (3) to the supervisory authority at the same time, the information may be provided in phases without undue further delay.

(5) The controller shall document any personal data breaches referred to in subsection (1), comprising the facts relating to the personal data breach, its effects and the remedial action taken.

(6) Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in subsection (3) shall be communicated to the controller of that Member State without undue delay.

29.-*(1)* Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain the information referred to in section 28(3), paragraphs 2)-4).

(3) The provision in subsection (1) shall not apply if:

1) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,

2) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialize, or

3) it would involve a disproportionate effort by the controller.

(4) In cases as mentioned in subsection (3), para 3), there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

(5) If the controller has not already communicated the personal data breach to the data subject, the supervisory 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 subsection (3) are met.

(6) The communication to the data subject may be delayed, restricted or omitted on the grounds referred to in section 14(1).

Chapter VI

Data protection officer

Part 14

Designation of the data protection officer

30.-*(1)* The controller designates a data protection officer on the basis of his or her professional qualities, including in particular expert knowledge of data protection law and practice and the ability to fulfil the tasks referred to in Part 15 of the Act, which is involved in all issues relating to the protection of personal data.

(2) A single data protection officer may be designated for several controllers, taking account of their size and organisational structure.

(3) The provision in subsection (1) does not apply to the courts when the courts process personal data in their capacity as courts.

(4) The controller shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Part 15

Position and tasks of the data protection officer

31. The controller shall ensure that the data protection officer is able to:

1) inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation,

2) monitor compliance with this Act and other data protection legislation and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits,

3) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 25, and

4) cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in section 26, and to consult, where appropriate, with regard to any other matter.

Chapter VII

Transfers of personal data to third countries or international organisations

Part 16

General principles

32.-*(1)* Transfer of personal data that are processed or are intended for processing after transfer to a third country or to an international organisation, including for onward transfers to another third country or international organisation, may only take place complying with the provisions pursuant to this Act and if the conditions laid down in this Part are met, namely that:

1) the transfer is necessary for the purposes set out in section 1(1),

2) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in section 1(1),

3) a competent authority in another Member State has given its prior authorisation to the transfer in accordance with its national law and the personal data are transmitted or made available by this authority,

4) the legal basis of transfer is provided for in Part 17 of the Act, and

5) In the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(2) Transfers without the prior authorisation provided for in subsection (1), para 3), can be permitted if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

Part 17

Legal basis for transfers of personal data

33.- A transfer of personal data may take place where the Commission 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.

34.-*(1)* In the absence of a decision pursuant to section 33, a transfer may take place where:

1) appropriate safeguards with regard to the protection of personal data are provided for in an international agreement, or

2) the controller has assessed all the circumstances surrounding the transfer of personal data and concluded that appropriate safeguards exist with regard to the protection of personal data.

(2) The controller shall inform the supervisory authority about categories of transfers under subsection (1), para 2).

(3) A transfer pursuant to subsection (1), para 2), shall be documented as regards the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. The documentation shall be made available to the supervisory authority on request.

35.-*(1)* In the absence of a decision pursuant to section 33 or of appropriate safeguards pursuant to section 34, a transfer or a category of transfers may take place only where the transfer is necessary:

1) to protect the vital interests of the data subject or another person,

2) to safeguard legitimate interests of the data subject, if provided for in law,

3) to prevent an immediate and serious threat to public security of a Member State or a third country;

4) In individual cases for the purposes as mentioned in section 1(1), or

5) In an individual case for the establishment, exercise or defence of legal claims relating to the purposes as mentioned in section 1(1).

(2) Personal data shall not be transferred on the basis of subsection (1), para 4)-5), if the fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.

(3) Where a transfer is based on subsection (1), such a transfer shall be documented regarding the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. The documentation shall be made available to the supervisory authority on request.

36.-*(1)* The competent authorities may transfer personal data directly to other recipients than the competent authorities and international organisations, established in third countries, on the basis of an international agreement or in individual and specific cases, if:

1) The transfer is strictly necessary for the transferring competent authority's performance of a task that follows from the law and pursues the purposes as referred to in section 1(1),

2) The transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand,

3) The transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in section 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time,

4) The authority that is competent for the purposes referred to in section 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate,

5) The transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

(2) The transferring competent authority shall document and inform the supervisory authority about transfers under subsection (1).

