



Hendriks & James
Legal Translations



THE PERSONAL DATA PROTECTION ACT

including the data breach notification obligation and the extension of the powers of the Personal Data Protection Authority to impose administrative penalties (2016)

This publication contains the text of the Dutch Personal Data Protection Act in force as at 1 January 2016, as well as the English translation of it.

The texts contain the amendments regarding the data breach notification obligation and the extension of the powers of the Personal Data Protection Authority to impose administrative penalties (*Bulletin of Acts and Decrees* 2015, 230). Headings summarising the substance of the sections have been added by Eliëtte Vaal of AKD, a law firm that specialises in privacy and other areas of the law. The translation has been provided by Hendriks & James Legal Translations, an agency whose areas of specialisation include texts on privacy law. Hendriks & James has produced a clear, readable and accurate translation, drafted in line with the terminology used in the European Data Protection Directive 95/46/EC. The translation is not an official translation, nor may any rights be exercised under it.

© 2016 deLex / AKD N.V. / E.F. Vaal / Hendriks & James Legal Translations

ISBN: 978-90-8692-058-7

NUR: 820

Cover: rdesign*

Layout: az grafisch serviceburo, Den Haag

Uitgeverij deLex, Amsterdam

www.delex.nl

This publication has been sponsored by:

AKD

+31 88 253 5000

info@akd.nl

www.akd.nl

Hendriks & James Legal Translations

Korte Leidsedwardsstraat 12

1017 RC Amsterdam

+31 20 421 8519

info@hendriks-james.nl

www.hendriks-james.nl

Contents

Part 1	General provisions	7
Part 2	Rules on the lawfulness of the processing of personal data	9
	§ 1. Processing of personal data in general	9
	§ 2. The processing of special personal data	12
Part 3	Codes of conduct	17
Part 4	Notification and prior checking	18
	§ 1. Notification	18
	§ 2. Prior checking	20
Part 5	Information to be given to the data subject and the obligation to notify breaches of security of personal data to the Authority	21
Part 6	The data subject's rights	23
Part 7	Exceptions and restrictions	26
Part 8	Legal protection	27
Part 9	Supervision	28
	§ 1. The Dutch Data Protection Authority	28
	§ 2. The data protection official	32
Part 10	Sanctions	33
	§ 1. Administrative enforcement	33
	§ 2. Administrative penalties	33
	§ 3. Criminal sanctions	34
Part 11	Flow of data to countries outside the European Union	35
Part 12	Transitional and final provisions	37

The Personal Data Protection Act

Act of 6 July 2000, containing rules on the protection of personal data

We, Beatrix, by the Grace of God, Queen of the Netherlands, Princess of Oranje-Nassau, etc., etc., etc.

To all who shall see or hear these presents, greetings!

Whereas We have considered it necessary to implement Directive 95/46/EC of the European Parliament and of the Council of 23 November 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJEC L 281);

Having regard to Article 10 (2) and (3) of the Constitution;

We, therefore, having heard the Council of State, and in consultation with the States General, have approved and decreed as We hereby approve and decree:

Part 1 **General provisions**

Section 1

In this Act and the provisions based upon it:

- a. personal data means: any information relating to an identified or identifiable natural person;
- b. processing of personal data means: any operation or set of operations which is/are performed upon personal data, including in any case the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data;
- c. filing system means: any structured set of personal data, whether centralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria and relates to different persons;
- d. controller means: the natural or legal person or any other party who or the administrative body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Definitions

- e. processor means: the person who processes personal data on behalf of the controller without being subject to his direct authority;
- f. data subject means: the person to whom the personal data relate;
- g. third party means: any person other than the data subject, the controller, the processor or any person who, under the direct authority of the controller or the processor, is authorised to process the personal data;
- h. recipient means: the party to whom personal data are disclosed;
- i. the data subject's consent means: any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;
- j. the Minister means: the Minister of Security and Justice;
- k. Data Protection Authority or the Authority means: the Authority referred to in Section 51;
- l. official means: the data protection official referred to in Section 62;
- m. prior checking means: a check as referred to in Section 31;
- n. disclosure of personal data means: the publication or making available of personal data;
- o. collection of personal data means: obtaining personal data;
- p. Framework Act means: the Non-Departmental Administrative Bodies Framework Act;
- q. binding order: an independent order imposed for a violation;
- r. independent order: an order to perform specific acts, referred to in Section 5:2 (2) of the General Administrative Law Act to promote compliance with legal rules.

Section 2

- Scope**
1. This Act applies to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
 2. This Act does not apply to the processing of personal data:
 - a. in the course of a purely personal or household activity;
 - b. by or on behalf of the intelligence and security services referred to in the Intelligence and Security Services Act 2002;
 - c. for the purpose of performing the police responsibilities referred to in Sections 3 and 4 (1) of the Police Act 2012;
 - d. which is governed by or pursuant to the Persons Database Act;
 - e. for the implementation of the Judicial Information and Criminal Records Act, and
 - f. for the implementation of the Elections Act.

3. This Act does not apply to the processing of personal data by the armed forces if the Minister of Defence decides on this for purposes of deploying or making available the armed forces to maintain or promote the international legal order. The Authority will be notified of such decision as soon as possible.

Section 3

1. This Act does not apply to the processing of personal data carried out solely for journalistic, artistic or literary purposes, subject to the other provisions of this Part as well as Sections 6 to 11, 13 to 15, 25 and 49.

Exceptions for journalistic, artistic or literary purposes

2. The prohibition on processing personal data referred to in Section 16 does not apply in so far as this is necessary for the purposes referred to in subsection 1.

Section 4

1. This Act applies to the processing of personal data in the context of the activities of an establishment of a controller in the Netherlands.

Territorial scope

2. This Act applies to the processing of personal data by or on behalf of a controller who is not established in the European Union and who makes use of equipment, automated or otherwise, situated in the Netherlands, unless such equipment is used only for purposes of the transit of personal data.

3. A controller as referred to in subsection 2 is prohibited from processing personal data unless he designates a person or body in the Netherlands that acts on his behalf in accordance with the provisions of this Act. For the purposes of this Act and the provisions based upon it, he will be regarded as the controller.

Section 5

1. If the data subject is a minor and has not yet reached the age of sixteen, or has been placed under guardianship or under a protection order, instead of his consent that of his legal representative is required.

Consent of legal representative

2. Such consent may be withdrawn by the data subject or his legal representative at any time.

Part 2

Rules on the lawfulness of the processing of personal data

§ 1. *Processing of personal data in general*

Section 6

Personal data are processed in accordance with the law and in a proper and careful manner.

Fair processing

Section 7

Purpose limitation Personal data are collected for specified, explicit and legitimate purposes.

