51 (1981) Nr. 2

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 1993 Nr. 116

A. TITEL

Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens; Straatsburg, 28 januari 1981

B. TEKST

De tekst van het Verdrag is geplaatst in *Trb.* 1988, 7.
Het Verdrag is voorts nog ondertekend voor:

Finland	10 april 1991
Hongarije	13 mei 1993

C. VERTALING

Zie *Trb.* 1988, 7.

D. PARLEMENT

De artikelen 1 en 2 van de wet van 20 juni 1990 (*Stb.* 351) luiden als volgt:

„Artikel 1

Het op 28 januari 1981 te Straatsburg tot stand gekomen Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, waarvan de Engelse en Franse tekst alsmede de vertaling in het Nederlands zijn geplaatst in het Tractatenblad 1988, nr. 7, wordt goedgekeurd voor Nederland.

Artikel 2

1. Bij de aanvaarding wordt een verklaring afgelegd in de zin van artikel 3, tweede lid, onderdelen b en c, van het in artikel 1 bedoelde

Verdrag waarin worden opgesomd de categorieën persoonsregistraties bedoeld in artikel 2, eerste, tweede en derde lid, onderdeel b, van de Wet persoonsregistraties (*Stb.* 1988, 665), onderscheidenlijk de persoonsregistraties aangewezen ingevolge artikel 54, vierde lid, van die wet.

2. De regering wordt gemachtigd de verklaring bedoeld in het voorgaande lid te wijzigen indien met betrekking tot een of meer van de daarin opgenomen categorieën persoonsregistraties bij of krachtens wet regels worden gesteld ter bescherming van de persoonlijke levenssfeer in verband met de geautomatiseerde verwerking van persoonsgegevens.".

Deze wet is gecontrasigneerd door de Minister van Justitie E. M. H. HIRSCH BALLIN, de Minister van Binnenlandse Zaken C. I. DALES en de Minister van Buitenlandse Zaken H. VAN DEN BROEK.

Voor de behandeling in de Staten-Generaal zie: Kamerstukken II 1988/89, 1989/90, 21 093; Handelingen II 1989/90, blz. 3556-3559; Kamerstukken I 1989/90, nrs. 201, 201a; Handelingen I 1989/90, zie vergadering dd. 19 juni 1990.

E. BEKRACHTIGING

Behalve de in *Trb.* 1988, 7[1]) genoemde hebben nog de volgende Staten in overeenstemming met artikel 22, eerste lid, van het Verdrag een akte van bekrachtiging, aanvaarding of goedkeuring bij de Secretaris-Generaal van de Raad van Europa nedergelegd:

Luxemburg[2])	10 februari 1988
Oostenrijk[3])	30 maart 1988
Denemarken[4])	23 oktober 1989
Ierland[5])	25 april 1990
IJsland	25 maart 1991
Finland[6])	2 december 1991
België[7])	28 mei 1993
het *Koninkrijk der Nederlanden*[8]) (voor Nederland)	24 augustus 1993

[1]) De Regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland heeft de volgende bevoegde autoriteit aangewezen (doorgegeven door de depositaris op 17 maart 1988):
"The Data Protection Registrar
Springfield House
Water Lane
Wilmslow
CHESHIRE SK9 5AX".

[2]) Onder de volgende verklaringen:
"Article 3, paragraphe 2, alinéa (a)
Le Grand Duché de Luxembourg déclare qu'il se réserve le droit, dans les limites de l'article 3(2)a) de la Convention, de ne pas appliquer la Convention:
a) aux banques de données qui en vertu d'une loi ou d'un règlement sont accessibles au public;
b) à celles qui contiennent exclusivement des données en rapport avec le propriétaire de la banque;
c) à celles qui sont établies pour le compte des institutions de droit international public.
Article 13, paragraphe 2, alinéa (a)
Le Grand-Duché de Luxembourg désigne comme autorité compétente pour accorder l'assistance pour la mise en œuvre de cette Convention: la Commission consultative instituée par la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques
c/o Ministère de la Justice,
L-2910 LUXEMBOURG.».

