Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)

Chapter I Purpose and scope of the Act

Section 1 Purpose of the Act

The purpose of this Act is to protect natural persons from violation of their right to privacy through the processing of personal data.

The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

Section 2 Definitions

For the purposes of this Act, the following definitions shall apply:

1) personal data: any information and assessments that may be linked to a natural person,
2) processing of personal data: any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses,
3) personal data filing system: filing systems, records, etc. where personal data is systematically stored so that information concerning a natural person may be retrieved.
4) controller: the person who determines the purpose of the processing of personal data and which means are to be used,
5) processor: the person who processes personal data on behalf of the controller,
6) data subject: the person to whom personal data may be linked,
7) consent: any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her,
8) sensitive personal data: information relating to
    a) racial or ethnic origin, or political opinions, philosophical or religious beliefs,
    b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act,
    c) health,
    d) sex life,
    e) trade-union membership.

Section 3 Substantive scope of the Act

This Act shall apply to

a) processing of personal data wholly or partly by electronic means,
b) other processing of personal data which form part of or are intended to form part of a personal data register, and
c) all forms of video surveillance, as defined in section 36, first paragraph.

This Act shall not apply to processing of personal data carried out by a natural person for exclusively personal or other private purposes.

The King may prescribe regulations to the effect that this Act or parts of this Act shall not apply to specified institutions and administrative spheres.

The King may prescribe regulations regarding special forms of processing of personal data, and of processing of personal data in special activities or sectors. As regards the processing of personal data in connection with credit information services, provisions may be laid down in regulations regarding *inter alia* the type of data that may be processed, the sources from which personal data may be obtained, the persons to whom credit information may be disclosed and how such disclosure may be effected, the erasure of negative credit information and the obligation of professional secrecy of the employees of the credit information agency. Rules may also be prescribed to the effect that the Act or individual provisions laid down in or pursuant to the Act shall apply to the processing of credit information relating to persons other than natural persons.

Amended by Act of 9 January 2009 no. 3, Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree April 2012 no. 335).

Section 4 Territorial extent of the Act

This Act shall apply to controllers who are established in Norway. The King may by regulations decide that the Act shall wholly or partly apply to Svalbard and Jan Mayen, and lay down special rules regarding the processing of personal data for these areas.

This Act shall also apply to controllers who are established in states outside the territory of the EEA if the controller makes use of equipment in Norway. However, this shall not apply if such equipment is used only to transfer personal data through Norway.

Controllers such as are mentioned in the second paragraph shall have a representative who is established in Norway. The provisions that apply to the controller shall also apply to the representative.

Section 5 Relationship to other Acts

The provisions of this Act shall apply to the processing of personal data unless otherwise provided by a special statute which regulates the method of processing.

Section 6 Relationship to the statutory right of access to information pursuant to other statutes

This Act shall not limit the right of access to information pursuant to the Freedom of Information Act, the Public Administration Act or any other statutory right of access to personal data.

If another statutory right of access provides broader access to information than this Act, the controller shall on his own initiative provide information concerning the right to request such access.

Amended by Act of 19 May 2006 no.16, (effective 1 January 2009 under Royal Decree 17 October 2008 no. 1118).

Section 7 Relationship to freedom of expression

The processing of personal data exclusively for artistic, literary or journalistic purposes shall only be governed by the provisions of sections 13-15, 36-41, cf. Chapter VIII.

Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Chapter II General rules for the processing of personal data

Section 8 Conditions for the processing of personal data

Personal data (cf. section 2, no. 1) may only be processed if the data subject has consented thereto, or there is statutory authority for such processing, or the processing is necessary in order

a) to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract,
b) to enable the controller to fulfil a legal obligation,
c) to protect the vital interests of the data subject,
d) to perform a task in the public interest,
e) to exercise official authority, or
f) to enable the controller or third parties to whom the data are disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject.

