https://lovdata.no/dokument/NLE/lov/2010-05-28-16

Act relating to the processing of data by the police and the prosecuting authority (the Police Databases Act)

Date	LOV-2010-05-28-16
Ministry	Ministry of Justice and Public Security
Entry into force	01.07.2014, 13.09.2013, 27.09.2013, 01.01.2016, 06.05.2018
Last consolidated	LOV-2020-04-24-33 from 01.02.2021
Not yet incorporated	LOV-2021-06-11-72, LOV-2021-06-18-97
Last update	23.03.2021
Abbreviated title	The Police Databases Act
Original title	Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

Kapitteloversikt:

Amendment acts incorporated in this text: This translation included originally amendment Act 29 March 2019 No. 9 and all earlier amendment Acts.
Amendment Acts incorporated in this text: Act 21 June 2019 No. 50 (in force 1 July 2019), Act 4 December 2020 No. 135, Act 24 April 2020 No. 33 (in force 1 February 2021.)

Amendment acts *not yet incorporated* in this text:
Act 11 June 2021 No. 72 (amending section 3 (not yet in force) and sections 12, 13, 36, 40, 60, 66 and 69 (in force 11 June 2021).
Act 18 June 2021 No. 97 (amending section 40, not yet in force).

Chapter 1. Purpose, definitions and scope of the Act

Section 1.*Purpose of the Act*

The purpose of the Act is to promote the effective performance of the functions of the police and the prosecuting authority, the protection of privacy and predictability for individuals in connection with the processing of data.

Section 2.*Definitions*

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

1. personal data: any information or assessment relating to a natural person who can be identified directly or indirectly,

2. processing of data: any electronic or manual use of data, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction or a combination of such uses,
3. database: a collection of data that have been stored systematically in such a way as to enable the retrieval of data relating to an individual,
4. controller: whoever, pursuant to statute or regulations, alone or jointly with others determines the purposes and means of the processing of data,
5. processor: whoever processes data on behalf of the controller,
6. data subject: a natural or legal person to whom data in a database or in a processing operation can be linked,
7. consent: any freely given, specific and informed declaration by the data subject to the effect that he agrees to the processing of data relating to him,
8. unverified data: data that have not been confirmed,
9. referencing: the marking of stored data without the aim of limiting their processing in the future,
10. restriction of processing: the marking of stored data with the aim of limiting their processing in the future,
11. criminal case: a case that is dealt with pursuant to the Criminal Procedure Act,
12. criminal records check: use of data to assess whether a natural or legal person is suitable for a particular position, occupation, activity or other function,
13. police purposes:
    (a) the police's activities against crime, including investigation, preventive efforts and the activities of the uniformed service, and
    (b) the police's service and assistance functions and keeping of police logs.
14. personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed,
15. genetic data: 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,
16. biometric data: 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,
17. international organisation: 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.

Section 3.*The scope of the Act*

This Act applies to the processing of data by the police and the prosecuting authority, except for the processing of data which

1. is regulated by the Act of 16 July 1999 No. 66 relating to the Schengen Information System (SIS),
2. forms part of the police's public administration activities or civil duties.

The public administration activities of the Police Security Service nevertheless fall within the scope of the Act.

The Act applies to the electronic processing of data, and to the manual processing of data when the latter form part of a database or are intended to form part of a database.

For data regarding objects, chapter 4 and the provisions on the duty of confidentiality apply insofar as the data fall within the scope of section 23.

This Act also applies to Svalbard, Jan Mayen and the Norwegian dependencies, with such amendments as are prescribed by the King to take account of local conditions.

Chapter 2. Requirements relating to the processing of data

Section 4.*Specificity of purpose*

Data may be processed for the purpose for which they are collected or for other police purposes, unless it is provided by statute or in pursuance of statute that the right to process data is limited, or that the data may be processed for purposes other than police purposes.

Section 5.*The requirement of necessity*

Data may only be processed when this is necessary for such purposes as are mentioned in section 4. Moreover, the following limitations apply:

1. In an individual criminal case, data may be processed in accordance with the provisions of the Criminal Procedure Act.
2. The processing of personal data shall be permitted for the purpose of combating crime beyond the scope of the individual criminal case if the person in question
    (a) is associated with a group whose activities largely consist of committing criminal offences, or who may be assumed, on the basis of other objective grounds, to commit such offences. This applies even if the person is below the age of criminal responsibility or the personal conditions for criminal liability are otherwise not satisfied,
    (b) has a special connection with such persons as are mentioned in (a),
    (c) has been, or is likely to be, the victim of a criminal offence, or

(d) is an informant.
(d) also applies in criminal cases.

3. For such police purposes as are mentioned in section 2, sub-section 13(b), processing of data, including data relating to persons who present a special security risk, may extend beyond the purpose of the activity in order to ensure the safety of an individual.

Section 6.*Requirements regarding the quality of data*

Data that are processed shall

1. be adequate and relevant to the purpose of the processing,
2. be accurate and up-to-date, and
3. not be stored any longer than necessary for the purpose of the processing.

Unverified data may be processed if necessary for the purpose of the processing.

When data are processed it shall, as far as possible, and if relevant, be indicated to which category of persons the data subject belongs, for instance whether the subject is convicted, a suspect, an aggrieved party or a witness, has reported a crime or has a connection with such persons. Correspondingly, it shall, as far as possible, be indicated whether data are based on facts or assessments. In addition, data processed under section 5 sub-section 2 shall be marked to indicate the reliability of the source and the validity of the data.

In the context of a police investigation, the keeping of a police log and similar operations, the requirement in the first paragraph, sub-paragraph 2, regarding the accuracy of data, means that the data shall be reported as they were provided by the source. The requirement in the first paragraph, sub-paragraph 2, that the data shall be up-to-date, means, for the investigation, that the data shall as far as possible be updated before being used as evidence.

Section 7.*Processing of special categories of personal data*

The processing of personal data which reveal racial or ethnic origin, political, religious or philosophical beliefs, or trade union membership, and the processing of genetic and biometric data to uniquely identify a natural person, or data concerning health, sex life or sexual orientation shall only take place if strictly necessary for the purpose of the processing. Such data may also be processed if strictly necessary to protect the vital interests of the data subject or another person.