[3]) Onder de volgende interpretatieve verklaringen:
Article 2(c)
The Republic of Austria takes the assumption that the term "dissemination" covers the terms "communication" and "making available" used in section 3 paragraphs 9 and 10 of the amendment to the Austrian Data Protection Act, Federal Law Gazette No. 370/1986.
Article 5(e)
The Republic of Austria takes the assumption that this requirement is fully met by the stipulation of the Austrian Data Protection Act concerning the deletion of data upon application by the data subject.
Article 9(2)
The Republic of Austria takes the assumption that the contents of the phrase "provided for by the law of the Party" contained in the introductory sentence of Article 9(2) of the Convention conforms to the contents of the phrase "in accordance with the law" contained in Article 8(2) of the European Convention on Human Rights, and that it is therefore in agreement with the Convention if under the Austrian basic right to data protection it is admissible to restrict such basic right only if provided for by the law.
Furthermore, the Republic of Austria takes the assumption that, in its scope, the restriction in the interest of the "monetary interests of the State" as provided for in Article 9(2)a of the Convention in conjunction with the restriction under paragraph 2(b) corresponds to the restriction in the interest of the "economic well-being of the country" contained in Article 8(2) of the European Convention on Human Rights.
en de volgende verklaringen:
1. In compliance with Article 13(2) it is hereby notified that the authority responsible for rendering assistance in the implementation of this Convention shall be:
Bundeskanzleramt
Ballhausplatz 2,
A-1014 VIENNA
2. In accordance with Article 3(2)b it is hereby notified that Austria will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations or any other bodies consisting directly or indirectly of individuals whether or not such bodies possess legal

personality (legal persons or associations of persons within the meaning of section 3(2), Data Protection Act).".

[4]) Onder de volgende verklaring en aanwijzing:
"Article 24, paragraph 1
The Convention shall not apply to the Faroe Islands and Greenland.
Article 13, paragraph 2a):
The Danish authority designated shall be:
Data Surveillance Authority (D.S.A.)
(Registertilsynet)
Christians Brygge 28, 4
DK-1559 COPENHAGEN V
Tel: 31 14 38 44".

[5]) Onder de volgende verklaring en aanwijzing:
"The Government of Ireland wish to make a declaration in accordance with Article 3(2)(a) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data to the effect that the Convention will not apply to the following categories of automated personal data files, which are set out at Section 1(4) of the Data Protection Act 1988, to wit:
a. personal data that in the opinion of the Minister for Justice or the Minister for Defence are, or at any time, were, kept for the purpose of safeguarding the security of the State;
b. personal data consisting of information that the person keeping the data is required by law to make available to the public;
c. personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes.
In accordance with Article 13(2)(a) of the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data, I have the honour to inform you that the designated authority, in respect of Ireland, is:
Mr Dónal Linehan
Data Protectioin Commissioner
Earl Court
Adelaine Road
Dublin 2
Ireland".

[6]) De Regering van Finland heeft in overeenstemming met artikel 13 als bevoegde autoriteit aangewezen:
„Data Protection Ombudsman
Kauppakartanonkatu 7 A 41
P.O. Box 31
00931 HELSINKI
FINLAND"

[7]) Onder de volgende verklaringen:
«Conformément à l'article 3, paragraphe 2, a, de la Convention, la Belgique n'appliquera pas la Convention:
– aux traitements de données à caractère personnel gérés par des personnes physiques qui, de par leur nature, sont destinés à un usage privé, familial ou domestique et conservent cette destination;
– aux traitements portant exclusivement sur des données à caractère personnel qui font l'objet d'une publicité en vertu d'une disposition légale ou réglementaire;

– aux traitements portant exclusivement sur des données à caractère personnel dont la personne à laquelle elles se rapportent assure ou fait assurer la publicité, pour autant que le traitement respecte la finalité de cette publicité.

Conformément à l'article 3, paragraphe 2, c, de la Convention, la Belgique appliquera également la Convention aux fichiers de données à caractère personnel tenus sur des supports non-automatisés.

Article 13 de la Convention:

L'autorité désignée pour fournir les informations visées à l'article 13, paragraphe 3, a, est le

Ministère de la Justice
Administration des Affaires civiles et criminelles
Place Poelaert, 3
1000 BRUXELLES

L'autorité compétente pour fournir les informations visées à l'article 13, paragraphe 3, b, est la

Commission de la protection de la vie privée
Place Poelaert, 3
1000 BRUXELLES

Article 14 de la Convention:

L'autorité désignée est la

Commission de la protection de la vie privée
Place Poelaert, 3
1000 BRUXELLES"

[8]) Onder de volgende verklaringen:

"In accordance with article 24, first paragraph, the Convention shall apply to the Kingdom in Europe.