Section 8

Legal grounds for data processing

Personal data may be processed only if:

- a. the data subject has unambiguously given his consent to the processing;
- b. the data processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract and which are necessary for the conclusion of a contract;
- c. the data processing is necessary for compliance with a legal obligation to which the controller is subject;
- d. the data processing is necessary in order to protect a vital interest of the data subject;
- e. the data processing is necessary for the proper performance of a public law task by the relevant administrative body or the administrative body to which the data are disclosed, or
- f. the data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, unless such interests are overridden by the interests or the fundamental rights and freedoms of the data subject, notably the right to privacy, which require protection.

Section 9

Processing for incompatible purposes

1. Personal data may not be further processed in a way incompatible with the purposes for which they were collected.
2. When assessing whether processing is incompatible as referred to in subsection 1, the controller will in any event give consideration to:
 - a. the relationship between the purposes of the envisaged processing and the purposes for which the data were collected;
 - b. the nature of the data concerned;
 - c. the consequences of the envisaged processing for the data subject;
 - d. the way in which the data were collected, and
 - e. the extent to which appropriate safeguards have been put in place with respect to the data subject.
3. Further processing of the data for historical, statistical or scientific purposes is not considered incompatible if the controller has taken the measures necessary to ensure that the further processing is carried out solely for those specific purposes.
4. Personal data are not processed in so far as this is precluded by an obligation of secrecy resulting from an office, profession or legal rule.

Section 10

1. Personal data may not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the data were collected or for which they are further processed.
2. Personal data may be kept for longer than provided in subsection 1 in so far as they are kept for historical, statistical or scientific purposes and the controller has taken the measures necessary to ensure that the data concerned are used solely for those specific purposes.

Term of storage

Section 11

1. Personal data may be processed only in so far as they are adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.
2. The controller will take the measures necessary to ensure that personal data are correct and accurate in relation to the purposes for which they are collected or further processed.

Data minimisation and quality

Section 12

1. Any person acting under the authority of the controller or of the processor, including the processor himself, in so far as they have access to personal data, only processes them on instructions from the controller, unless required to do so by law.
2. The persons referred to in subsection 1 who are not already subject to an obligation of secrecy by virtue of an office, profession or legal rule are obliged to maintain secrecy with regard to the personal data to which they have access, save in so far as they are obliged to disclose them under any legal rule or pursuant to their responsibilities. Article 272 (2) of the Criminal Code does not apply.

Confidentiality

Section 13

The controller implements appropriate technical and organisational measures to protect personal data against loss or any unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures will guarantee a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. These measures also seek to prevent the unnecessary collection and further processing of personal data.

Security measures

Section 14

**Obligations
regarding
engagement of
processor**

1. If the controller has processing of personal data carried out by a processor on his behalf, he will ensure that the latter provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and in respect of the report of a breach of security, referred to in Section 13, which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data processed by him.

The controller will ensure compliance with those measures.

2. The carrying out of processing by way of a processor is governed by a contract or pursuant to a different legal act which establishes a commitment between the processor and the controller.

3. The controller will ensure that the processor:

- a. processes the personal data in accordance with Section 12 (1);
- b. fulfils the obligations incumbent on the controller pursuant to Section 13, and
- c. fulfils the obligations that are incumbent on the controller as regards the requirement to report a breach of security, referred to in Section 13, which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data processed by him.

4. If the processor is established in a different Member State of the European Union, then the controller will ensure that the processor complies with the law of that Member State, by way of derogation from subsection 3 (b) and (c).

5. For the purposes of keeping proof, the parts of the contract or the legal act relating to protection of personal data, the security measures, referred to in Section 13, and the obligation to report a breach of security which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data processed by him, will be in writing or in another equivalent form.

Section 15

Duty of compliance

The controller will ensure that the obligations referred to in Sections 6 to 12 and Section 14 (2) and (5) of this Part are complied with.

§ 2. The processing of special personal data

Section 16

**Prohibition on
processing
sensitive personal
data**

The processing of personal data relating to a person's religion or belief, race, political affinity, health, sex life and trade union membership is prohibited, subject to the provisions of this Division.

The same applies to personal data concerning criminal law matters and personal data on unlawful or objectionable conduct in connection with a prohibition imposed in response to such conduct.

Section 17

1. The prohibition on processing personal data relating to a person's religion or belief referred to in Section 16 does not apply if the processing is carried out by: **Exceptions for religion or belief**
- a. church societies, independent sections of them or other societies based on spiritual principles in so far as such data concern persons belonging to them;
 - b. institutions founded on religious or philosophical principles in so far as this is necessary in relation to their purpose and for achieving their principles, or
 - c. other institutions in so far as this is necessary for the purposes of providing spiritual care to the data subject, unless he has objected to this in writing.
2. In the cases referred to in subsection 1 (a), the prohibition also does not apply to personal data relating to the religion or belief of the data subject's family members in so far as:
- a. the society concerned has regular contact with the family members by reason of its purpose, and
 - b. those family members have not objected to this in writing.
3. In the cases referred to in subsections 1 and 2, no personal data may be disclosed to third parties without the data subject's consent.

Section 18

- The prohibition on processing personal data relating to a person's race referred to in Section 16 does not apply if the processing is carried out: **Exceptions for race**
- a. to identify the data subject and only in so far as this is unavoidable for that purpose;
 - b. with the purpose of conferring a preferential position on persons of a certain ethnic or cultural minority group in order to eliminate or reduce *de facto* disadvantages connected with race, and only if:
 - 1°. this is necessary for that purpose;
 - 2°. the data relate solely to the country of birth of the data subject, his parents or grandparents, or to other criteria set by law on the basis of which it can be objectively determined whether a person belongs to a minority group as referred to in the opening lines of (b), and
 - 3°. the data subject has not objected to this in writing.

Section 19

Exceptions for political affinity

1. The prohibition on processing personal data relating to a person's political affinity referred to in Section 16 does not apply if the processing is carried out:
 - a. by institutions founded on political principles in relation to their members or their employees or other persons belonging to such institutions, in so far as this is necessary for achieving its principles in relation to the purpose of any such institution, or
 - b. in view of the requirements that may reasonably be made regarding political affinity in connection with the performance of duties in administrative bodies and on advisory boards.
2. In the case referred to in subsection 1 (a), personal data may not be disclosed to third parties without the data subject's consent.

Section 20

Exception for trade union membership

1. The prohibition on processing personal data relating to a person's membership of a trade union referred to in Section 16 does not apply if the processing is carried out by the trade union concerned or the trade union confederation to which that union belongs, in so far as this is necessary in relation to the purpose of the trade union or trade union confederation.
2. In the case referred to in subsection 1, personal data may not be disclosed to third parties without the data subject's consent.

