Berliner
Datenschutzbeauftragter

**BERLIN**

# Internationaler und Europäischer Datenschutz

# International and European Data Protection

**Materialien zum**

24

Internationaler und Europäischer Datenschutz

International and European Data Protection

Impressum

Herausgeber: Berliner Datenschutzbeauftragter
verantwortlich: Claudia Schmid
Pallasstraße 25/26, 10781 Berlin
Telefon: (0 30) + 78 76 88 44
Telefax: (0 30) 2 16 99 27
Bildschirmtext: * 92 67 90 #

Internet: http://www.datenschutz-berlin.de
E-Mail: mailbox datenschutz-berlin.de

Redaktion,
Layout: Volker Brozio

Satz und Druck: Verwaltungsdruckerei Berlin

1. Auflage: September 1996



# Vorwort/Foreword

Die Verarbeitung und Nutzung personenbezogener Daten beschränkt sich nicht länger auf den Nationalstaat, sondern findet auf globaler Ebene statt. Die sich daraus ergebenden Risiken für die Privatsphäre des Einzelnen und den Datenschutz können deshalb nur weltweit begrenzt werden. Das explosive Wachstum des Internet hat mehrere Regierungen dazu veranlaßt, auf den Abschluß von internationalen Vereinbarungen zu dringen, die bestimmte Aspekte dieses „Netzes der Netze“ betreffen. Das ist durchaus auch für den Datenschutz und die Privatsphäre zu prüfen. Allerdings lohnt es sich, zunächst die vorhandenen internationalen und supranationalen Vereinbarungen und Richtlinien zu analysieren, die den grenzüberschreitenden Datenfluß regeln. Einige von ihnen sind kaum bekannt. Andere sind zwar nicht rechtsverbindlich, gehören aber zur Kategorie des „weichen Rechts“, das durchaus später zu bindenden Rechtsregeln führen kann. Als Beitrag zu der gegenwärtigen Diskussion dieser Fragen haben wir in dieser Broschüre eine Sammlung bestehender internationaler und europäischer Richtlinien und Konventionen in einer zweisprachigen Version veröffentlicht.

Außerdem enthält diese Veröffentlichung zwei Dokumente aus den Vereinigten Staaten und aus der Russischen Föderation, die zum Bereich der nationalen Regulierung gehören. Bemerkenswert ist, daß die US Privacy Principles im Gegensatz zum Gesetz der Russischen Föderation über Information, Informatisierung und Informationsschutz keine Gesetzeskraft haben. Das bedeutet naturgemäß nicht, daß dieses Gesetz in der Praxis mehr bewirkt als die amerikanischen Grundsätze. Die US Privacy Principles sind interessant zu lesen vor dem Hintergrund der Europäischen Richtlinie (95/46/EG) und ihren Auswirkungen auf transatlantische Datenflüsse.

Anmerkungen der Leser dieser Veröffentlichung und Vorschläge für eine spätere Ergänzung sind jederzeit willkommen.

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

The processing and use of personal data is no longer confined to the nation state but happens on a global level. The corresponding risks to data protection and privacy can therefore only be tackled on a worldwide basis. The explosive growth of the Internet has prompted governments to call for international agreements on certain aspects of the use of the „network of networks“. This is also to be considered with respect to data protection and privacy on the Internet. However, it is worthwhile first to examine the existing set of international and supra-national rules and guidelines governing transborder data flow. Some of them are little known. Others do not have a binding legal effect but belong to the category of „soft law“ which might lead to strict rules of law at a later stage. In order to contribute to the ongoing discussion of these issues we have published in this brochure a bilingual collection of existing international and European rules, guidelines, conventions and directives.

In addition this publication contains two documents from the United States and from the Russian Federation which belong to the national sphere of regulation. It is interesting to note that the US Privacy Principles do not have the force of law whereas the Law of the Russian Federation on Information, Informatisation and Information Protection is legally binding. This does not mean that the former is less effective in practice than the latter. The US Privacy Principles are interesting to read against the background of the European Directive 95/46/EC and its repercussions on transatlantic data flow.

You are invited to comment on this publication and to suggest further texts to be included in future editions.