Section 8.*Time-limited exemption from the requirements of specificity of purpose, necessity and relevance*

Data may in any case be processed for 4 months if necessary in order to ascertain whether the requirements in section 4, section 5, sub-sections 1 and 2, and section 6, first paragraph, sub-paragraph 1, are satisfied.

The data shall be checked as soon as possible, to ensure that they are either erased or processed on a legal basis other than section 8. As part of such checking, the data may be made known to other employees of the police or the prosecuting authority. The data may also be disclosed to others if this is strictly necessary for the purpose of checking.

The time limit shall not apply to the processing of data in individual criminal cases.

Chapter 3. Databases and other systems of the police

Section 9.*Sanctions database*

The police shall keep a sanctions database containing data relating to natural or legal persons who have been the subject of a penalty or other criminal sanctions or other measures as a result of a criminal offence. Identity details, sanctions and measures shall be registered. The duty of confidentiality in section 23 does not preclude the use of the data in the database in criminal statistics. The King makes regulations containing more details on the registration of foreign sanctions and measures.

Section 10.*Police log*

The police shall keep databases that provide a continuous, 24-hour overview of all significant data relating to the organisation and performance of police services at the site in question. The database may be used for police, public administration and police administration purposes.

Section 11.*Criminal intelligence databases*

The police may keep criminal intelligence databases, provided that the conditions of section 5, sub-section 2, and the other conditions of the Act are satisfied.

Section 12.*DNA database*

The police shall keep a DNA database consisting of a convicted offenders database, a known suspects database and a crime-scene samples database.

Are eligible for registration in the convicted offenders database persons who

1. have been sentenced to a penalty under section 29 of the Penal Code for an act which by law carries a custodial sentence. Registration may not take place until the decision is legally enforceable or the case has been finally decided. An act for which an on-the-spot fine has been issued does not constitute grounds for registration,
2. on account of the provisions of section 20 of the Penal Code may not be sentenced to a penalty for an act that qualifies for registration. The same applies when the person is held inculpable due to his state,
3. are Norwegian nationals or who work or are staying in Norway, and who have been sentenced abroad to a penalty equivalent to those mentioned in section 29 of the Penal Code, and the offence committed would carry a custodial sentence if committed in Norway, or
4. so request for reasons that are deemed to be satisfactory.

All DNA profiles produced from biological material obtained pursuant to section 158, first paragraph, of the Criminal Procedure Act shall be registered in the known suspects database. As soon as the police have made a decision regarding registration in the convicted offenders database, the DNA profile of the person concerned shall be transferred from the known suspects database to the convicted offenders database.

Data relating to persons of unknown identity may be registered in the crime-scene samples database when the data are assumed to be connected with an unsolved criminal case.

The police may keep an elimination database. Data collected pursuant to section 158, second paragraph, of the Criminal Procedure Act relating to employees of the police, analysis institutions and other persons of known identity who regularly come into contact with crime scenes and evidence may be recorded in the elimination database.

The data in the database shall only be used for criminal justice purposes. The King may nevertheless make regulations providing that the data may also be used for research purposes and may make more detailed rules on such use.

The King will make regulations containing more detailed provisions on DNA registration, such as rules regarding registration in the convicted offenders database, the known suspects database and the crime-scene samples database, regarding the keeping and use of the databases, regarding searches of the databases and regarding retention of DNA profiles.

Section 13.*Fingerprint and photo database*

The police shall keep a database of fingerprints and photographs that have been collected in accordance with section 160 of the Criminal Procedure Act and the provisions of the Prosecution Regulations.

The police may keep a database of fingerprints of police employees who may come into contact with crime scenes or evidence.

Section 14.*Requirement to establish databases by means of regulations*

Prior to the establishment of a central database, the King will make regulations specifying

1. the legal basis for the processing,
2. the purpose of the processing,
3. the identity of the controller,
4. the categories of data that may be recorded,
5. which persons in the police or the prosecuting authority have access to the data,
6. data disclosure rules,
7. access to, rectification, restriction of processing and erasure of data, and
8. data security and internal control.

The requirement to make regulations does not apply to the alignment of data from databases that are subject to the Police Databases Regulations if the processing follows the rules that apply to the source database.

Chapter 4. Data security and internal control

Section 15.*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 data.

To achieve satisfactory data security, the controller and the processor shall document the data system and the security measures. Such documentation shall be accessible to the staff of the controller and of the processor. The documentation shall also be accessible to the supervisory authorities.

Any controller who allows others to have access to data shall ensure that they satisfy the requirements of the first and second paragraphs.

Section 16.*Internal control*

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

The controller shall document the measures. Such documentation shall be accessible to the staff of the controller and of the processor. The documentation shall also be accessible to the supervisory authorities.

Section 17.*Requirement of trackability*

The use of data shall be trackable.

Data regarding use of the system may be utilised to

1. administer the system,
2. detect and resolve security breaches in the system, or
3. detect and impose sanctions for the unlawful processing of personal data.

Data regarding use of the system shall be recorded and stored for at least one year and erased after no more than three years.

Section 18.*The processor's handling of personal data*

No processor may process personal data otherwise than in the manner prescribed in a written agreement or instructions. Nor may the data be handed over to third parties for storage or manipulation without such agreement.

The agreement with the controller shall state that the processor has a duty to implement such security measures as are prescribed in section 15.

Any person who is employed by or performs a service or work for a processor, and who gains access to data that are subject to a duty of confidentiality under this Act, shall be subject to a duty of confidentiality under section 35. Such a duty shall be set out in the agreement with the controller. Any person who is employed by or performs a service or work for a processor may be required to submit an exhaustive, expanded police certificate of conduct. The processor is subject to a duty to state who has access to the confidential data.

Chapter 5. Disclosure and access to data

Section 19.*General provisions on the disclosure of data*

The police and the prosecuting authority may disclose data if they are allowed to do so under the provisions on the duty of confidentiality in chapter 6, and the conditions governing disclosure laid down in section 8, second paragraph, and section 20 have been met for such data as are mentioned there.

Section 20.*Special provisions on the disclosure of unverified data*

As far as possible, data shall be verified before they are disclosed. The data shall preferably be disclosed in written form, and in such case shall be presented as unverified. If unverified data are disclosed orally, attention should be called to the fact that the data are unverified.