Section 21

Exceptions for health

1. The prohibition on processing personal data relating to a person's health referred to in Section 16 does not apply if the processing is carried out by:
 - a. healthcare providers, institutions or health care or social services facilities in so far as this is necessary for the proper treatment or care of the data subject or the management of the institution or professional practice concerned;
 - b. insurers as referred to in Section 1:1 of the Financial Supervision Act and financial service providers who provide insurance brokerage services as referred to in Section 1:1 of the Financial Supervision Act, in so far as this is necessary in order to:
 - 1°. assess the risk to be insured by the insurer and the data subject has not made any objection, or
 - 2°. perform the insurance agreement;
 - c. schools in so far as this is necessary in relation to special support for pupils or for making special arrangements in connection with the state of their health;
 - d. an institution of rehabilitation, a special probation officer, the Child Care and Protection Board or the certified body, referred to in Section 1:1 of the Youth

Act, and the legal person, referred to in Article 256 (1) or Article 302 (2) of Book 1 of the Civil Code, in so far as this is necessary for the performance of their statutory duties;

- e. the Minister in so far as this is necessary in relation to the enforcement of custodial sentences or measures involving the deprivation of liberty, or
 - f. administrative bodies, pension funds, employers or institutions that perform activities on their behalf in so far as this is necessary for:
 - 1°. proper compliance with legal rules, pension schemes or collective employment contracts that provide entitlements depending on the state of the data subject's health, or
 - 2°. the reintegration or support of employees or recipients of welfare benefits in connection with illness or disability.
2. In the cases referred to in subsection 1, the data are only processed by persons who have an obligation of secrecy by virtue of an office, profession or legal rule or pursuant to a contract. If the controller processes data personally and he is not already subject to an obligation of secrecy by virtue of an office, profession or legal rule, he is obliged to maintain secrecy with regard to the data, save in so far as he is obliged to disclose them by law or his responsibilities require that they be disclosed to others who are authorised to process them pursuant to subsection 1.
3. The prohibition on processing other personal data referred to in Section 16 does not apply in so far as this is necessary in addition to the processing of personal data relating to a person's health referred to in subsection 1 (a), for the proper treatment or care of the data subject.
4. Personal data relating to hereditary characteristics may be processed only in so far as such processing is carried out in relation to the data subject from whom the data concerned have been collected, unless:
- a. a compelling medical interest prevails, or
 - b. the processing is needed for scientific research or statistics.
- In the case referred to in (b), Section 23 (1) (a) and (2) apply equally.
5. Further rules may be issued regarding the application of subsection 1 (b) and (f), by order in council.

Section 22

1. The prohibition on processing personal data relating to criminal law matters referred to in Section 16 does not apply if the processing is carried out by bodies that are responsible pursuant to the law for applying criminal law or by controllers who have acquired them pursuant to the Police Data Act or the Judicial Data and Criminal Records Act.
2. The prohibition does not apply to a controller who processes these data for his own purposes in order to:

Exceptions for data relating to criminal law matters

- a. assess a request from the data subject to take a decision on him or to provide a service to him, or
 - b. protect his interests in cases of criminal offences committed against him or which, on the basis of facts and circumstances, can be expected to be committed against him or persons employed by him.
3. The processing of these data on staff employed by the controller is carried out in accordance with rules adopted in line with the procedure referred to in the Works Councils Act.
 4. The prohibition does not apply if these data are processed on behalf of third parties:
 - a. by controllers acting pursuant to a licence under the Private Security Organisations and Detective Agencies Act, or
 - b. if such third party is a legal person who is part of the same group as referred to in Article 2:24 (b) of the Civil Code, or
 - c. if appropriate and specific safeguards have been put in place and the procedure referred to in Section 31 has been followed.
 5. The prohibition on processing personal data other than referred to in Section 16 does not apply in so far as this is necessary in addition to the processing of data relating to criminal law matters for the purposes for which such data are processed.
 6. The prohibition does not apply to the processing of personal data relating to criminal law matters by and on behalf of alliances of controllers or groups of controllers governed by public law if the processing is necessary to enable such controllers or groups of controllers to perform their functions and safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised.
 7. Subsections 2 to 6 apply equally to personal data relating to a prohibition imposed by the courts for unlawful or objectionable conduct.
 8. Rules may be issued regarding the appropriate and specific safeguards referred to in subsection 4 (c), by order in council.

Section 23

**General exceptions
from the prohibition
on processing
sensitive personal
data**

1. Without prejudice to Sections 17 to 22, the prohibition on processing personal data referred to in Section 16 does not apply in so far as:
 - a. this is carried out with the data subject's explicit consent;
 - b. the data have manifestly been made public by the data subject;
 - c. this is necessary for the establishment, exercise or defence of legal claims;
 - d. this is necessary to protect the vital interests of the data subject or of a third party and it proves impossible to request his explicit consent;
 - e. this is necessary to comply with an obligation under international public law, or

- f. this is necessary for reasons of a compelling public interest, appropriate safeguards have been put in place to protect privacy, and it is provided for by law or the Authority has granted an exemption. The Authority may impose limitations and regulations when granting such an exemption;
 - g. the data are processed by the Authority or an ombudsman as referred to in Section 9:17 of the General Administrative Law Act and this is necessary, for reasons of a compelling public interest, for the performance of the functions entrusted to them by law, and safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised.
2. The prohibition on processing personal data referred to in Section 16 for scientific research or statistics does not apply in so far as:
 - a. the research serves a public interest;
 - b. the processing is necessary for the research or statistics concerned;
 - c. it proves impossible or would involve a disproportionate effort to request express consent, and
 - d. safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised.
 3. The processing referred to in subsection 1 (f) will be notified to the European Commission. The Minister concerned will send this notification if such processing is provided for by law. The Authority will send the notification if it has granted an exemption for such processing.

Section 24

1. A number prescribed by law for the identification of a person may only be used when processing personal data in order to comply with the law concerned or for purposes provided for by law.
2. Cases other than those referred to in subsection 1 may be designated by order in council in which a number, to be designated as referred to in subsection 1, may be used. Further rules may be issued about the use of such number.

**Processing of
citizen service
number and other
identification
numbers**

Part 3

Codes of conduct

Section 25

1. Any organisation(s) that intend(s) to adopt a code of conduct may request the Authority to declare that the rules included in it correctly elaborate this Act or other laws relating to the processing of personal data, taking account of the specific features of the sector or sectors of society in which that/those organisation(s) operate(s). If a code of conduct provides for the resolution of

**Declaration by the
Authority**

disputes about compliance with it, the Authority may issue such a declaration only if safeguards about its independence have been provided.

2. Subsection 1 applies equally to amendments or extensions to existing codes of conduct.

3. The Authority will deal with the request only if it considers that the party/parties making the request is/are sufficiently representative and the sector or sectors concerned is/are described sufficiently accurately in the code.

4. A decision on a request as referred to in subsection 1 is regarded as a decision within the meaning of the General Administrative Law Act. Division 3.4 of that Act applies to its preparation.