Dr. Hansjürgen Garstka
Berlin Data Protection Commissioner





# Inhaltsverzeichnis/Table of Contents

**Nationale Dokumente/National Documents**







# A. Vereinte Nationen/United Nations

## I. Richtlinien betreffend personenbezogene Daten in automatisierten Dateien

von der Generalversammlung beschlossen am 14. Dezember 1990

Die Verfahrensweisen für die Anwendung der Bestimmungen bezüglich personenbezogener Daten in automatisierten Dateien werden der Initiative der einzelnen Staaten überlassen. Sie müssen sich jedoch an folgenden Grundsätzen orientieren:

### A. Grundsätze betreffend den Mindeststandard, der durch die nationale Gesetzgebung gewährleistet werden sollte

#### 1. Grundsatz der Rechtmäßigkeit und der Beachtung von Treu und Glauben

Personenbezogene Informationen sollten nicht auf rechtswidrige Weise oder unter Verstoß gegen Treu und Glauben erhoben oder verarbeitet werden, noch sollten die Informationen für Zwecke verwendet werden, die im Gegensatz zu den Zielsetzungen und Grundsätzen der Charta der Vereinten Nationen stehen.

#### 2. Grundsatz der Richtigkeit

Die für die Zusammenstellung und Führung von Dateien verantwortlichen Personen sind dazu verpflichtet, die Richtigkeit und Relevanz der erfaßten Daten regelmäßig zu überprüfen und dafür Sorge zu tragen, daß sie, um Irrtümer und Auslassungen zu vermeiden, so vollständig wie möglich geführt und regelmäßig oder anläßlich der Verwendung der in der Datei gespeicherten Angaben auf den neuesten Stand gebracht werden, solange mit den Daten gearbeitet wird.

#### 3. Grundsatz der Zweckbestimmung

Der Zweck, dem eine Datei dienen soll, und deren dementsprechende Verwendung sollten genau bestimmt werden, rechtmäßig sein, und eine Datei sollte bei ihrer Einrichtung zu einem gewissen Grad öffentlich bekannt gemacht oder der Betroffene davon in Kenntnis gesetzt werden. Dadurch soll anschließend sichergestellt werden können daß

a) alle erhobenen und erfaßten personenbezogenen Daten für die solcherart festgelegten Zwecke relevant und angemessen bleiben;

b) keine der genannten personenbezogenen Daten für Zwecke, die im Widerspruch mit den solcherart festgelegten Zwecken stehen, genutzt oder übermittelt werden, es sei denn, der Betroffene hat eingewilligt;

c) der Zeitraum, über den die personenbezogenen Daten gespeichert bleiben, nicht länger ist als der Zeitraum, der zur Erfüllung des solcherart festgelegten Zwecks erforderlich ist.

**4. Grundsatz der Möglichkeit des Betroffenen zur Einsichtnahme**

Jeder, der seine Identität nachweist, hat das Recht, Kenntnis davon zu erlangen, ob seine Person betreffende Informationen verarbeitet werden und sie ohne unangemessene Verzögerung oder Kosten in verständlicher Form zur Verfügung gestellt zu bekommen sowie im Falle unrechtmäßiger, nicht erforderlicher oder ungenauer Eintragungen eine entsprechende Berichtigung bzw. Löschung zu erwirken und über die Adressaten in Kenntnis gesetzt zu werden, falls die Informationen weitergegeben werden. Entsprechende Rechtsmittel sollten festgelegt werden, und, falls erforderlich, sollte die in Grundsatz 8 aufgeführte Aufsichtsbehörde angegeben werden. Die Kosten einer Berichtigung sind von der für die Datei verantwortlichen Person zu tragen. Es wäre wünschenswert, daß die Bestimmungen ungeachtet der Staatsangehörigkeit und des Wohnsitzes für alle Personen gelten.

**5. Grundsatz der Nichtdiskriminierung**

Vorbehaltlich der restriktiv im Grundsatz 6 niedergelegten Ausnahmen sollten Daten, die leicht zu ungesetzlicher oder willkürlicher Diskriminierung führen können, u.a. Angaben über rassische oder ethnische Herkunft, Hautfarbe, Sexualleben, politische Anschauungen, religiöse, weltanschauliche und andere Überzeugungen sowie die Mitgliedschaft in einer Vereinigung oder einer Gewerkschaft nicht erfaßt werden.