Unverified data may be disclosed if necessary for verification of the data.

In connection with disclosure of data for use in an individual criminal case and in connection with activities to avert and prevent criminal offences, see sections 26 and 27, only the first paragraph, second sentence, applies.

The provision in section 53 applies correspondingly.

Section 21.*Access to data within the police and the prosecuting authority*

Employees of the police and the prosecuting authority may be granted access (the right to make direct searches) to data, or data may otherwise be made available to them, to the extent that they have an official need for the data, and it is for purposes that fall within the scope of this Act.

Data which by their nature are sensitive, or which have been provided by someone with a special need for protection, or which are unverified, should be subject to special limitations on access.

Section 22.*Disclosure of data to another country*

Data may be disclosed to foreign authorities for such purposes as are mentioned in section 26. Data may also be disclosed to cooperating foreign police authorities and security and intelligence services in order to avert or prevent criminal offences or if disclosure is necessary in order to verify the data. The provisions of section 27, third and fifth paragraphs, apply correspondingly. Disclosure of data to countries not bound by Directive (EU) 2016/680 and to international organisations is also subject to the conditions laid down in regulations.

Moreover, data may be disclosed or otherwise made available to foreign authorities or international organisations when this is prescribed by statute or convention or an agreement that is binding on Norway, or by an agreement between Norwegian and other Nordic authorities.

Chapter 6. Limitations to the duty of confidentiality

Section 23.*Scope of the duty of confidentiality*

Any person who is employed by or performs a service or work for the police or the prosecuting authority is under a duty to prevent others from gaining access to or obtaining knowledge of anything that comes to his knowledge in connection with such service or work concerning

1. an individual's personal affairs, or
2. technical devices or procedures, as well as operational or business matters, which for competition reasons it is important to keep secret in the interests of the person whom the data concerns.

The duty of confidentiality also applies to data which it is necessary to keep secret in the interests of the investigation of the particular case, the interests of surveillance and intelligence activities or the interests of police operations and the organisation of such operations. The limitations to the duty of confidentiality in section 22 and sections 24 to 34 are only applicable insofar as appropriate.

The duty of confidentiality also applies after the person concerned has terminated his service or work. Moreover, he may not use such data as are mentioned in this section in his own business or in service or work for others.

The duty of confidentiality also applies to disclosure to other persons in the police and the prosecuting authority, unless section 21 is applicable.

With regard to the duty of confidentiality in connection with interception of communications, chapter 16a of the Criminal Procedure Act applies.

Section 24.*The duty of confidentiality when there is no need for protection*

The duty of confidentiality does not preclude the data

1. being made known to others, insofar as the person to whom the duty of confidentiality is owed consents thereto,
2. being used when the need for protection must be deemed to be met by presenting the data in the form of statistics or by otherwise eliminating identifiers, or
3. being used when no legitimate interest indicates that the data should be kept secret, for example when they are publicly known or publicly accessible elsewhere.

Section 25.*The duty of confidentiality in relation to parties or the person whom the data concern, and to use in cases concerning compensation*

The duty of confidentiality does not preclude the data in a case being made known to the parties to the case, to aggrieved parties or surviving relatives, or to their representatives, and otherwise to those whom the data directly concern.

Nor does the duty of confidentiality preclude the use of data in cases concerning compensation following criminal prosecution under chapter 31 of the Criminal Procedure Act.

This does not apply to data that may be detrimental to the police's efforts to prevent or detect criminal offences or maintain peace and order if they become known, unless otherwise prescribed by the provisions of the Criminal Procedure Act regarding access to documents.

Section 26.*The duty of confidentiality in individual criminal cases*

The duty of confidentiality does not preclude the use of data in an individual criminal case, including in connection with criminal investigation, case preparation, the decision on the case, implementation of the decision, follow-up and checks.

Section 27.*The duty of confidentiality in connection with activities to avert and prevent criminal offences*

The duty of confidentiality shall not preclude the police disclosing data if disclosure is necessary in order to avert the commission of a criminal offence.

Nor does the duty of confidentiality preclude the disclosure of data to

1. public bodies, in order to prevent criminal offences, or
2. private bodies or individuals, if this is necessary in order to prevent criminal offences and other solutions must be assumed to be inadequate.

Disclosure must in any event be a proportionate measure in the situation in question, and particular importance shall be attached to whether the data are transmitted to a recipient who is subject to a duty of confidentiality, how the recipient can be expected to use the data and whether uncertainty attaches to the data due to their nature or source. If it is possible and appropriate to notify the data subject, this should be done before the data are disclosed.

Nor does the duty of confidentiality preclude the police disclosing data to other public bodies and institutions that are part of a crime-prevention cooperation mechanism when this is necessary in order to prevent crime. The provision of the third paragraph applies.

Decisions regarding disclosure of data under the second paragraph shall be made by the controller. The data shall preferably be disclosed in written form. The controller shall record which data are disclosed, to whom they are disclosed and the reason for their

disclosure. If the data are unverified, this shall be specifically stated. The duty to record the disclosure also applies to the disclosure of data under the first paragraph.

Section 28.*The duty of confidentiality in connection with the police's other tasks*

The duty of confidentiality does not preclude the disclosure of data to public bodies and private bodies or individuals insofar as this is necessary for the performance of the activities of the uniformed service or the police's service and assistance functions.

The provisions of section 27, third paragraph, apply correspondingly.

Section 29.*The duty of confidentiality in connection with disclosure of data for use in the police's public administration activities, etc.*

The duty of confidentiality does not preclude the disclosure of data to other employees of the police or the prosecuting authority insofar as this is necessary for the exercise of the police's public administration activities and civil duties.

The King will make regulations containing more detailed provisions on the disclosure of data for use in the police's public administration activities and civil duties.

Section 30.*The duty of confidentiality in connection with disclosure of data to public bodies in their interest*

The duty of confidentiality does not preclude the disclosure of data to other public bodies in their interest, if this is necessary in order to promote the statutory tasks of the recipient body or to prevent it from conducting its activities in an improper manner.

The provisions of section 27, third paragraph, first sentence, and fifth paragraph, apply correspondingly.