5. The declaration remains valid for the term of validity of the code of conduct, but for no longer than five years after the publication date of the declaration. If the declaration is requested for an amendment to a code of conduct for which a declaration was previously issued, then it will remain valid for the term of that previous declaration.

6. The Authority is responsible for publishing the declaration, together with the code of conduct to which it relates, in the Government Gazette.

Section 26

**Sector specific
rules by order in
council**

1. Further rules may be issued by order in council for a particular sector regarding the matters governed by Sections 6 to 11 and 13.

2. The Authority states in its annual report the extent to which it considers that subsection 1 should be applied.

Part 4

Notification and prior checking

§ 1. Notification

Section 27

**Notification
obligation regarding
data processing and
prior checking**

1. The processing of personal data wholly or partly by automatic means, which is intended to serve a single purpose or several related purposes, will be notified.

2. The processing of personal data by non-automatic means, which is intended to serve a single purpose or several related purposes, will be notified if this is subject to prior checking.

3. The controller will notify the processing to the Authority or the official before commencing with the data processing.

Section 28

1. The notification will include the following:
 - a. the name and address of the controller;
 - b. the purpose(s) of the processing;
 - c. a description of the category or categories of data subjects and of the data or categories of data relating to them;
 - d. the recipients or categories of recipients to whom the data might be disclosed;
 - e. any proposed transfers of data to countries outside the European Union;
 - f. a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Sections 13 and 14 to ensure the security of the processing.
2. The notification will include the purpose(s) for which the category or categories of data are or will be collected.
3. A change to the name or the address of the controller will be notified within one week. Any changes to the notification concerning subsection 1 (b) to (f) will be notified within one year of the previous notification in so far as they are more than incidental in nature.
4. Data processing which differs from what has been notified in accordance with subsection 1 (b) to (f) will be recorded and stored for at least three years.
5. Further rules may be issued by or pursuant to an order in council regarding the manner in which the notification should be made.

**Contents of the
notification**

Section 29

1. It may be determined by order in council that certain data processing unlikely to affect the fundamental rights and freedoms of the data subject is exempt from the notification referred to in Section 27.
2. In such cases the following will be specified:
 - a. the purposes of the processing;
 - b. the data or categories of data undergoing processing;
 - c. the categories of data subjects;
 - d. the recipients or categories of recipients to whom the data are to be disclosed, and
 - e. the length of time the data are to be stored.
3. It may be determined by order in council, if necessary for the purposes of investigating criminal offences in a particular case, that certain data processing by controllers who are responsible pursuant to the law for carrying out investigations is exempt from the notification. In such cases compensatory safeguards may be put in place to protect personal data. The processed data may be used only for the purposes expressly stated in the said order in council.
4. The obligation to notify does not apply to public registers established by law or to disclosures to an administrative body pursuant to a legal obligation.

**Exemptions from
notification
obligation**

Section 30

Public register of data processing

1. Both the Authority and the official will keep a register of the data processing notified to them. The register will contain at least the information listed in Section 28 (1) (a) to (e).
2. The register may be inspected by any person free of charge.
3. The controller will make the information referred to in Section 28 (1) (a) to (e) regarding the data processing that is exempt from notification available to any person on request.
4. Subsection 3 does not apply to:
 - a. data processing that is exempt from notification pursuant to Section 29 (3), or
 - b. public registers which have been established by law.

§ 2. Prior checking

Section 31

Prior checking by the Authority

1. Prior to data processing the Authority will carry out a check if the controller:
 - a. intends to process a number that identifies persons for a purpose other than for which that number was specifically intended, in order to link data to data being processed by another controller, unless the number is being used for the cases described in Section 24;
 - b. intends to record data based on the targeted collection of information by carrying out his own investigation without informing the data subject of this, or
 - c. intends to process data relating to criminal law matters or to unlawful or objectionable conduct, on behalf of third parties, other than in the cases referred to in Section 22 (4) (a) and (b).
2. Subsection 1 (b) does not apply to public registers which have been established by law.
3. Subsection 1 (c) does not apply to data processing that has already been submitted for prior checking by another controller and for which the Authority has issued a declaration as referred to in Section 32 (5).
4. Other data processing that poses a specific risk to the personal rights and freedoms of the data subject, to which subsection 1 applies, may be designated by law or order in council. In its annual report the Authority will indicate the extent to which it considers that such a designation is desirable.
5. The Authority will notify data processing as referred to in subsection 1 (c) to the European Commission.

Section 32

1. Data processing to which Section 31 (1) applies will be notified as such by the controller to the Authority.
2. Notification of such data processing obliges the controller to suspend the processing he intends to carry out until the Authority has completed its check or he has received a message that no further check will be carried out.
3. Where notification is made of data processing to which Section 31 (1) applies, the Authority will issue a decision in writing within four weeks of the notification about whether a further check will be carried out.
4. In the decision to carry out a further check, the Authority will indicate the period within which it intends to carry out this check. This period will not exceed twenty weeks.
5. The further check referred to in subsection 4 will result in a declaration regarding the lawfulness of the data processing.
6. The Authority's declaration is regarded as a decision within the meaning of the General Administrative Law Act. Division 3.4 of that Act applies to its preparation.

Notification obligation regarding data processing subject to prior checking

Part 5

Information to be given to the data subject and the obligation to notify breaches of security of personal data to the Authority

Section 33

1. If personal data are to be collected from the data subject, the controller will, before the time of collection, provide the data subject with the information referred to in subsections 2 and 3, except where he already has it.
2. The controller will disclose his identity and the purposes of the processing for which the data are intended to the data subject.
3. The controller will provide further information in so far as such information is necessary, having regard to the nature of the data, the circumstances in which they are collected or the use that is made of them, to guarantee proper and careful processing in respect of the data subject.

Information obligation to data subject regarding data collection from data subject

Section 34

1. If personal data are collected differently from the manner referred to in Section 33, the controller will provide the data subject with the information referred to in the subsections 2 and 3, except where he already has it:
 - a. at the time of recording the data relating to him, or
 - b. if disclosure of the data to a third party is envisaged, no later than when the data are first disclosed.

Information obligation to data subject regarding different collecting

2. The controller will disclose his identity and the purposes of the processing to the data subject.
3. The controller will provide further information in so far as such information is necessary, having regard to the nature of the data, the circumstances in which they are collected or the use that is made of them, to guarantee proper and careful processing in respect of the data subject.
4. Subsection 1 does not apply if it proves impossible or would involve a disproportionate effort to disclose the information to the data subject. In that case the controller will record the source of the data.
5. Nor does subsection 1 apply if the recording or the disclosure is prescribed by or pursuant to the law. In that case the controller must inform the data subject, at his request, about the legal rule that resulted in the recording or disclosure of the data relating to him.