Pursuant to article 3, second paragraph, under a, of the Convention, the Kingdom of the Netherlands (for the Kingdom in Europe) declares that:

I. the Convention shall not apply to the following personal data files:

– personal data files which are by their nature intended for personal or domestic use;

– personal data files kept exclusively for public information purposes by the press, radio or television;

– books and other written publications, or index systems pertaining to them;

– personal data files kept in archives repositories designated for that purpose by law;

– personal data files which are established and to which public access is required by law;

– personal data files kept for the purpose of implementing the Elections Act ('Kieswet');

II. the Convention shall as yet not apply to the following personal data files:

– personal data files established under or pursuant to the Criminal Records and Certificates of Good Behaviour Act ('Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag');

– personal data files established pursuant to the Population and Residence Registers Act ('Wet bevolkings- en verblijfsregisters');

– the central register of students in higher education, established under the University Education Act, the Higher Vocational Education Act and the Open University Act ('Wet op het wetenschappelijk onderwijs, Wet op het hoger beroepsonderwijs, Wet op de open universiteit'); and

– files of registered vehicle registration marks and of issued driving licences, established pursuant to the Road Traffic Act ('Wegenverkeerswet').

In accordance with article 13, second paragraph, under a, of the Convention the authority designated by the Kingdom of the Netherlands (for the Kingdom in Europe) is:

Registratiekamer
Postbus 3011
NL-2280 GA RIJSWIJK
The Netherlands
tel.: +(70) 319 01 90
fax.: +(70) 394 04 60"

G. INWERKINGTREDING

Zie *Trb.* 1988, 7.

Wat het *Koninkrijk der Nederlanden* betreft, zal het Verdrag ingevolge artikel 22, derde lid, op 1 november 1993 in werking treden voor Nederland.

H. TOEPASSELIJKVERKLARING

In overeenstemming met artikel 24, tweede lid, is het Verdrag van toepassing verklaard door:

het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland op

het eiland Man[1]) . . . . . 21 januari 1993

[1]) Onder de volgende verklaringen:

"In accordance with Article 3, paragraph 2, sub-paragraph (a) of the Convention, I declare that the Convention will not be applied to personal data files held only for distributing or supplying or recording the distribution or supply of articles, information or services to the data subjects.

In accordance with Article 13, paragraph 2, sub-paragraph (a) I would like to designate the Isle of Man Data Protection Register, Willow House, Main Road, Onchan, Isle of Man as the competent authority to render assistance in the Isle of Man in order to implement this Convention.".

J. GEGEVENS

Zie *Trb.* 1988, 7.

Voor het op 5 mei 1949 te Londen tot stand gekomen Statuut van de Raad van Europa zie ook, laatstelijk, *Trb.* 1992, 111.

Op 17 september 1987 heeft het Comité van Ministers van de Lidstaten Aanbeveling R(87)15 aangenomen. De Engelse tekst van die Aanbeveling luidt als volgt:

Recommendation No. R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector[1])

(Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Aware of the increasing use of automatically processed personal data in the police sector and of the possible benefits obtained through the use of computers and other technical means in this field;

Taking account also of concern about the possible threat to the privacy of the individual arising through the misuse of automated processing methods;

Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other;

Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in particular the derogations permitted under Article 9;

Aware also of the provisions of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms,

Recommends the governments of member states to:
- be guided in their domestic law and practice by the principles appended to this recommendation, and
- ensure publicity for the provisions appended to this recommen-

[1]) When this recommendation was adopted:
- in accordance with Article 10.2.c of the Rules of Procedure for the meetings of the Ministers' Deputies, the Representative of Ireland reserved the right of his Government to comply with it or not, the Representative of the United Kingdom reserved the right of her Government to comply or not with Principles 2.2 and 2.4 of the recommendation, and the Representative of the Federal Republic of Germany reserved the right of his Government to comply or not with Principle 2.1 of the recommendation:
- in accordance with Article 10.2.d of the said Rules of Procedure, the Representative of Switzerland abstained, stating that he reserved the right of his Government to comply with it or not and underlining that his abstention should not be interpreted as expressing disapproval of the recommendation as a whole.

dation and in particular for the rights which its application confers on individuals.