The King will make regulations containing more detailed provisions on the disclosure of data to public bodies in their interest, including to whom the data shall be disclosed, which categories of data may be disclosed, the criteria that determine the necessity of disclosure, the duty of the controller under section 48 to inform the data subject and the data subject's right of access under section 49, first paragraph.

Section 31.*The duty of confidentiality in connection with disclosure of data to private recipients in their interest*

The duty of confidentiality does not preclude the disclosure of data to private recipients in their interest, if this is necessary in order to promote the recipient's statutory tasks or to prevent the improper conduct of activities.

The provisions of section 27, third paragraph, first sentence, and fifth paragraph, apply correspondingly.

The King will make regulations containing more detailed provisions on the disclosure of data to private recipients in their interest, including to whom data must be disclosed, which categories of data may be disclosed, the criteria that determine the necessity of disclosure, the duty of the controller under section 48 to inform the data subject and the data subject's right of access under section 49, first paragraph.

Section 32.*The duty of confidentiality in connection with statistical processing, the preparation of reports and plans, etc.*

The duty of confidentiality does not preclude the use of data for statistical processing, for the preparation of reports and plans or in connection with auditing or other forms of inspection.

Section 33.*The duty of confidentiality in connection with research*

When it is deemed reasonable and does not entail a disproportionate disadvantage to other interests, it may be decided that data in individual cases are to be disclosed for use in research, notwithstanding the duty of confidentiality in section 23.

In criminal cases, any decision under the first paragraph shall be made by the Director of Public Prosecutions and otherwise by the National Police Directorate, or by the Ministry of Justice in relation to data in cases handled by the Police Security Service.

The provisions of section 13d, second and third paragraphs, and section 13e of the Public Administration Act are applicable insofar as appropriate.

Section 34.*The duty of confidentiality in connection with disclosure to the public of data in criminal cases*

The duty of confidentiality mentioned in section 23, first paragraph, does not preclude the disclosure of data from a criminal case to the public, subject to the following conditions:

1. When disclosure is necessary to safeguard the general deterrent effect of prosecution, to carry out public control of the exercise of authority and to provide objective, matter-of-fact information about events of general interest. Data may also be disclosed with the aim of helping to solve a criminal offence, see section 26.
2. Data shall be provided without using names or other identifying data, unless this is necessary for the purpose of disclosure, or to prevent confusion, or the data are already publicly known.

3. Data that have not been investigated shall normally not be made public. The provision in section 20, first paragraph, first sentence, applies correspondingly.

The King will make regulations containing more detailed provisions on the disclosure of data to the public in criminal cases.

Section 35.*Imposition of a duty of confidentiality*

The police or the prosecuting authority may impose a duty of confidentiality when someone receives data that are subject to a duty of confidentiality in connection with making a statement to or in any other way assisting the police or the prosecuting authority. The same applies when aggrieved parties, surviving relatives or their representatives receive data that are subject to a duty of confidentiality, see section 25, first paragraph.

The police or the prosecuting authority may impose on any person who performs a service or works for a state or municipal body a duty of confidentiality in respect of such data as are mentioned in section 23, second paragraph, when the body receives data that are subject to a duty of confidentiality under this Act.

A breach of the duty of confidentiality under the first and second paragraphs is punishable under section 209 of the Penal Code, provided that the person concerned has been warned that a breach may have such consequences. The authority concerned shall ensure that the duty of confidentiality and the threat of punishment are made known to those concerned, and may require a written declaration to the effect that they are aware of and will respect the rules.

Chapter 7. Criminal records checks and certificates

Section 36.*Criminal records checks*

A criminal records check may only be carried out when it is authorised by statute or by regulations laid down pursuant to statute. The data disclosed through the check shall be provided in the following ways:

1. As a police certificate of conduct. The document is issued for use in the recipient's interest and may contain data detailing whether a natural or legal person has been sentenced to a penalty or other criminal sanctions or other measures as a result of a criminal offence, or is being prosecuted. A police certificate of conduct issued in another EEA country is deemed equivalent to a Norwegian police certificate of conduct. The disclosure of new or updated data after a police certificate of conduct has been issued is regulated by section 43.

2. As a conduct assessment. The assessment is given to a recipient who has the right to collect data relating to an individual because that individual is or will be subject to special duties by law. Data may be collected on such matters as are mentioned in the first paragraph, sub-paragraph 1.
3. As a criminal record printout. The document is issued for use in criminal cases and may contain data detailing whether a natural or legal person has been the subject of a penalty or other criminal sanctions or other measures as a result of a criminal offence.

A requirement of up to 5 years' residence in Norway may be laid down by statute or regulations made pursuant to statute if, in connection with a criminal records check, no such police certificate of conduct as is mentioned in the first paragraph, sub-paragraph 1, can be presented, and significant public interests warrant doing so. The required period of residence may only exceed 5 years if this is warranted by significant security interests.

Section 37.*Purposes that warrant use of a police certificate of conduct*

A police certificate of conduct, see section 36, first paragraph, sub-paragraph 1, may only be used to exclude a natural or legal person from a position, occupation, activity or other function if

1. the criminal offence renders a person unsuitable, and the failure to exclude him could entail substantial harmful consequences,
2. the failure to exclude a person could be offensive or undermine public confidence,
3. the position, etc. entails responsibility for or requires the trust of persons whose ability to take care of themselves or their interests is impaired by age, illness or disability,
4. exclusion may prevent persons from abusing or having a harmful influence on minors, or help to increase confidence that minors are in the care of suitable persons,
5. exclusion may help to ensure that a person who is to adopt a minor, or who is to have responsibility, over time or on a regular basis, for the 24-hour care of minors, is suitable for the task, or
6. there is a risk that a person will reoffend.

A police certificate of conduct may also be used if international legal obligations require documentation of such matters as are mentioned in section 36, first paragraph, sub-paragraph 1.

Section 38.*Police certificate of conduct issued in special cases*

A police certificate of conduct may be issued to a person who requires such a certificate for entry to, a visa for, a work permit for or settlement in another country, or for other purposes for which provisions in other countries require documentation regarding such matters as are mentioned in section 36, first paragraph, sub-paragraph 1. This applies correspondingly to a person who applies for employment at

a foreign embassy or similar institution in Norway. The certificate may be exhaustive and expanded, see section 41, if this is deemed necessary and relevant based on the requirements set in the national legal provisions of the country in question.