Section 34a

**Data breach
notification
obligation**

1. The controller will, without delay, notify the Authority of a breach of security, referred to in Section 13, which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data.
2. The controller referred to in subsection 1 will, without delay, notify the data subject of the breach, referred to in subsection 1, if this breach is likely to have unfavourable consequences for his privacy.
3. The notification to the Authority and the data subject will in any case include the nature of the breach, the bodies where more information about the breach can be obtained, and the measures recommended to limit the negative consequences of the breach.
4. The notification to the Authority will also include a description of the observed and probable consequences of the breach for the processing of personal data and the measures that the controller has taken or is proposing to take to remedy these consequences.
5. The notification to the data subject will be made in such a way that, having regard to the nature of the breach, the observed and actual consequences of it for the processing of personal data, the data subjects involved and the costs of enforcement, a proper and careful provision of the information is guaranteed.
6. Subsection 2 does not apply where the controller has taken appropriate technical protective measures that render the personal data concerned incomprehensible or inaccessible to any person who does not have a right of access to the data.
7. If the controller does not notify the data subject, then the Authority may require the controller to notify him, if it considers that the breach is likely to have unfavourable consequences for the data subject's privacy.

8. The controller keeps a record of every infringement which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data. The record will in any case include facts and data regarding the nature of the breach, referred to in subsection 3, as well as the text of the notification to the data subject.
9. This section does not apply where the controller, in his capacity as a provider of a publicly available electronic communications service, has made a notification as referred to in Section 11.3a (1) and (2) of the Telecommunications Act.
10. Subsections 2 and 7 do not apply to financial enterprises within the meaning of the Financial Supervision Act.
11. Further rules may be issued regarding the notification by order in council.

Part 6

The data subject's rights

Section 35

1. The data subject may request the controller without constraint and at reasonable intervals to notify him about whether personal data relating to him are being processed. The controller will notify the data subject about whether or not his personal data are being processed in writing within four weeks.
2. Where such data are being processed, the notification will contain a full summary thereof in an intelligible form, a description of the purpose(s) of the processing, the categories of data concerned and the recipients or categories of recipients, as well as the available information on the source of the data.
3. Before a controller provides the notification referred to in subsection 1, against which a third party is likely to object, he will give that third party the opportunity to express his views where the notification contains data relating to him, unless this proves impossible or involves a disproportionate effort.
4. Upon request, the controller will provide knowledge of the logic involved in any automatic processing of data concerning him.

Right of access

Section 36

1. A person who has been notified of personal data relating to him in accordance with Section 35 may request the controller to correct, supplement, remove or block those data if they are factually incorrect, incomplete or irrelevant in relation to the purpose(s) of the processing or are otherwise being processed in breach of legal rules. The request will contain the changes to be made.
2. The controller will notify the applicant within four weeks of receiving the request in writing whether or to what extent he is complying with the request. A refusal will be reasoned.

Right to correct, supplement and remove

3. The controller will ensure that a decision to correct, supplement, remove or block data is implemented as soon as possible.
4. Where personal data have been recorded on a data carrier to which changes cannot be made, he will take the measures necessary to inform the user of the data of the impossibility of correcting, supplementing, removing or blocking data despite the fact that there are grounds to amend the data on the basis of this section.
5. The provisions of subsections 1 and 4 do not apply to public registers which have been established by law, where such law provides for a special procedure to correct, supplement, remove or block data.

Section 37

**Non-written
notification,
identification of
applicant and
request of legal
representative**

1. Where a compelling interest of the applicant so requires, the controller will comply with a request referred to in Sections 35 and 36, in a form other than in writing which has been brought into conformity with that interest.
2. The controller will ensure that the identity of the applicant is properly established.
3. Requests referred to in Sections 35 and 36, which are made in respect of minors who have not yet reached the age of 16, and in respect of those who have been placed under guardianship, will be made by their legal representatives. The notification concerned will also be made to the legal representatives.

Section 38

**Obligation to notify
third parties of
corrections**

1. The controller who has corrected, supplemented, removed or blocked personal data as a result of a request made pursuant to Section 36 must promptly notify third parties to whom the data have already been disclosed of the correction, supplement, removal or blocking, unless this proves impossible or involves a disproportionate effort.
2. The controller will, at the request of the applicant referred to in Section 36, state which parties he has so notified.

Section 39

**Payment for right
of access**

1. The controller may require payment of the costs incurred in providing the information referred to in Section 35, the amount of which will be laid down by or pursuant to an order in council and may not exceed € 5.
2. The costs will be reimbursed where the controller has corrected, supplemented, removed or blocked data at the request of the data subject, on the recommendation of the Authority or by order of the court.
3. The amount referred to in subsection 1 may in special cases be amended by order in council.

Section 40

1. The data subject may at any time object to the controller where data are being processed pursuant to Section 8 (e) and (f) on grounds relating to his particular circumstances.
2. The controller will assess whether the objection is justified within four weeks of receiving the objection. If the objection is justified, he will immediately cease processing the data concerned.
3. The controller may require payment of the costs incurred in dealing with an objection, which may not exceed an amount to be laid down by or pursuant to an order in council. The costs will be reimbursed where the objection is allowed.
4. This section does not apply to public registers which have been established by law.

Right to object

Section 41

1. Where data are processed in connection with the creation or maintenance of a direct relationship between the controller or a third party and the data subject with a view to canvassing for commercial or charitable purposes, the data subject may at all times file an objection with the controller against this and at no cost.
2. If an objection is filed, the controller will take measures to immediately terminate this form of processing. At the request of the data subject, the controller will, within four weeks, notify the former of the measures that have been taken. If the notification cannot be issued within four weeks, the controller will inform the data subject within four weeks of the date of receipt of the request within which time limit the notification can be issued.
3. The controller who processes those personal data for the purposes referred to in subsection 1 will take suitable measures to notify the data subjects of the possibilities available to them to object to this form of processing.
4. The controller who processes personal data for the purposes referred to in subsection 1 ensures that any message sent directly to the data subject for that purpose will contain a reference to the possibility of objecting to this form of processing.

Right to object with regard to commercial or charitable purposes

Section 42

1. No-one may be subjected to a decision which produces legal effects concerning him or which significantly affects him where such decision is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him.

Automated decision on the basis of a personal profile

2. Subsection 1 does not apply if the decision:
 - a. is taken in the course of the entering into or performance of a contract and
 - 1°. provided the request lodged by the data subject has been satisfied, or
 - 2°. suitable measures have been taken to safeguard his legitimate interests, or
 - b. is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.
3. A suitable measure referred to in subsection 2 (a) is taken if arrangements are made allowing the data subject to put forward his point of view about the decision referred to in subsection 1.
4. In the case referred to in subsection 2, the controller will notify the data subject of the logic involved in any automated processing of personal data concerning him.