Chapter VIII

Supervisory authority

Part 18

Supervisory authority

37.-*(1)* The Data Protection Agency, which consists of a Council and a Secretariat, is responsible for monitoring any processing operation covered by this Act, see however Part 19 of the Act.

(2) The rules laid down in section 27, subsections (2) – (9) of the Danish Data Protection Act shall apply to the Data Protection Agency.

Part 19

Supervision of the courts

38.-*(1)* The Court Administration shall carry out supervision of the processing of data carried out for the courts when they do not act in their capacity of courts.

(2) In respect of other processing of data, the decision must be made by the relevant court. An interlocutory appeal against the decision may be lodged with a higher court. For special courts or tribunals whose decisions cannot be brought before a higher court, an interlocutory appeal against the decision referred to in the first sentence of this subsection may be lodged with the high court in whose district the court is located. The time allowed to lodge an appeal is four weeks from the day when the decision was notified to the individual concerned.

Part 20

Tasks and powers of the supervisory authorities

39. The supervisory authorities act with complete independence in performing their functions.

40.-*(1)* In Denmark, the supervisory authorities shall:

1) Monitor and enforce the application of the provisions pursuant to this Act,

2) Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing,

3) Advise the Danish Parliament (Folketinget), the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing,

4) Promote the awareness of controllers and processors of their obligations pursuant to this Act,

5) Upon request, provide information to any data subject concerning the exercise of their rights pursuant to this Act and, if appropriate, cooperate with the supervisory authorities in other Member States to that end,

6) Deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with section 48, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a period of three months, in particular if further investigation or coordination with another supervisory authority is necessary,

7) Transmit complaints to the competent supervisory authority of another Member State,

8) Upon request, provide further assistance to a data subject that has lodged a complaint which has been transmitted to a supervisory authority in another Member State,

9) Inform a data subject that has lodged a complaint of the possibility of seeking a judicial remedy pursuant to Part 22 of the Act.

10) Upon request, check the lawfulness of processing concerning failure, delay, restriction or denial pursuant to Parts 4-6 of the Act and inform the data subject within a reasonable period of time about the outcome of the check or of the reasons why the check has not been carried out, and of the process and judicial remedy pursuant to Part 22 of the Act,

11) Cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Act,

12) Conduct investigations on the application of this Act, including on the basis of information received from another supervisory authority or other public authority,

13) Monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies,

14) Provide advice on the processing operations referred to in section 26, and

15) Contribute to the activities of the Europe Data Protection Board.

(2) The supervisory authorities shall facilitate the submission of complaints referred to in subsection (1), para 6).

(3) The supervisory authorities may refuse to comply with requests that are manifestly unfounded or excessively repetitive pursuant to this Act.

41.-*(1)* The supervisory authorities may demand being given all information of importance for its activities, including for the decision of whether a particular matter falls within the provisions of this Act.

(2) The members and staff of the supervisory authorities shall at any time against appropriate proof of identity and without any court warrant have access to all premises from where a personal data processing operation is carried out.

42.-*(1)* The supervisory authorities may issue an opinion to the controller and the processor on intended processing operations that are likely to infringe the provisions pursuant to this Act, order the controller or processor to bring processing operations into compliance with the provisions pursuant to this Act, or impose a temporary or definitive limitation, including a ban, on processing of personal data.

(2) The decisions of the supervisory authorities may not be brought before any other administrative authority.

43. The opinion of the Data Protection Council shall be obtained when general regulations of importance for the processing of personal data are being drafted. If the general regulations are of importance for the processing of personal data at the Danish courts, an opinion shall be obtained from the Danish Court Administration.

44. The supervisory authority may bring issues concerned with infringement of this Act before the court to be considered under the rules of the administration of civil justice.

45. The supervisory authorities shall draw up an annual report on their activities for the Danish Parliament (Folketinget) and the Minister of Justice. The report shall be made public.

Part 21

Cooperation

46. The supervisory authorities shall cooperate to the extent required to fulfil their obligations, particularly through the exchange of all relevant information.