Section 9 Processing of sensitive personal data

Sensitive personal data (cf. section 2, no.8) may only be processed if the processing satisfies one of the conditions set out in section 8 and

a) the data subject consents to the processing,
b) there is statutory authority for such processing,
c) the processing is necessary to protect the vital interests of a person, and the data subject is incapable of giving his or her consent,
d) the processing relates exclusively to data which the data subject has voluntarily and manifestly made public,
e) the processing is necessary for the establishment, exercise or defence of a legal claim,
f) the processing is necessary to enable the controller to fulfil his obligations or exercise his rights in the field of employment law,
g) the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where the data are processed by health professionals subject to the obligation of professional secrecy, or
h) the processing is necessary for historical, statistical or scientific purposes, and the public interest in such processing being carried out clearly exceeds the disadvantages it might entail for the natural person.

Non-profit associations and foundations may process sensitive personal data in the course of their activities even if such processing does not satisfy one of the conditions laid down in the first paragraph, litra a-h. Such processing may apply solely to data relating to members or to persons who, on account of the purposes of the association or foundation, voluntarily have regular contact with it, and solely to data which are collected through such contact. The personal data may not be disclosed without the consent of the data subject.

The Norwegian Data Protection Authority may decide that sensitive personal data may also be processed in other cases if this is warranted by important public interests and steps are taken to protect the interests of the data subject.

Section 10 Register of criminal convictions

A complete register of criminal convictions may only be kept under the control of official authority.

Section 11 Basic requirements for the processing of personal data

The controller shall ensure that personal data which are processed

a) are processed only when this is authorized pursuant to sections 8 and 9,
b) are used only for explicitly stated purposes that are objectively justified by the activities of the controller,
c) are not used subsequently for purposes that are incompatible with the original purpose of the collection, without the consent of the data subject,
d) are adequate, relevant and not excessive in relation to the purpose of the processing, and
e) are accurate and up-to-date, and are not stored longer than is necessary for the purpose of the processing, cf. sections 27 and 28.

Subsequent processing of personal data for historical, statistical or scientific purposes is not deemed to be incompatible with the original purposes of the collection of the data, cf. first paragraph, litra c, if the public interest in the processing being carried out clearly exceeds the disadvantages this may entail for natural persons.

Personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child.

Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 12 Use of national identity numbers, etc.

National identity numbers and other clear means of identification may only be used in the processing when there is a objective need for certain identification and the method is necessary to achieve such identification.

The Data Protection Authority may require a controller to use such means of identification as are mentioned in the first paragraph to ensure that the personal data are of adequate quality.

The King may by regulations prescribe further rules regarding the use of national identity numbers and other clear means of identification.

Section 13 Data security

The controller and the processor shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

To achieve satisfactory data security, the controller and processor shall document the data system and the security measures. Such documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to The Data Protection Authority and the Privacy Appeals Board.

Any controller who allows other persons to have access to personal data, e.g. a processor or other persons performing tasks in connection with the data system, shall ensure that the said persons fulfil the requirements set out in the first and second paragraphs.

The King may prescribe regulations regarding data security in connection with the processing of personal data, including further rules regarding organisational and technical security measures.

Section 14 Internal control

The controller shall establish and maintain such planned and systematic measures as are necessary to fulfil the requirements laid down in or pursuant to this Act, including measures to ensure the quality of personal data.

The controller shall document the measures. The documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to The Data Protection Authority and the Privacy Appeals Board.

The King may prescribe regulations containing further rules regarding internal control.

Section 15 The processor's right of disposition over personal data

No processor may process personal data in any way other than that which is agreed in writing with the controller. Nor may the data be turned over to another person for storage or manipulation without such agreement.

It shall also be stated in the agreement with the controller that the processor undertakes to carry out such security measures as ensue from section 13.

Section 16 Time limit for replying to inquiries regarding data, etc.

The controller shall reply to inquiries regarding access or other rights pursuant to sections 18, 22, 25, 26, 27 and 28 without undue delay and not later than 30 days from the date of receipt of the inquiry.

If special circumstances should make it impossible to reply to the inquiry within 30 days, implementation may be postponed until it is possible to reply. In such case, the controller shall give a provisional reply stating the reason for the delay and when a reply is likely to be given.

Section 17 Payment

The controller may not request compensation for providing data pursuant to Chapter III or for meeting demands of the data subject pursuant to Chapter IV.