Part 7

Exceptions and restrictions

Section 43

- Exceptions** The controller may refrain from applying Sections 9 (1), 30 (3), 33, 34, 34a (2) and 35 where necessary in the interests of:
- a. national security;
 - b. the prevention, investigation and prosecution of criminal offences;
 - c. important economic or financial interests of the state and other public bodies;
 - d. supervision of compliance with legal rules established for the interests referred to in (b) and (c), or
 - e. the protection of the data subject or of the rights and freedoms of others.

Section 44

- Processing for scientific research, statistics or archived records**
1. Where processing is carried out by institutions or services for purposes of scientific research or statistics, and the necessary steps have been taken to ensure that the personal data can be used solely for statistical and scientific purposes, the controller does not have to issue the notification referred to in Section 34 and may refuse to grant a request as referred to in Section 35.
 2. The controller does not have to issue the notification referred to in Section 34 where processing of personal data, that form part of archived records that are transferred to a repository pursuant to Section 12 or Section 13 of the Public Records Act 1995, takes place.

Part 8

Legal protection

Section 45

A decision on a request as referred to in Sections 30 (3), 35, 36 and 38 (2) as well as a decision taken on an objection as referred to in Sections 40 or 41 are regarded as an order within the meaning of the General Administrative Law Act in so far as they are taken by an administrative body.

**General
Administrative Law
Act order**

Section 46

1. Where a decision as referred to in Section 45 is taken by a body other than an administrative body, the interested party may file a written application with the court to order the controller to grant or refuse a request as referred to in Sections 30 (3), 35, 36 or 38 (2) or to allow or reject an objection as referred to in Sections 40 or 41.
2. The application must be filed within six weeks of receipt of the controller's answer. If the controller has not answered within the stipulated time limit, the application must be filed within six weeks from that time limit.
3. The court will grant the request in so far as it deems it well-founded. Before the court takes a decision, it will, where necessary, give the interested parties the opportunity to put their points of view forward.
4. The application does not have to be filed by a lawyer.
5. Division 3 of Title 5 of Book 2 of the Code of Civil Procedure applies equally.
6. The court may request parties and others to submit written information and documents they hold within a time limit set by the court. The controller and the interested party must comply with this request. Section 8:45 (2) and (3) and Section 8:29 of the General Administrative Law Act apply equally.

**Application
proceedings**

Section 47

1. The interested party may also file a request with the Authority, within the time limit stipulated for the appeal under the General Administrative Law Act, to mediate in or advise on his dispute with the controller or to use a dispute resolution scheme under a code of conduct which has already been issued with a declaration as referred to in Section 25 (1). In that case, by way of derogation from Section 6:7 of the General Administrative Law Act, the appeal may still be filed or proceedings as referred to in Section 46 may still be issued after the interested party has received a notification from the Authority or pursuant to a dispute resolution scheme under a code of conduct which has already been issued with a declaration as referred to in Section 25 (1), that the case has been closed, but not more than six weeks after such date.

**Mediation, advice or
dispute resolution
by the Authority**

2. During the appeal hearing and the proceedings, referred to in subsection 1, the bodies charged with resolving the dispute may request the Authority to give an opinion.

Section 48

Copy of decision to the Authority The bodies charged with resolving the dispute will send a copy of their decision to the Authority.

Section 49

- Liability and damages**
1. If anyone suffers damage as a result of acts concerning him which infringe the rules by or pursuant to this Act, the following subsections apply, without prejudice to the entitlements on the grounds of other legal rules.
 2. For any non-economic damage, the injured party is entitled to damages that will be determined in all fairness.
 3. The controller is liable for any loss or damage resulting from non-compliance with the rules referred to in subsection 1. The processor is liable for such loss or damage in so far as it results from his activity.
 4. The controller or the processor may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the damage.

Section 50

- Court order of remedial measures**
1. If the controller or the processor acts in breach of provisions laid down by or pursuant to this Act and another party suffers damage or is at risk of suffering damage as a result, the court may prohibit such conduct at the request of that other party and order the controller to take measures to remedy the consequences of that conduct.
 2. A request by a legal person as referred to in Section 1:2 (3) of the General Administrative Law Act or Article 3:305a of the Civil Code may not be based on data processing, in so far as the person affected by this processing objects to it.

Part 9 Supervision

§ 1. *The Dutch Data Protection Authority*

Section 51

- Dutch Data Protection Authority**
1. The Dutch Data Protection Authority is charged with the supervision of the processing of personal data in accordance with the provisions laid down by and pursuant to the law. The Authority also monitors the processing of personal data in the Netherlands when personal data are processed in accordance with the law of another Member State of the European Union.

2. The Authority is requested to give an opinion on bills and draft orders in council that relate wholly or to a large extent to the processing of personal data.
3. The Framework Act applies to the Authority, save for the exceptions set out in this Act.
4. The Authority is generally referred to as the “Personal Data Authority” in society.

Section 51a

1. The Authority may make arrangements with other supervisory authorities in the interest of efficient and effective supervision of the processing of personal data and draw up cooperation protocols with these supervisory authorities for that purpose. Any cooperation protocol is to be published in the Government Gazette.
2. The Authority and the supervisory authorities, referred to in subsection 1, may on their own initiative and must on request disclose to one another the data relating to the processing of personal data that are necessary for the exercise of their functions.

**Cooperation of
supervisory
authorities**

Section 52

1. The Authority exercises the functions entrusted to it by law or treaty.
2. The Authority will act with complete independence in exercising its functions.

**Functions of the
Authority**

Section 53

1. The Authority comprises a chairman and a maximum of two other members. Extraordinary members may also be appointed to the Authority. In the appointment of extraordinary members, all efforts will be made to reflect the diversity of the different sectors of society.
2. The chairman must satisfy the requirements for appointment as a judge to the court by or pursuant to Section 5 of the Judicial Officers (Legal Status) Act.
3. The chairman, the other members and the extraordinary members are appointed by royal decree, on the nomination of the Minister, for a period of five years. They may be reappointed for one more period of five years. They are dismissed by the Minister at their own request. Section 12 of the Framework Act does not apply.
4. An advisory board advises the Authority on general aspects of the protection of personal data. Its members come from different sectors of society and are appointed by the Minister on the nomination of the Authority. The members are appointed for a maximum period of four years. They may be reappointed twice, each time for a maximum period of four years. The

**Organisation of the
Authority**

reimbursement of costs to the members is laid down by or pursuant to an order in council.

Section 54

Mutatis mutandis provision Sections 46c, 46d (2), 46f, 46g, 46i, except for subsection 1 (c), 46j, 46l (1) and (3), 46m, 46n, 46o and 46p of the Judicial Officers (Legal Status) Act apply equally on the understanding that:

- a. the disciplinary measure referred to in Section 46c (1) is imposed on the members of the Authority by the chairman of the Authority;
- b. the prohibition referred to in Section 46c (1) (b) on engaging with parties or their lawyers or representatives in an interview or a meeting and accepting special information or written documents from them does not apply to the members of the Authority.