47.-*(1)* The supervisory authorities shall reply to requests from a supervisory authority in another Member State without undue delay and no later than one month after receiving the request. The information requested by a supervisory authority in another Member State shall be supplied by electronic means, using a standardised format.

(2) Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

(3) The requested supervisory authority shall not refuse to comply with the request, unless it is not competent for the subject-matter of the request, or for the measures it is requested to execute, or compliance with the request would infringe this Act or other legislation. The requested supervisory authority shall provide reasons for any refusal to comply with a request.

Chapter IX

Remedies, liability and penalties

Part 22

Remedies, liability and penalties

48.-*(1)* The data subject or the data subject's representative may lodge a complaint with the competent supervisory authority about the processing of data concerning the data subject.

(2) Decisions made by the supervisory authorities or their failure to consider a complaint from a data subject or their lack of reporting pursuant to section 40(1), para 6), can be brought before the courts by the data subject or the data subject's representative to be considered under the rules of the administration of civil justice.

(3) The data subject or the data subject's representative may bring issues of whether data controllers or data processors comply with this Act before the courts to be considered under the rules of the administration of civil justice.

49. Any person who has suffered a material or non-material loss as a consequence of an unlawful processing activity or any other processing contrary to the provisions of this Act, have the right to receive compensation for the damage suffered from the controller according to the general Union law on liability.

50.-*(1)* Unless a higher penalty must be imposed under other legislation, a private processor acting under the authority of a competent authority that infringes sections 22(2-3), 23(2), 27 and 28(2) of this Act or fails to comply with an order or ban pursuant to section 42, shall be liable to a fine or imprisonment for a term not exceeding four months.

(2) A controller who fail to comply with an order or ban pursuant to section 42, shall be liable to a fine.

(3) Penalties in the form of a fine or imprisonment for a term not exceeding four months may be prescribed by rules issued in pursuance of this Act.

(4) Companies etc. (legal persons) may incur criminal liability according to the rules of Part 5 of the Criminal Code.

Chapter X

Final provisions

Part 23

Final provisions including commencement provisions etc.

51.-*(1)* The competent minister may in exceptional cases lay down specific rules on the processing of personal data covered by the Act that is carried out on behalf of the Police, the Prosecution Service, including the Danish Military Prosecution Service, the Danish Prison and Probation Service and the Independent Police Complaints Authority.

(2) The Minister of Justice may lay down rules necessary to implement the legal acts issued by the Commission in order to implement the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, or rules that are necessary for the application of the legal acts issued by the Commission in the area of the directive.

52.-*(1)* This Act shall enter into force on the day following that of its proclamation in the Law Gazette.

(2) This Bill may be affirmed immediately after its adoption.

53. Sections 25 and 26 apply to additional processing of data that is initiated, and filing systems that are initiated on 1 May 2017 or later

54. Transfers of personal data to third counties and international organisations may be carried out on the basis of international agreements that are concluded prior to 6 May 2016, until those agreements are amended, replaced or revoked.

55. In Act no. 429 of 31 May 2000 on the Processing of Personal Data, as recently amended pursuant to section 1 of Act no. 639 of 12 June 2013, the following amendments shall be made:

1. *Section 2(4)* is repealed.

Subsections (5) – (11) shall become subsections (4) – (10).

2. After section 2, the following is added to Part 1 of the Act:

»**Section 2 a.** This Act shall not apply to the processing covered by the Danish Act on the processing of personal data by law enforcement authorities, see however subsection (2).

(2) Rules issued in pursuance of sections 32(5), 41(5), 55(4) and 72, shall apply to the processing of personal data covered by the Danish Act on the processing of personal data by law enforcement authorities, unless it would be contrary to this Act.«

56. This Act shall not extend to the Faroe Islands; however, the processing of personal data by realm authorities may be extended by Royal Decree subject to such adaption as may be required by the particular circumstances of the Faroe Islands. This Act shall not extend to Greenland, but may be extended by Royal Decree subject to such adaption as may be required by the particular circumstances of Greenland.

Done at Marselisborg Slot, this 27 April 2017

Under Our Royal Hand and Seal

MARGRETHE R.

/ Søren Pape Poulsen

[1] 1) This Act implements Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union 2016, no. 119, p. 89.