Chapter III Information on processing of personal data

Section 18 Right of access

Any person who so requests shall be informed of the kind of processing of personal data a controller is performing, and may demand to receive the following information as regards a specific type of processing:

a) the name and address of the controller and of his representative, if any,
b) who has the day-to-day responsibility for fulfilling the obligations of the controller,
c) the purpose of the processing,
d) descriptions of the categories of personal data that are processed,
e) the sources of the data, and
f) whether the personal data will be disclosed, and if so, the identity of the recipient.

If the person requesting access is a data subject, the controller shall inform him of

a) the categories of data concerning the data subject that are being processed, and
b) the security measures implemented in connection with the processing insofar as such access does not prejudice security.

The data subject may demand that the controller elaborate on the information in the first paragraph, litra a-f to the extent that this is necessary to enable the data subject to protect his or her own interests.

The right to information pursuant to the second and third paragraphs shall not apply if the personal data are being processed exclusively for historical, statistical or scientific purposes and the processing will have no direct significance for the data subject.

Section 19 Obligation to provide information when data is collected from the data subject

When personal data is collected from the data subject himself, the controller shall on his own initiative first inform the data subject of

a) the name and address of the controller and of his representative, if any
b) the purpose of the processing,
c) whether the data will be disclosed and if so, the identity of the recipient,
d) the fact that the provision of data is voluntary, and
e) any other circumstances that will enable the data subject to exercise his rights pursuant to this Act in the best possible way, such as information on the right to demand access to data, cf. section 18, and the right to demand that data be rectified, cf. sections 27 and 28.

Notification is not required if there is no doubt that the data subject already has the information in the first paragraph.

Section 20 Obligation to provide information when data is collected from persons other than the data subject

A controller who collects personal data from persons other than the data subject shall on his own initiative inform the data subject of which data are being collected and provide such information as is mentioned in section 19, first paragraph, as soon as the data have been obtained. If the purpose of collecting the data is to communicate them to other persons, the controller may wait to notify the data subject until such disclosure takes place.

The data subject is not entitled to notification pursuant to the first paragraph if

a) the collection or communication of data is expressly authorized by statute,
b) notification is impossible or disproportionately difficult, or
c) there is no doubt that the data subject already has the information which shall be contained in the notification.

When notification is omitted pursuant to litra b, the information shall nonetheless be provided at the latest when the data subject is contacted on the basis of the data.

Section 21 Obligation to provide information in connection with the use of personal profiles

When a person contacts the data subject or makes decisions to which the data subject is subject on the basis of personal profiles that are intended to describe

behaviour, preferences, abilities or needs, for instance in connection with marketing activities, the controller shall inform the data subject of

a) the identity of the controller,
b) the categories of data which are being used, and
c) the sources of the data.

Section 22 Right to information regarding automated decisions

If a decision has legal or another significant effects for the data subject and is based solely on automated processing of personal data, the data subject who is subject to the decision may demand that the controller give an account of the rules incorporated in the computer software which form the basis for the decision.

Section 23 Exceptions to the right to information

The right to access pursuant to sections 18 and 22 and the obligation to provide information pursuant to sections 19, 20 and 21 do not encompass data

a) which, if known, might endanger national security, national defence or the relationship to foreign powers or international organizations,
b) regarding which secrecy is required in the interests of the prevention, investigation, exposure and prosecution of criminal acts,
c) which it must be regarded as inadvisable for the data subject to gain knowledge of, out of consideration for the health of the person concerned or for the relationship to persons close to the person concerned,
d) to which a statutory obligation of professional secrecy applies,
e) which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons,
f) regarding which it will be contrary to obvious and fundamental private or public interests to provide information, including the interests of the data subject himself.

Data pursuant to the first paragraph, litra c, may nonetheless on request be made known to a representative of the data subject when there are no special reasons for not doing so.

Any person who refuses to provide access to data pursuant to the first paragraph must give the reason for this in writing with a precise reference to the provision governing exceptions.

The King may prescribe regulations regarding other exceptions from the right of access and the obligation to provide information and regarding conditions for the use of right of access.

Section 24 How the information shall be provided

The information may requested in writing from the controller or from his processor as mentioned in section 15. Before providing access to data relating to a data subject, the controller may require that the data subject furnish a written, signed request.