Appendix to Recommendation No. R(87)15

Scope and definitions

The principles contained in this recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing.

For the purposes of this recommendation, the expression "personal data"covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.

The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

The expression "responsible body" (controller of the file) denotes the authority, service or any other public body which is competent according to national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them.

A member state may extend the principles contained in this recommendation to personal data not undergoing automatic processing.

Manual processing of data should not take place if the aim is to avoid the provisions of this recommendation.

A member state may extend the principles contained in this recommendation to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.

The provisions of this recommendation should not be interpreted as limiting or otherwise affecting the possibility for a member state to extend, where appropriate, certain of these principles to the collection, storage and use of personal data for purposes of state security.

Basic principles

Principle 1 – Control and notification

1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this recommendation.

1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.

1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this recommendation.

1.4. Permanent automated files should be notified to the supervisory authority. The notification should specify the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.

Ad hoc files which have been set up at the time of particular inquiries should also be notified to the supervisory authority either in accordance with the conditions settled with the latter, taking account of the specific nature of these files, or in accordance with national legislation.

Principle 2 – Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.

2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.

2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

Principle 3 – Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within

the framework of national law and their obligations arising from international law.

3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.

3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.

Principle 4 – Use of data by the police

4. Subject to Principle 5, personal data collected and stored by the police for police purposes should be used exclusively for those purposes.

Principle 5 – Communication of data

5.1. *Communication within the police sector*
The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

5.2.i. *Communication to other public bodies*
Communication of data to other public bodies should only be permissible if, in a particular case:
a) there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if
b) these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:
a) the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if
b) the communication is necessary so as to prevent a serious and imminent danger.

5.3.i. *Communication to private parties*
The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation

or authorisation, or with the authorisation of the supervisory authority.

5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:

a) the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b) the communication is necessary so as to prevent a serious and imminent danger.

5.4. *International communication*

Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

a) if there exists a clear legal provision under national or international law,

b) in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law,

and provided that domestic regulations for the protection of the person are not prejudiced.

5.5.i. *Requests for communication*

Subject to specific provisions contained in national legislation or in international agreements, requests for communication of data should provide indications as to the body or person requesting them as well as the reason for the request and its objective.

5.5.ii. *Conditions for communication*

As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.

If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their non-conformity.

5.5.iii. *Safeguards for communication*

The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.

Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.

5.6. *Interconnection of files and on-line access to files*

The interconnection of files with files held for different purposes is subject to either of the following conditions:

a) the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or

b) in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this recommendation.

Principle 6 – Publicity, right of access to police files, right of rectification and right of appeal

6.1. The supervisory authority should take measures so as to satisfy itself that the public is informed of the existence of files which are the subject of notification as well as of its rights in regard to these files. Implementation of this principle should take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies.

6.2. The data subject should be able to obtain access to a police file at reasonable intervals and without excessive delay in accordance with the arrangements provided for by domestic law.

6.3. The data subject should be able to obtain, where appropriate, rectification of his data which are contained in a file.

Personal data which the exercise of the right of access reveals to be inaccurate or which are found to be excessive, inaccurate or irrelevant in application of any of the other principles contained in this recommendation should be erased or corrected or else be the subject of a corrective statement added to the file.

Such erasure or corrective measures should extend as fas as possible to all documents accompanying the police file and, if not done immediately, should be carried out, at the latest, at the time of subsequent processing of the data or of their next communication.

6.4. Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others.

In the interests of the data subject, a written statement can be excluded by law for specific cases.

6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.

6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

Principle 7 – Length of storage and updating of data

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data.

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

Principle 8 – Data security

8. The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration.

The different characteristics and contents of files should, for this purpose, be taken into account.

Uitgegeven de *eerste* september 1993.

De Minister van Buitenlandse Zaken,

P. H. KOOIJMANS

317620F
ISSN 0920 - 2218
Sdu Uitgeverij Plantijnstraat
's-Gravenhage 1993