The King may make regulations under this Act providing that a police certificate of conduct may be used in cases other than the cases provided for in this Act. The conditions in section 37 apply correspondingly.

Any person authorised by the King may decide that a police certificate of conduct may also be used in other special cases. Such decisions shall apply for a limited period of time not exceeding 15 months. The decision may not be renewed.

Section 39.*Police certificate of conduct for persons who are to care for or perform tasks related to minors (childcare certificate of conduct)*

In police certificates of conduct issued for the purposes mentioned in section 37, first paragraph, sub-paragraph 4, it shall be indicated whether the person has been charged or indicted, accepted a fine issued by the prosecuting authority or been convicted of contravention of sections 162, 192, 193, 194, 195, 196, 197, 199, section 200, second paragraph, section 201 first paragraph (c), sections 201 a, 203, 204 a, 219, 224, section 229 second and third penalty alternatives, sections 231, 233 or 268, see section 267, of the General Civil Penal Code of 1902, or sections 231, 232, 257, 258, 274, 275, 282, 283, 291, 293, 294, 295, 296, 299, 301, 302, 303, 304, 305, 306, 309, 310, 311, 312, 314, 327 or 328 of the Penal Code. Contravention of sections 192, 193, 194, 195, 196, 197, 199, section 200, second paragraph, section 201, first paragraph, (c), sections 201 a, 204 a or 233 of the General Civil Penal Code of 1902 or sections 275, 291, 293, 294, 295, 296, 299, 301, 302, 303, 304, 305, 306, 310, 311, 312 or 314 of the Penal Code shall be indicated in accordance with section 41, sub-section 1. Contravention of sections 162, 203, 219, 224, section 229, second and third penalty alternatives, sections 231 or 268, see section 267, of the General Civil Penal Code of 1902, or sections 231, 232, 257, 258, 274, 282, 283, 309, 327 or 328 of the Penal Code shall be indicated in accordance with section 40.

Special grounds must exist in order to introduce requirements in regulations made pursuant to other legislation specifying more or fewer penal provisions than those set out in the first paragraph.

A police certificate of conduct issued for the purposes mentioned in section 37, first paragraph, sub-paragraph 5, may be exhaustive and expanded, see section 41, if so prescribed by other legislation.

Section 40.*Ordinary police certificate of conduct*

1. Unless specified otherwise in a statute or in regulations made pursuant to statute, an ordinary police certificate of conduct shall be issued.
2. Unless otherwise stated in sub-sections 5, 6 or 7, an ordinary police certificate of conduct shall indicate

(a) suspended and immediate sentences of imprisonment,
(b) preventive detention sentences or, if applicable, preventive supervision sentences,
(c) community sentences or, if applicable, community service sentences,
(d) youth sentences,
(e) sentences of loss of rights,
(f) fines for criminal offences subject to a maximum penalty of imprisonment for a term exceeding 6 months, and
(g) convictions resulting in committal to psychiatric care or committal to care or, if applicable, preventive supervision.

3. With the exception of the cases dealt with in sub-section 4, an ordinary police certificate of conduct shall not indicate
(a) convictions resulting in deferment of sentencing,
(b) waivers of prosecution under sections 69 and 70 of the Criminal Procedure Act,
(c) fines for criminal offences subject to a maximum penalty of imprisonment for a term not exceeding 6 months,
(d) on-the-spot fines,
(e) cases remitted to the National Mediation Service for mediation, see section 71a of the Criminal Procedure Act, or
(f) cases transferred to the Child Welfare Service.

4. If sanctions referred to in both sub-section 2 and sub-section 3 are imposed simultaneously, the total sanction may be indicated in the certificate.

5. An ordinary police certificate of conduct shall not indicate sanctions imposed by a judgment passed, or a fine issued by the prosecuting authority accepted, more than 3 years prior to the issue of the certificate, unless otherwise provided by sub-sections 6, 7 or 8. The permanent loss of rights shall always be indicated.

6. An ordinary police certificate of conduct shall not indicate
(a) suspended sentences of imprisonment or fines, if the offence was committed by an individual under 18 years of age more than 2 years prior to the issue of the certificate, or
(b) youth sentences or community sentences, if the offence was committed by an individual under 18 years of age more than 5 years prior to the issue of the certificate.

7. An ordinary police certificate of conduct shall indicate convictions resulting in
(a) immediate imprisonment for a term exceeding 6 months, if the convicted person was released less than 10 years prior to the issue of the certificate,
(b) sentences of preventive detention or, if applicable, preventive supervision, if the convicted person was released less than 10 years prior to the issue of the certificate,
(c) community sentences or, if applicable, community service, where the alternative sentence is imprisonment for a term exceeding 6 months and the community sentence was served less than 10 years prior to the issue of the certificate,
(d) loss of rights, which terminated less than 10 years prior to the issue of the certificate, and

(e) committal to psychiatric care or committal to care or, if applicable, preventive supervision, if the sanction terminated less than 10 years prior to the issue of the certificate. The termination of such a sanction shall also be indicated in the certificate.

8. If a person has several convictions resulting in immediate imprisonment for a term of 6 months or more, preventive supervision, preventive detention or committal to psychiatric care or committal to care, all of the convictions shall be included in the certificate, even if only one of them should be indicated pursuant to the time-limit laid down in sub-section 7.
9. The King will make regulations containing more detailed provisions on the indication of foreign sanctions and measures in police certificates of conduct.

Section 41.*Exhaustive and expanded police certificate of conduct*

1. An exhaustive police certificate of conduct shall indicate all penalties, other criminal sanctions and other measures recorded in the sanctions database in connection with a criminal offence. The time limitations in section 40 do not apply. However, an exhaustive police certificate of conduct shall not indicate
   (a) cases remitted to the Mediation Service under section 71a, first and second paragraphs, of the Criminal Procedure Act, if the person concerned has not committed any further criminal offences 2 years after the mediation procedure was concluded with an approved agreement, a youth plan or a Mediation Service plan.
   (b) on-the-spot fines, and
   (c) sanctions imposed on a person who was under the age of 18 at the time the act was committed and who has not committed any serious or repeated criminal offences, nor committed any further offences. The King will make regulations containing more detailed provisions on, inter alia, the period of time for which offences committed at a young age shall be indicated in an exhaustive police certificate of conduct and what are to be deemed serious and repeated offences.
2. In such police certificates of conduct as are mentioned in sub-section 1 and section 40, pending cases may only be indicated if this is required by statute or regulations made pursuant to statute (expanded police certificate of conduct). If pending cases are indicated, the police certificate of conduct shall provide a brief explanation of what each pending case concerns, what kind of penal provisions are involved and how far the prosecution of the case has progressed.