Chapter IV Other rights of the data subject

Section 25 Right to demand manual processing

Any person who is subject to a fully automated decision such as is mentioned in section 22 or to whom the case otherwise directly relates may demand that the decision be reviewed by a physical person.

The right pursuant to the first paragraph shall not apply if the data subject's interests in terms of protection of privacy are adequately safeguarded and the decision is authorized by statute or is related to the performance of a contract.

Section 26 Repealed by Act of 9 January 2009 no. 2 (effective 1 June 2009 under Royal Decree 9 Jan 2009 no. 7).

Section 27 Rectification of deficient personal data

If personal data which are inaccurate or incomplete or of which processing is not authorized, the controller shall on his own initiative or at the request of the data subject rectify the deficient data. The controller shall if possible ensure that the error does not have an effect on the data subject, for instance by notifying recipients of disclosed data.

The rectification of inaccurate or incomplete personal data which may be of significance as documentation shall be effected by marking the data clearly and supplementing them with accurate data.

If weighty considerations relating to protection of privacy so warrant, the Data Protection Authority may, notwithstanding the second paragraph, decide that rectification shall be effected by erasing or blocking the deficient personal data. If the data may not be destroyed pursuant to the Archives Act, the Director General of the National Archives of Norway shall be consulted prior to making an administrative decision regarding erasure. This decision shall take precedence over the provisions of sections 9 and 18 of the Archives Act of 4 December 1992 No. 126.

Erasure should be supplemented by the recording of accurate and complete data. If this is impossible, and the document which contained the erased data therefore provides a clearly misleading picture, the entire document shall be erased.

The King may prescribe regulations containing supplementary provisions as regards how to effect rectification.

Section 28 Prohibition against storing unnecessary personal data

The controller shall not store personal data longer than is necessary to carry out the purpose of the processing. If the personal data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased.

The controller may, notwithstanding the first paragraph, store personal data for historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the person concerned. In this case, the controller shall ensure that the data are not stored in ways which make it possible to identify the data subject longer than necessary.

The data subject may demand that data which are strongly disadvantageous to him or her shall be blocked or erased if this

a) is not contrary to another statute, and
b) is justifiable on the basis of an overall assessment of, *inter alia* the needs of other persons for documentation, the interests of the data subject, cultural historical interests and the resources required to carry out the demand.

After the Director General of the National Archives of Norway has been consulted, the Data Protection Authority may decide that the right to erase data pursuant to the third paragraph shall take precedence over the provisions of sections 9 and 18 of the Archives Act of 4 December 1992 No. 126.

If the document which contained the erased data gives a clearly misleading picture after the erasure, the entire document shall be erased.

Chapter V Transfer of personal data to other countries

Section 29 Basic conditions

Personal data may only be transferred to countries which ensure an adequate level of protection of the data. Countries which have implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data meet the requirement as regards an adequate level of protection.

In assessing the adequacy of the level of protection, emphasis shall be placed, *inter alia* on the nature of the data, the purpose and duration of the proposed processing and the rules of law and the professional rules and security measures which apply in the country in question. Importance shall also be attached to whether the country has acceded to the Council of Europe's Convention No. 108 of 28 January 1981 on the protection of individuals with regard to the automatic processing of personal data.

Section 30 Exceptions

Personal data may also be transferred to countries which do not ensure an adequate level of protection if

a) the data subject has consented to the transfer,
b) there is an obligation to transfer the data pursuant to an international agreement or as a result of membership of an international organization,
c) the transfer is necessary for the performance of a contract with the data subject, or for the performance of tasks at the request of the data subject prior to entering into such a contract,
d) the transfer is necessary for the conclusion or performance of a contract with a third party in the interest of the data subject,
e) the transfer is necessary in order to protect the vital interests of the data subject,
f) the transfer is necessary in order to establish, exercise or defend a legal claim,
g) the transfer is necessary or legally required in order to protect an important public interest, or
h) there is statutory authority for demanding data from a public register.

The Data Protection Authority may allow transfer even if the conditions of the first paragraph are not fulfilled if the controller provides adequate safeguards with respect to
the protection of the rights of the data subject. The Data Protection Authority may stipulate conditions for the transfer.