Section 12 (2) of the Framework Act does not apply.

Section 55

Legal position of the chairman and members The legal position of the chairman, the other members and the extraordinary members is laid down by ministerial regulations.

Section 56

Secretariat of the Authority

1. The Authority has a secretariat whose officials are appointed, suspended and dismissed by the Minister, on the recommendation of the chairman.
2. The chairman directs the activities of the Authority and of the secretariat.
3. The Authority adopts administrative regulations. These contain, in any event, rules on financial management and the administrative organisation, as well as working methods and procedures with a view to the good and careful performance of its various duties. These also provide safeguards against combining the supervisory, advisory and sanctioning duties of the Authority. They may also set out further rules for the advisory board as referred to in Section 53 (4).

Section 57

Representation of the Authority

1. The Authority is represented by the chairman and the other members, or by one of them.
2. The members set out the division of duties and thereby involve the extraordinary members in so far as possible.

Section 58

Annual report of the Authority The annual report referred to in Section 18 of the Framework Act will be forwarded to the data protection officials referred to in Section 62 and made generally available.

Section 59

Section 20 of the Framework Act does not apply if the Authority has collected the information from third parties on condition that its confidential nature be maintained.

Exception to the Authority's obligation to provide information

Section 59a

1. Sections 21 and 22 of the Framework Act do not apply to the Authority.
2. Section 23 of the Framework Act only applies to the financial management and administrative organisation of the Authority.

Limitations to the Minister's powers

Section 60

1. The Authority may, on its own initiative or at the request of an interested party, conduct an audit of the manner in which provisions established by or pursuant to the law are implemented in respect of data processing.
2. The Authority will notify the controller or group of controllers involved in the audit of its preliminary findings and allow them to put their point of view forward. If these preliminary findings relate to the implementation of any law, the Authority will also notify the Minister concerned.
3. Where an audit has been initiated at the request of an interested party, the Authority will notify that party of its findings, unless such notification is incompatible with the purposes of the data processing or the nature of the personal data, or compelling interests of parties other than the applicant, including the controller, would be harmed disproportionately as a result. If the Authority fails to notify its findings to the interested party, it will send him such message as it deems appropriate.

Privacy audit

Section 61

1. The members and extraordinary members of the Authority, the officials of the Authority's secretariat as well as the persons designated by order of the Authority are responsible for monitoring compliance as referred to in Section 51.
2. The persons referred to in subsection 1 may enter a dwelling without the permission of the occupant.
3. The persons referred to in subsection 1 require the explicit and special authority of the Authority for the purpose of exercising the power set out in subsection 2, without prejudice to Section 2 of the General Act on Entry into Dwellings.
4. The Authority may impose an administrative enforcement order to enforce Section 5:20 (1) of the General Administrative Law Act in so far as it concerns the obligation to cooperate with an official designated by or pursuant to subsection 1.

Supervision and enforcement by the Authority

5. No obligation of secrecy may be invoked in so far as information or cooperation is requested in connection with the person concerned's own involvement with the processing of personal data.

6. Upon request, the Authority must lend any assistance to the supervisory authorities of other Member States of the European Union in so far as required for the performance of their duties.

§ 2. The data protection official

Section 62

Data protection official A controller or an organisation to which controllers are affiliated may appoint its own data protection official, without prejudice to the powers of the Authority under Parts 9 and 10 of this Act.

Section 63

Requirements for the appointment of a data protection official 1. Only natural persons who, for the performance of their duties, have sufficient knowledge and who may be deemed to be sufficiently reliable may be appointed as a data protection official.

2. The official may not receive instructions regarding the performance of his duties from the controller or from the organisation that has appointed him. He suffers no disadvantage from the performance of his duties. The controller will allow the official to properly perform his duties. The official may request the subdistrict court judge to rule that the controller must comply with the obligation set out in the second sentence of this subsection.

3. The official will only commence his duties after the controller or the organisation that has appointed him has registered him with the Authority. The Authority keeps a list of officials that have been registered.

4. The official must observe the confidentiality of any information that becomes known to him pursuant to a complaint by or request from a data subject, unless the data subject agrees to disclosure.

Section 64

Powers of the data protection official 1. The official will supervise the processing of personal data in accordance with provisions laid down by or pursuant to the law. The supervision extends to the processing of personal data by the controller who has appointed him or by the controllers who are affiliated with the organisation that has appointed him.

2. Where a code of conduct adopted pursuant to Section 25 applies to the processing, the supervision also extends to compliance with this code.

3. The controller or the organisation referred to in subsection 1 will ensure that, in performing his duties, the official has the powers, that are equivalent to the powers laid down in Title 5.2 of the General Administrative Law Act.

4. The official may make recommendations to the controller to improve the protection of the data that are being processed. In cases of doubt he will consult the Authority.

Part 10 Sanctions

§ 1. Administrative enforcement

Section 65

The Authority may impose an administrative enforcement order to enforce obligations laid down by or pursuant to this Act.

**Administrative
enforcement**

§ 2. Administrative penalties

Section 66

1. The Authority may impose an administrative penalty not exceeding the amount of a fine of the fourth category of Article 23 (4) of the Criminal Code for violation of the provisions by or pursuant to Section 4 (3) or Section 78 (2), opening lines and (a).

**Administrative
penalties**

2. The Authority may impose an administrative penalty not exceeding the amount of a fine of the sixth category of Article 23 (4) of the Criminal Code for violation of the provisions by or pursuant to Sections 6 to 8, 9 (1) and (4), 10 (1), 11 to 13, 16, 24, 33, 34 (1), (2) and (3), 34a, 35 (1), second sentence, (2), (3) and (4), 36 (2), (3) and (4), 38 to 40 (2) and (3), 41 (2) and (3), 42 (1) and (4), 76, 77 or 78 (3) and (4), as well as Section 5:20 of the General Administrative Law Act. Article 23(7) of the Criminal Code applies equally.

3. The Authority will only impose an administrative penalty for violation of provisions by or pursuant to the sections referred to in Section 66 (2) after it has issued a binding order. The Authority may set a time limit within which the offender must comply with the order.

4. Subsection 3 does not apply if the violation was deliberate or the result of serious negligence.

5. The Authority may impose an administrative penalty not exceeding the amount of the fine of the sixth category of Article 23 (4) of the Criminal Code for non-compliance with a binding order. Article 23 (7) of the Criminal Code applies equally.

Section 67

Prior to adopting a policy rule regarding the interpretation of the provisions by or pursuant to the sections referred to in Section 66 (2), the Authority will consult the Minister and the Minister of the Interior and Kingdom Relations.