Section 42.*Indication of fewer data in police certificates of conduct*

Any person so authorised by the King may decide that fewer data shall be indicated in the police certificate of conduct, as long as this is not incompatible with the purpose of the certificate.

Section 43.*Disclosure of new or updated data after the police certificate of conduct has been issued*

Significant new data may be disclosed to the user of a previously issued police certificate of conduct if the conditions for the issue of the certificate are still fulfilled. No data other than those specified in the legal basis for issuing the original certificate may be disclosed.

Any person who has requested the issue of a police certificate of conduct shall as soon as possible be notified that new data have been disclosed to the user. If there are no new data, the matter shall be concluded by notifying the user accordingly.

Section 44.*Rules of procedure for the issue of a police certificate of conduct*

A request for the issue of a police certificate of conduct must be submitted by the person whom the certificate concerns. The person must provide adequate proof of identity.

The person requesting such issue must document that he meets the conditions.

The police certificate of conduct shall be issued as soon as possible, and be sent to the person who has requested it.

Section 45.*Conduct assessments*

A conduct assessment shall indicate such sanctions as are mentioned in section 41, sub-section 1, unless otherwise provided by statute or by regulations made pursuant to statute.

The recipient may demand a conduct assessment without the consent of the person whom the assessment concerns. The provision in section 48, second paragraph, sub-paragraph 1, applies correspondingly.

The King will make regulations containing more detailed provisions on conduct assessments.

Section 46.*Criminal record printouts*

For use in an individual criminal case, the police, the prosecuting authority, the correctional services or the courts may submit a request for a criminal record printout relating to a person specified by name.

The criminal record printout shall indicate all penalties, other criminal sanctions and other measures resulting from criminal offences. Data relating to an enterprise may only be indicated in a printout concerning the enterprise.

Section 47.*The duty of confidentiality of recipients of data in connection with a criminal records check*

Any person who receives such data as are mentioned in sections 38 to 45 in connection with a criminal records check shall prevent unauthorised persons from gaining access to or knowledge of the data in the criminal records check.

A breach of the duty of confidentiality under the first paragraph is punishable under section 209 of the Penal Code, if the recipient of the data was informed that contravention could have such consequences.

Chapter 8. Duty to inform the data subject, access, rectification, restriction of processing and erasure

Section 48.*The duty to inform the data subject*

The controller has a duty to inform the data subject that personal data has been disclosed to public bodies and private bodies or individuals in their interest, see sections 30 and 31.

However, the duty to inform the data subject shall not apply

1. if the controller is subject to a duty of disclosure laid down by statute or pursuant to statute,
2. if it is necessary to make an exception in the interests of fighting crime, national and public security, the execution of criminal sanctions, the protection of persons other than the data subject or the recipient body's statutory supervisory functions,
3. if disclosure is not of significant importance for the data subject, or
4. if it is provided by statute or pursuant to statute that the duty to inform the data subject does not apply.

Section 49.*Access to information*

In an individual criminal case, the data subject has a right of access to documents in accordance with the provisions of the Criminal Procedure Act.

Other than in an individual criminal case, the data subject has the right to be informed of which data relating to him have been recorded.

Both in an individual criminal case and generally, the data subject has the right to be informed of whether data relating to him have been disclosed, to whom they have been disclosed and which data have been disclosed.

Access to information under the second and third paragraphs may be refused if necessary in the interests of

1. fighting crime,

2. national and public security,
3. the execution of criminal sanctions,
4. the protection of persons other than the data subject, or
5. the recipient body's statutory supervisory functions.

Section 50.*Erasure, restriction of processing and deposit of data that are no longer required for the purpose of the processing*

Data shall not be stored any longer than is necessary for the purpose of the processing. The data shall be erased or restricted, unless they are to be retained in accordance with the Act of 4 December 1992 No. 126 relating to archives or other legislation.

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 outweighs the disadvantages this may entail for the individual concerned. The data shall not be retained in ways that make it possible to identify the data subject any longer than necessary.

Data obtained through interception of communications which has not been used in the case shall be restricted when the case has been decided by final and enforceable judgment or final decision not to prosecute. Restricted data may be used in the event of a petition for reopening of a court case, the resumption of a criminal investigation, or to protect the legitimate interests of a person charged. Data which is not lawful to retain pursuant to the Criminal Procedure Act 216 g shall be erased as soon as possible. The provision applies correspondingly to data obtained pursuant to the Criminal Procedure Act sections 216 m and 216 o, and to data obtained pursuant to the Criminal Procedure Act sections 202 a and 202 c insofar as appropriate. The King will make regulations containing more detailed provisions on the erasure and use of restricted data from interception of communications.

Section 51.*Rectification, restriction of processing and erasure of data that are inaccurate or deficient*

The controller shall on his own initiative or upon request by the data subject rectify data that are deficient and, if possible or necessary, supplement or update them. Deficient data that obviously have no documentary value may be erased.

Data containing an error that cannot be rectified shall be restricted or erased. If there are grounds to believe that erasure could affect the legitimate interests of the data subject, the data shall be restricted.

Data that are restricted pursuant to this section may only be used if this is necessary in order to document which data were processed.

Section 52.*Use of data that have been restricted*

Data that have been restricted pursuant to sections 50 or 51 or on another basis may only be used for the purposes due to which the data were not erased. The King will make regulations containing more detailed provisions on the purposes for which restricted data may be used.

Section 53.*The police's duty to act in the event of errors or deficiencies*

If such deficient data as are mentioned in section 51 have been processed or other breaches of the Act have occurred, the controller shall as far as possible ensure that the error does not affect the data subject. If the data have been disclosed, the recipient of the data shall be notified of the error without undue delay and requested to rectify, erase or restrict the data in accordance with the legal basis of the recipient.