The King may prescribe regulations regarding the transfer of personal data to another country, including regarding stopping or limiting transfers to specified countries which do not satisfy the requirements set out in section 29.

Chapter VI Obligation to give notification and to obtain a licence

Section 31 Obligation to give notification

The controller shall notify the Data Protection Authority before

a) processing personal data by automatic means

b) establishing a manual personal data filing system which contains sensitive personal data.

Notification shall be given not later than 30 days prior to commencement of processing. The Data Protection Authority shall give the controller a receipt of notification.

New notification must be given prior to processing that exceeds the limits for processing provided for in section 32. Even if no changes have taken place, new notification shall be given three years after the previous notification was given.

The King may prescribe regulations to the effect that certain methods of processing or controllers are exempted from the obligation to give notification, subject to a simplified obligation to give notification or subject to an obligation to obtain a licence. For processing that is exempt from the obligation to give notification, regulations may be prescribed to limit the disadvantages that processing otherwise may entail for the data subject.

Section 32 Content of the notification

The notification shall provide information regarding

a) the name and address of the controller and his representative and processor, if any,
b) when the processing will begin,
c) who has the day-to-day responsibility for fulfilling the obligations of the controller,
d) the purpose of the processing,
e) an overview of the categories of personal data that are to be processed,
f) the sources of the personal data,
g) the legal basis for collecting the data,
h) the persons to whom the personal data will be disclosed, including recipients in other countries, if any, and
i) the security measures relating to the processing.

The King may prescribe regulations regarding the data which notifications shall contain and the implementation of the obligation to give notification.

Section 33 Obligation to obtain a licence

A licence from the Data Protection Authority is required for the processing of sensitive personal data. This does not apply, however, to the processing of sensitive personal data which have been volunteered by the data subject.

The Data Protection Authority may decide that the processing of data other than sensitive personal data shall also be subject to licensing, if such processing otherwise will clearly violate weighty interests relating to protection of privacy. In assessing whether a licence is necessary, The Data Protection Authority shall, *inter alia* take account of the nature and quantity of the personal data and the purpose of the processing.

If The Data Protection Authority determines that a processing licence will clearly be unnecessary, it may decide that the processing does not require a licence.

The controller may demand that The Data Protection Authority decide whether processing will be subject to licensing.

The obligation to obtain a licence pursuant to the first and second paragraphs shall not apply to the processing of personal data in central government or municipal bodies when such processing is authorized by special statute.

The King may prescribe regulations to the effect that certain processing methods are not subject to licensing pursuant to the first paragraph. As regards processing methods which are exempt from licensing, regulations may be prescribed to limit the disadvantages which processing may otherwise entail for the data subject.

Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 34 Decision as to whether to grant a licence

When deciding whether to grant a licence, it shall be clarified whether the processing of personal data may cause disadvantages for an individual which are not remedied by the provisions of Chapters II-V and conditions pursuant to section 35. In such case, an assessment must be made as to whether the disadvantages are offset by considerations that favour the processing.

Section 35 Conditions laid down in the licence

In the licence, an assessment shall be made as to whether to lay down conditions for processing when such conditions are necessary to limit the disadvantages the processing would otherwise entail for the data subject.

Chapter VII Video surveillance

Heading amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 36 Definition

The term “video surveillance” shall mean or regularly repeated surveillance of persons by means of a remote-controlled or automatically operated video camera, camera or similar device, which is permanently fixed. Video surveillance is considered to be surveillance undertaken both with and without the possibility of recording audio and image material. The same applies to equipment that is easily mistaken for a genuine camera solution.

Video surveillance may only be undertaken when the conditions for so doing under Section 37 (Basic requirements for video surveillance) and Sections 38 to 40 (Additional requirements for surveillance) have been met.
Amended by Act of 9 January 2009 no. 3, Act of 20 April 2012 no. 18.

Section 37 Basic requirements for video surveillance

The Personal Data Act applies in its entirety to all forms of video surveillance, cf. section 3, first paragraph, (c), complete with all the specifications stated in the second to fourth paragraphs.