Section 68

[Repealed as of 01-07-2009]

Section 69

[Repealed as of 01-07-2009]

Section 70

[Repealed as of 01-07-2009]

Section 71

Suspensive effect of objection or appeal

The operation of the decision to impose the administrative penalty will be suspended until the period for objecting or appealing has expired or, if an objection has been filed or an appeal has been lodged, a decision has been taken regarding the objection or the appeal.

Section 72

[Repealed as of 01-07-2009]

Section 73

[Repealed as of 01-07-2009]

Section 74

[Repealed as of 01-01-2014]

§ 3. Criminal sanctions**Section 75**

Criminal penalties

1. The controller who acts in violation of the provisions by or pursuant to Section 4 (3) or Section 78 (2) will be punished with a fine of the third category.
2. The controller who deliberately commits a criminal offence referred to in subsection 1 will be punished with imprisonment not exceeding six months or a fine of the fourth category.
3. The criminal offences referred to in subsection 1 are minor offences. The criminal offences referred to in subsection 2 are serious offences.
4. In addition to the officials designated by or pursuant to Article 141 of the Criminal Code, the officials of the Authority's secretariat designated by the

Minister are responsible for the investigation of the criminal offences referred to in this section.

Part 11

Flow of data to countries outside the European Union

Section 76

1. Personal data which are undergoing processing or which are intended for processing after transfer may be transferred to a country outside the European Union only if, without prejudice to compliance with the law, that country ensures an adequate level of protection.
2. By way of derogation from subsection 1, the transfer of personal data which are undergoing processing or are intended for processing after transfer to a country outside the European Union may take place if that country is a party to the Agreement on the European Economic Area signed in Oporto on 2 May 1992 (*Treaty Series* 1992, 132), unless it follows from a decision of the Commission of the European Communities or the Council of the European Union that such transfer is restricted or prohibited.
3. The adequacy of the level of protection will be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration will be given to the nature of the data, the purpose(s) and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question, and the professional rules and security measures which are complied with in that country.

Transfer of personal data to countries outside the EU

Section 77

1. By way of derogation from Section 76 a transfer or set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place if:
 - a. the data subject has given his unambiguous consent to the proposed transfer;
 - b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request and which are necessary for the conclusion of a contract;
 - c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

Exceptions to the prohibition on the transfer to countries outside the EU

- d. the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims;
 - e. the transfer is necessary in order to protect a vital interest of the data subject, or
 - f. the transfer is made from a register established by legal rules and open to consultation either by anyone or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;
 - g. a standard contract is used as referred to in Article 26 (4) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281).
2. By way of derogation from subsection 1, the Minister, having consulted the Authority, may issue a licence for a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection. The licence will be subject to further rules that are necessary to guarantee the protection of privacy and of the fundamental rights and freedoms of individuals and the exercise of the corresponding rights.

Section 78

**Notification to the
European
Commission**

1. The Minister will notify the Commission of the European Communities of:
 - a. the cases in which a third country does not, in his view, ensure an adequate level of protection within the meaning of Section 76 (1), and
 - b. a licence as referred to in Section 77 (2).
2. Where this arises from a decision of the Commission of the European Communities or the Council of the European Union, the Minister of Security and Justice will determine by way of a ministerial regulation or decision that:
 - a. the transfer to a country outside the European Union is prohibited, or
 - b. a licence granted pursuant to Section 77 (2) is to be revoked or modified.
3. The transfer of personal data to a third country, which the Commission of the European Communities or the Council of the European Union has determined ensures an adequate level of protection, may take place without prejudice to the provisions by or pursuant to this Act.
4. By way of derogation from subsection 3, the Minister of Security and Justice, having consulted the Authority, may, by way of a ministerial regulation or decision, suspend the transfer of personal data to a third country which the Commission of the European Communities or the Council of the European Union has determined ensures an adequate level of protection, in order to protect persons involved with the processing of personal data in the cases in which:

- a. a competent authority in the third country has determined that the recipient concerned is in breach of the applicable standards relating to data protection;
 - b. there is a substantial likelihood that the standards for data protection will not be complied with, there are well-founded reasons to assume that the competent authority in the third country will fail to take appropriate measures to resolve the problem in good time, continuing the transfer entails an imminent risk of serious damage to the data subject, and the Authority has used sufficient endeavours to notify the controller based in the third country of its findings and to allow him to respond to those findings.
5. The ministerial regulation or the decision referred to in subsection 4 will remain in force until it is determined that the standards for data processing are being complied with and the Authority has been notified of this by the competent authority concerned in a case as referred to in subsection 4 (a), or the Authority has determined this in a case as referred to in subsection 4 (b). The Authority will notify the Minister of Security and Justice of its findings.
6. The notifications referred to in subsection 1 (a) and (b) are published in the Government Gazette.

Part 12

Transitional and final provisions

Section 79

1. Within one year of the entry into force of this Act, the data processing that was already taking place on that date will be brought into conformity with this Act and notified to the Authority or the official. The time limit referred to in the first sentence may be extended to a maximum of three years by way of an order in council as regards the notification obligation. **Transitional regime**
2. A time limit of three years applies to the adjustment of the processing of special data to Division 2 of Part 2, on the understanding that no renewed consent as referred to in Section 23 (1) (a) needs to be requested for the processing that was already taking place and that is necessary for the performance of contracts that were concluded before the entry into force of this Act.
3. Section 32 (2) does not apply to the processing referred to in Section 31 (1) and (3) that was already taking place on the date of the entry into force of this Act or of the Act or the order in council which applied to that processing.

Section 80

Evaluation regime The Minister of Security and Justice and the Minister of the Interior and Kingdom Relations will send a report on the actual effectiveness and effects of this Act to the States General within five years of the entry into force of this Act.

Section 81

**Repeal of the
Registration of
Personal Data Act** The Registration of Personal Data Act is repealed.

Section 82

Entry into force This Act will enter into force on a date to be determined by royal decree.

Section 83

Short title This Act may be cited as the “Personal Data Protection Act”.

Mandate and order that this will be published in the Bulletin of Acts and Decrees and that all ministerial departments, authorities, councils and government officials concerned will ensure its precise implementation.

Done in The Hague, 6 July 2000

Beatrix

The Minister of Justice,
A. H. Korthals

The Minister of Urban Policy and Integration of Ethnic Minorities
R. H. L. M. van Boxtel

Issued on the twentieth of July 2000

The Minister of Justice,
A.H. Korthals

© 2016 deLex / AKD N.V. / E.F. Vaal / Hendriks & James Legal Translations

This publication has been sponsored by:

AKD
+31 88 253 5000
info@akd.nl
www.akd.nl

Hendriks & James Legal Translations
Korte Leidsedwardsstraat 12
1017 RC Amsterdam
+31 20 421 8519
info@hendriks-james.nl
www.hendriks-james.nl