Section 54.*Procedural rules for access, rectification, restriction of processing and erasure*

Requests for access to and rectification, restriction of processing or erasure of data shall be submitted in writing to the police or the prosecuting authority. The request must specify the processing operations concerned. The person submitting the request must provide adequate proof of identity. The controller decides whether the request shall be complied with, and ensures that only the data relating to the person concerned are rectified, restricted, erased or accessed.

A response shall be given to the request as soon as possible, and within 30 days at the latest. If the request is complied with, the data shall be disclosed in writing, unless the King decides otherwise in respect of a particular processing operation.

If the request is rejected, grounds shall be given which do not reveal that data have been recorded.

Chapter 9. Right of appeal, compensation and legal remedies

Section 55.*Right of appeal*

The data subject or any person who believes himself to be a data subject may appeal decisions made pursuant to this Act to a superior body, including decisions on

1. criminal records checking,
2. breaches of the duty of confidentiality,
3. access, rectification, restriction of processing and erasure, or
4. compensation.

Decisions made by the Director of Public Prosecutions may not be appealed. The provisions of chapter VI of the Public Administration Act apply in so far as they are appropriate.

The rights of the data subject under sections 59 and 68 are not affected by the provisions of this section.

The provision in section 54, last paragraph, applies accordingly.

Section 56.*Compensation*

The controller shall pay compensation for damage suffered as a result of data being processed contrary to provisions laid down in or pursuant to this Act, even if no one is to blame for the damage. In the event of breaches of the provisions on disclosure and the duty of confidentiality in sections 19 to 35, the general rules of compensation apply. The compensation shall be equivalent to the financial loss incurred by the injured party as a result of the unlawful processing of the data.

The compensation may be extended to such compensation for damage of a non-financial nature as seems reasonable, unless it is established that the damage is not due to an error or omission on the part of the controller.

When a claim is lodged after a person has been charged in a criminal case, the procedural rules of chapter 31 of the Criminal Procedure Act shall nevertheless apply in so far as they are appropriate and unless otherwise prescribed pursuant to this Act.

Section 57.*Judicial remedies*

The data subject may, without prejudice to the rights under section 55, first paragraph, and section 59, bring proceedings against the controller or the processor if the rights of the person concerned under the Act have been infringed as a result of the processing of the data relating to the person concerned.

The data subject may, without prejudice to the rights under section 60, third paragraph, bring proceedings against the Data Protection Authority when the Data Protection Authority has made a decision that is legally binding on the data subject. The same applies if the Data Protection Authority neglects to deal with a request for a processing check within 3 months, or neglects to give notice of the progress of the request or its outcome within 3 months.

Chapter 10. Supervision

Section 58.*The supervisory powers of the Data Protection Authority*

The Data Protection Authority shall supervise that the Act and regulations made pursuant to the Act are complied with, and that errors or deficiencies are rectified. This does not apply to data processed by the Police Security Service, which is subject to supervision by the Parliamentary Oversight Committee on Intelligence and Security Services pursuant to section 68 and the Act of 3 February 1995 No. 7 pertaining to oversight of intelligence and security services.

Section 59.*Checks by the Data Protection Authority upon request by the data subject*

The Data Protection Authority shall, upon request by the data subject, or any person who believes himself to be a data subject, check that the data relating to the person concerned have been processed in accordance with the Act and that the rules regarding access have been observed.

The provision in section 54, last paragraph, applies accordingly.

Section 60.*The Data Protection Authority's corrective powers and administrative fines*

The Data Protection Authority may issue an order to the controller to the effect that processing of data that is contrary to sections 15 or 16 must cease, or may set conditions that must be met in order for the processing to comply with these provisions. Moreover, in connection with the processing of data other than in individual criminal cases, the Data Protection Authority may issue an order to the controller to the effect that processing contrary to this Act must cease, or may set conditions that must be met in order for the processing to comply with the Act. The Data Protection Authority may nevertheless not issue orders regarding access to data which are exempt from the right of access under section 49, or issue orders regarding compliance with the provisions on disclosure and the duty of confidentiality in chapters 5 and 6 or criminal records checks in chapter 7.

The Data Protection Authority may issue a reprimand if it deems that the processing of data in connection with criminal cases is contrary to the Act. The same applies to such processing as is mentioned in the first paragraph, last sentence. Such a reprimand shall be communicated to the controller, and a copy shall be sent to the controller's superior body.

The Data Protection Authority's decisions pursuant to the first paragraph can be appealed to the Privacy Appeals Board.

In connection with orders under the first paragraph, the Data Protection Authority may impose an administrative fine to run each day after expiry of the deadline set for compliance with the order until such time as the order is complied with.

Section 61.*Access*

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 their functions under this Act, the Data Protection Authority and the Privacy Appeals Board may demand admittance to places where data are processed and where devices for such processing are located. The Data Protection Authority may carry out such tests and 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 data or access to premises and devices pursuant to the first and second paragraphs is not limited by provisions relating to the duty of confidentiality.

Section 62.*Duty of confidentiality and police certificate of conduct*

Persons who as a result of inspection gain access to data that are subject to a duty of confidentiality under section 23 shall be subject to the same duty of confidentiality.

An exhaustive and expanded police certificate of conduct shall be required for persons who are to carry out supervision.

Section 63.*Data protection officer*

A data protection officer system shall be put in place.

The King will make regulations specifying the details of the system.

Chapter 11. The Police Security Service

Section 64.*The requirement of necessity for the Police Security Service*

The Police Security Service may only process data when this is necessary for police purposes and administrative activities within the Service. Furthermore, the conditions in the second and third paragraphs must be met.

In individual criminal cases, data processing powers are governed by the provisions of the Criminal Procedure Act.

Other than in individual criminal cases, data may only be processed by the Police Security Service where

1.