Video surveillance that must be assumed to be of significant importance to the prevention and solving of crime is permitted even if the conditions in section 9, first

paragraph (a) are not fulfilled. In cases of that nature, also the obligation to obtain a licence under Section 33 does not apply.

When considering what is of rightful interest under section 8(f) of the Personal Data Act in respect of video surveillance, particular emphasis shall be placed on the question of whether the surveillance contributes to safeguarding life or health or prevents repeated or serious criminal acts.

Video surveillance shall only be considered as processing of sensitive personal data where such data constitute a significant part of the information that is comprised by the surveillance.
Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 38 Additional requirements for surveillance of places normally frequented by a limited group of persons

Video surveillance of places frequented by a limited group of persons is only permitted if, due to the activity, there is a need to prevent hazardous situations from arising and to protect the safety of employees or others, or if the surveillance is deemed essential for other reasons.
Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 38a Additional requirements for surveillance of parks, beaches and similar recreational areas that are open to the general public

Video surveillance of parks, beaches and similar recreational areas that are open to the general public is only permitted when the need clearly exceeds the interests of individual persons not to be monitored.

When considering the need for surveillance, particular emphasis shall be placed on whether the surveillance is of significant importance for the prevention of criminal acts that may threaten life or health, or to prevent accidents or attend to similar interests of benefit to society.

When considering the interest of individual persons not to be under surveillance, particular emphasis shall be placed on how the surveillance is to be carried out and what kind of area should be monitored.
Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 39 Additional requirements for disclosure of image recordings made in connection with video surveillance

Personal data which are collected by means of image recordings made in connection with video surveillance may only be disclosed to a person other than the controller if the subject of the recording consents thereto or if there is statutory provision for such disclosure. However, unless the statutory obligation of professional secrecy prevents disclosure, image recordings may be disclosed to the police in connection with investigation of criminal acts or accidents.

Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 40 Additional requirements regarding notification that surveillance is being carried out

When a public place or a place which is regularly frequented by a limited group of persons is subject to video surveillance, attention shall be drawn clearly by means of a sign or in some other way to the fact that the place is under surveillance, that the surveillance may include sound recordings and to the identity of the controller.
Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Section 41 Regulations

The King may prescribe regulations containing further provisions regarding video surveillance and recordings in connection with such surveillance, and regarding the protection, use and erasure of image recordings made in connection with video surveillance and of the right of the surveillance subject to have access to the portions of the image recordings in which he or she appears. Regulations may also be prescribed to the effect that image recordings may be disclosed in circumstances other than those mentioned in section 39.
Amended by Act of 20 April 2012 no. 18. (effective 20 April 2012 under Royal Decree 20 April 2012 no. 335).

Chapter VIII Supervision and sanctions

Section 42 The organization and functions of The Data Protection Authority

The Data Protection Authority is an independent administrative body subordinate to the the King and the Ministry. The King and the Ministry may not issue instructions regarding or reverse The Data Protection Authority's exercise of authority in individual cases pursuant to statute.

The Data Protection Authority is headed by a director who is appointed by the King. The King may decide that the director shall be appointed for a fixed period of time.

The Data Protection Authority shall

1) keep a systematic, public record of all processing that is reported pursuant to section 31 or for which a licence has been granted pursuant to section 33, with information such as is mentioned in section 18, first paragraph, cf. section 23,
2) deal with applications for licences, receive notifications and assess whether orders shall be made in cases where this is authorized by law,
3) verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified,
4) keep itself informed of and provide information on general national and international developments in the processing of personal data and on the problems related to such processing,
5) identify risks to protection of privacy, and provide advice on ways of avoiding or limiting such risks,
6) provide advice and guidance in matters relating to protection of privacy and the protection of personal data to persons who are planning to process personal data

or develop systems for such processing, including assistance in drawing up codes of conduct for various sectors,

7) on request or on its own initiative give its opinion on matters relating to the processing of personal data, and

8) submit an annual report on its activities to the King.

Decisions made by The Data Protection Authority pursuant to sections 9, 12, 27, 28, 30, 33, 34, 35, 44, 46 and 47 may be appealed to the Privacy Appeals Board. Decisions made pursuant to sections 27 or 28 may be further appealed to the King if the decision concerns personal data which are processed for historical purposes.

Section 43 Organization and functions of the Privacy Appeals Board

The Privacy Appeals Board shall decide appeals against the decisions of The Data Protection Authority, cf. section 42, fourth paragraph. The Board is an independent administrative body subordinate to the King and the Ministry. Section 42, first paragraph, second sentence, shall apply correspondingly.

The Privacy Appeals Board consists of seven members who are appointed for a term of four years with the possibility of reappointment for a further four years. The chairman and deputy chairman are appointed by the Storting. The other five members are appointed by the King.

The Privacy Appeals Board may decide that the chairman or the deputy chairman together with two other board members may deal with appeals against decisions that must be decided without delay.

The Privacy Appeals Board shall give the King an annual report on its hearing of appeals.

Legal action regarding the validity of the decisions made by the Privacy Appeals Board shall be addressed to the State as represented by the Privacy Appeals Board.

The King may prescribe further rules regarding the organization and administrative procedures of the Privacy Appeals Board.

Section 44 Access of the supervisory authorities to data

The Data Protection Authority and the Privacy Appeals Board may demand any data necessary to enable them to carry out their functions.

In connection with its verification of compliance with statutory provisions, The Data Protection Authority may demand admittance to places where personal data filing systems, surveillance equipment and image recordings such as are mentioned in section 37, personal data that are processed automatically and technical aids for such processing are located. The Data Protection Authority may carry out such tests or inspections as it deems necessary and may demand such assistance from the personnel in such places as is necessary to carry out the tests or inspections.

The right to demand information or admittance to premises and aids pursuant to the first and second paragraphs shall apply notwithstanding any obligation of professional secrecy.

The King may prescribe regulations regarding exemptions from the first to third paragraphs in the interests of the security of the realm. The King may also issue regulations concerning the reimbursement of expenses incurred in connection with inspections.

Amended by Act of 9 January 2009 no. 3.

Section 45 Obligation of professional secrecy for the supervisory authorities

Employees of The Data Protection Authority, members of the Privacy Appeals Board and other persons who are in the service of the supervisory authorities shall be subject to the provisions regarding the obligation of professional secrecy laid down in sections 13 ff. of the Public Administration Act. The obligation of professional secrecy shall also apply to information concerning security measures, cf. section 13.

The Data Protection Authority and the Privacy Appeals Board may, notwithstanding their obligation of professional secrecy pursuant to the first paragraph, give information to the supervisory authorities of other countries when this is necessary in order to be able to make administrative decisions in connection with supervisory activities.

§ 46. Fines. Order to change or cease unlawful processing

The Data Protection Authority may issue orders to the effect that violation of provisions laid down in or pursuant to this Act shall result in a fine to the Treasury (Data Offence Fine) of maximum 10 times the National Insurance Basic Amount. Physical persons may only be fined for a data offence for deliberate or negligent violation. A business may not be fined for a data offence for a violation that is due to factors outside the control of the business.

In evaluating whether to impose a data offence fine and in determining its size, special consideration will be given to:

a) how seriously the violation has infringed the interests the Act is designed to protect;

b) the degree of culpability;

c) whether the violator could, by guidelines, instructions, training, inspection or other measures, have mitigated the violation;

d) whether the violation was committed to promote the violator's interests;

e) whether the violator has, or could have, achieved any benefit from the violation;

f) whether this is a repeat violation;

g) whether other sanctions following from the violation are imposed on the violator, or a person acting on his behalf, for instance punishment of a person for a criminal offence, and;

h) the violator's financial capacity.

The fulfilment date shall be four weeks from the final stipulation of the data offence fine order. If a data offence fine order is tested in court, all aspects of the case may be tried.

The Data Protection Authority may order that processing of personal data in violation of the provisions in, or in pursuance of, this Act shall cease, or impose conditions which must be met in order that the processing comes into compliance with the Act.

Amended by Act of 9 January 2009 no. 3 (penalty fines may only be imposed for offences committed after Amendment Act entered into force).

Section 47 Coercive fine

In connection with orders pursuant to sections 12, 27, 28 and 46, The Data Protection Authority may impose a coercive fine which will run for each day from the

expiry of the time limit set for compliance with the order until the order has been complied with.