(a) in connection with the opening of a pre-emptive case, there are grounds to investigate whether any person is preparing to commit a criminal offence which the Police Security Service is tasked with preventing, or

(b) it is otherwise deemed necessary for preventive purposes to process data of significance for the performance of the tasks mentioned in sections 17b or 17d of the Police Act, including data relating to a foreign national where the processing of such data is deemed necessary following a specific security assessment of the person concerned. In this assessment of necessity, consideration must be given to whether the processing is a proportionate measure based on whether the foreign national comes from a country or an area which a current threat assessment indicates is associated with a risk relevant to the tasks listed in sections 17b and 17c of the Police Act. Correspondingly, the Police Security Service may also process data relating to sponsors in Norway of such foreign nationals, or

(c) it is necessary for the implementation of freezing under section 17g of the Police Act,

2. such processing is necessary for the Police Security Service's preparation of threat assessments,
3. such processing is necessary for cooperation with the police authorities and security and intelligence services of other countries,
4. such processing is necessary for security vetting or accreditation, subject to the limitations set out in section 67, or
5. such processing is necessary in order to document which data of no relevance to the Police Security Service have been made available to others.

Section 65.*Time-limited exemption from the requirements of specificity of purpose, necessity and relevance*

Data may in any case be processed for 4 months if necessary in order to ascertain whether the requirements of section 4, section 64, third paragraph, and section 6, first paragraph, sub-paragraph 1, are met.

The provisions of section 8, second and third paragraphs, apply accordingly.

Section 66.*Duty to inform the data subject and access to data*

The provisions regarding the duty to inform the data subject in section 48 and the right of access in section 49, second and third paragraphs, do not apply to the Police Security Service.

The Freedom of Information Act does not apply to access to data that are processed by the Police Security Service pursuant to this Act.

With regard to access to data that are processed in connection with security clearance, the provisions laid down in or pursuant to the Security Act apply.

Access to case documents in a freezing matter may be given under the rules of the Criminal Procedure Act, which apply in so far as they are appropriate.

Section 67.*Security vetting*

The Police Security Service may process data relevant to the question of security clearance in the context of a current security vetting matter. If the Police Security Service receives data that raise doubt as to whether a person who has already been given security clearance is suitable in terms of security, the data may be processed and forwarded to the clearance authority.

The Police Security Service shall not collect or process data solely because the data might be relevant to future security vetting.

The provisions of section 20 apply correspondingly to the disclosure of data relating to security vetting.

Section 68.*Supervision and the data subject's request for a processing check*

The Parliamentary Oversight Committee on Intelligence and Security Services exercises supervision pursuant to the Act of 3 February 1995 No. 7 pertaining to oversight of intelligence and security services.

Upon request by the data subject or any person who believes himself to be a data subject, the Committee shall check that the data relating to the individual concerned have been processed in accordance with this Act. Requests for a check of the processing of data by the Police Security Service shall be submitted pursuant to the Act of 3 February 1995 No. 7 pertaining to oversight of intelligence and security services.

The provision in section 54, last paragraph, applies accordingly.

Chapter 12. Regulations

Section 69.*Regulations*

The King may make regulations containing more detailed provisions on the implementation of this Act, including provisions on

1. further delimitation of the scope of the Act, see section 3, and provisions to the effect that the Act shall be applicable to parties other than the police and the prosecuting authority,
2. how the provisions of this Act are to be adapted for the processing of data in criminal cases,
3. consent, see section 2, sub-section 7,
4. what data may be processed under sections 5 and 64,
5. procedures for time-limited exemptions, see sections 8 and 65,
6. the databases mentioned in chapter 3, including which data may be processed,

7. data security in connection with the processing of data under this Act, see section 15, including more detailed provisions on organisational and technical security measures, who is the controller in respect of the various processing operations, and who shall be informed in case of non-compliance,
8. internal control, see section 16,
9. access to data, including for the purposes mentioned in section 29 of the Police Databases Act, and which persons have an official need for data, see section 21,
10. the disclosure of unverified data, see section 27,
11. procedures relating to the provisions on disclosure and the duty of confidentiality, see chapters 5 and 6,
12. the use and issue of police certificates of conduct, including provisions regarding
    (a) the use of police certificates of conduct in special cases, see section 38,
    (b) the indication of pending cases, see section 41, sub-section 2,
    (c) the procedure for carrying out a renewed criminal records check, see section 43,
    (d) the ability to issue a police certificate of conduct before the conditions for obtaining such a certificate have been met, how persons making requests shall provide proof of identity, to whom a request for a police certificate of conduct shall be submitted, how certificates shall be transmitted if they are not sent directly to the person making the request, the processing time for requests for police certificates of conduct and requirements relating to the retention of police certificates of conduct, see sections 44 and 47,
13. criminal record printouts, see section 46, and accreditation, see inter alia section 64, third paragraph, sub-paragraph 4,
14. who has a right of access to information and how information shall be disclosed, see section 48,
15. access procedures, see section 49,
16. when and how rectification, restriction of processing and erasure shall be carried out, see sections 50 and 51, including that erasure of data from police databases may take place when life or health is at stake or to protect strong privacy interests, see section 9 (c) of the Act of 4 December 1992 No. 126 relating to archives.
17. the retention and use of restricted data, see section 52,
18. when an exception may be made with regard to written disclosure, if it is assumed that it might be misused, see section 54,
19. who is the appeals body for decisions that are appealed, see section 55, and more detailed provisions regarding the processing of appeals concerning breaches of the duty of confidentiality, see section 55, first paragraph, sub-paragraph 2,
20. exemptions from chapter VI of the Public Administration Act and procedural rules in appeal cases, see section 55,
21. the application of the procedural provisions of chapter 31 of the Criminal Procedure Act in cases concerning such compensation as is mentioned in section 56, third paragraph,
22. the right of the Data Protection Authority to charge a fee for dealing with repeated or manifestly unfounded requests,

23. the distribution of supervisory powers under section 58 between the Data Protection Authority and other supervisory bodies that have supervisory powers provided by statute or regulations made pursuant to statute,
24. procedural rules for checks under sections 59 and 60,
25. procedure in freezing matters other than in criminal proceedings.

The King may also make regulations containing more detailed provisions on the processing of data prescribed by such conventions, etc. as are mentioned in section 22, second paragraph.

Chapter 13. Final provisions

Section 70.*Entry into force*

The Act shall enter into force from such date as the King may decide. The King may decide that different provisions of the Act may enter into force at different times.

The King may lay down more detailed transitional rules.