The coercive fine shall not run until the time limit for lodging an appeal has expired. If the administrative decision is appealed, the coercive fine shall not run until so decided by the Privacy Appeals Board.

The Data Protection Authority may waive a coercive fine that has been incurred.

Section 47a. Recovery claims for expenses, data offence fines and coercive fines

Claims for reimbursement of inspection expenses as mentioned in section 44, data offence fines as mentioned in section 46, and coercive fines as mentioned in section 47, shall constitute enforcement grounds for the use of distraint.

When the National Collection Agency is ordered to recover claims as mentioned in the first paragraph, the claims may be recovered by attachment of wages or comparable benefits, under the rules of the Satisfaction of Claims Act, section 2-7. The National Collection Agency may also recover fines and fees by levying a distraint on the claim, provided the distraint will attract legal protection if registered in a mortgage register, or by notification to a third party, see Mortgage Act, Chapter 5, and the distraint proceedings may be held in the National Collection Agency's offices under the Enforcement Act, section 7-9, first paragraph.

Added by Act of 9 January 2009 no. 3.

Section 48 Penalties

Anyone who wilfully or through gross negligence

a) omits to send notification pursuant to section 31,
b) processes personal data without the necessary licence pursuant to section 33,
c) violates the conditions laid down pursuant to sections 35 or 46,
d) omits to comply with orders of The Data Protection Authority pursuant to sections 12, 27, 28 or 46,
e) processes personal data contrary to sections 13, 15, 26 or 39, or
f) omits to provide information pursuant to sections 19, 20, 21, 40 or 44,

shall be liable to fines or imprisonment for a term not exceeding one year or both.

In particularly aggravating circumstances, a sentence of imprisonment for a term not exceeding three years may be imposed. In deciding whether there are particularly aggravating circumstances, emphasis shall be placed, *inter alia* on the risk of great damage or inconvenience to the data subject, the gain sought by means of the violation, the duration and scope of the violation, manifest fault, and on whether the controller has previously been convicted of violating similar provisions.

An accomplice shall be liable to similar penalties.

In regulations issued pursuant to this Act, it may be prescribed that any person who wilfully or through gross negligence violates such regulations shall be liable to fines or imprisonment for a term not exceeding one year or both.

Section 49 Compensation

The controller shall compensate damage suffered as a result of the fact that personal data have been processed contrary to provisions laid down in or pursuant to this Act, unless it is established that the damage is not due to error or neglect on the part of the controller.

Controllers who provide credit information and who have communicated information which proves to be inaccurate or obviously misleading shall compensate any damage that has been suffered as a result of the erroneous communication, regardless of whether the damage is due to error or neglect on the part of the controller.

The compensation shall be equivalent to the financial loss incurred by the injured party as a result of the unlawful processing. The controller may also be ordered to pay such compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable.

Chapter IX Commencement. Transitional provisions. Amendments to other statutes.

Section 50 Commencement

This Act shall enter into force from the date decided by the King. The King may decide that the individual provisions of the Act shall enter into force on different dates.

Section 51 Transitional provisions

1. In respect of processing of personal data which commenced prior to the entry into force of this Act and which is subject to notification and licensing pursuant to the provisions of Chapter VI, notification shall be sent pursuant to section 31 or an application shall be made to The Data Protection Authority for a licence pursuant to section 33 not later than one year after the entry into force of this Act. If the processing is being carried out in accordance with a licence pursuant to section 9 of the Personal Data Filing System Act, the time limit for sending notification or applying for a licence shall be two years from the date of entry into force. Until notification has been sent or The Data Protection Authority has granted a licence, the personal data may be processed in accordance with the provisions of the Personal Data Filing System Act.
2. A consent given by a data subject prior to the entry into force of this Act shall still apply, if it satisfies the conditions set out in section 2, no. 7.
3. Appeals received by The Data Protection Authority after the entry into force of this Act shall be dealt with by the Privacy Appeals Board.
4. The King may by regulations prescribe further transitional provisions.

Section 52 Amendments to other statutes

The following amendments shall be made to other statutes:…