**6. Ausnahmebefugnisse**

Abweichungen von der Anwendung der unter 1 – 4 genannten Grundsätze dürfen nur zugelassen werden, wenn sie erforderlich sind, um die nationale Sicherheit, die öffentliche Ordnung, die öffentliche Gesundheit oder Moral wie auch die Rechte und Freiheiten anderer, insbesondere verfolgter Personen (humanitärer Vorbehalt), zu schützen, falls diese Abweichungen ausdrücklich durch Gesetz oder entsprechende Regelungen festgelegt sind. Diese Gesetze oder Regelungen müssen in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates ausdrücklich die Grenzen dieser Ausnahmen festlegen und einen angemessenen Schutz gewährleisten.

Abgesehen davon, daß für sie die für Ausnahmen von den Grundsätzen 1 bis 4 vorzusehenden Schutzbestimmungen bestehen müssen, dürfen Ausnahmen von dem im Grundsatz 5 verankerten Verbot der Diskriminierung nur zugelassen werden, wenn sie mit der Angemeinen Erklärung der Menschenrechte und anderen,maßgeblichen Rechtsinstrumenten zum Schutz der Menschenrechte und der Verhütung von Diskriminierung vereinbar sind.

**7. Grundsatz der Sicherheit**

Geeignete Maßnahmen sollten ergriffen werden, urn die Dateien sowohl gegen Naturgefahren, wie zufälligen Verlust oder Zerstörung, als auch gegen Gefahren durch menschliche Einwirkungen, wie z. B. unerlaubten Zugang, vorsätzlichen Mißbrauch von Daten oder das Einsetzen von Computerviren, zu schützen.





**8. Überwachung und Sanktionen**

Im Gesetz des jeweiligen Landes ist festzulegen, welche Stelle in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates dafür zuständig sein soll, die Einhaltung der obigen Grundsätze zu überwachen. Diese Stelle muß Garantien für Unparteilichkeit, für Unabhängigkeit gegenüber den für die Verarbeitung und Erhebung verantwortlichen Personen oder Behörden und fachliche Kompetenz bieten. Für den Fall der Verletzung der nationalen Rechtsvorschriften, die zur Verwirklichung der vorgenannten Prinzipien geschaffen worden sind, sollten strafrechtliche Maßnahmen oder andere Sanktionen und die jeweils angemessenen Rechtsmittel vorgesehen werden.

**9. Grenzüberschreitender Datenverkehr**

Sofem bei einem grenzüberschreitenden Datenverkehr, die Gesetzgebungen zweier oder mehrerer betroffener Staaten vergleichbare Sicherungen für den Schutz der Privatsphäre bieten, sollten die Informationen zwischen ihnen so frei wie innerhalb jedes Einzelstaates ausgetauscht werden können. Wenn keine entsprechenden Schutzbestimmungen bestehen, dürfen Beschränkungen für diesen Austausch nicht unangemessenerweise und nur insoweit verfügt werden, als der Schutz der Privatsphäre es erfordert.

**10. Geltungsbereich**

Die obigen Bestimmungen sollten in erster Linie für alle öffentlichen und privaten automatisierten Dateien einschließlich manueller Dateien gelten, für die diese Bestimmungen auf der Basis einer freiwilligen Ausweitung und unter dem Vorbehalt entsprechender Anpassungen Gültigkeit haben sollten. Ebenfalls auf freiwilliger Basis könnten spezielle Bestimmungen geschaffen werden, wodurch alle oder ein Teil der Grundsätze auch für Dateien über juristische Personen gelten sollen, besonders dann, wenn diese Angaben über Einzelpersonen enthalten.

**B. Anwendung der Richtlinien auf personenbezogene Daten in den Dateien internationaler staatlicher Organisationen**

Die vorliegenden Richtlinien sollten für personenbezogene Daten in Dateien staatlicher internationaler Organisationen gelten, vorbehaltlich etwa erforderlicher Anpassungen in bezug auf eventuelle Unterschiede, die zwischen Dateien für interne Zwecke, wie z. B. die Personalverwaltung betreffende Dateien, und Dateien für externe Zwecke bestehen könnten, die sich auf Dritte beziehen, welche mit der Organisation in Verbindung stehen.

Jede Organisation sollte eine Behörde benennen, die eine gesetzliche Zuständigkeit für die Überwachung der Einhaltung dieser Regelungen besitzt.

Humanitärer Vorbehalt: Eine Abweichung von diesen Prinzipien kann für Dateien vorgesehen werden, deren Zweck auf den Schutz der Menschenrechte und Grundfreiheiten des einzelnen oder humanitäre Hilfe gerichtet ist.

Eine entsprechende abweichende Bestimmung sollte in der nationalen Gesetzgebung für die staatlichen internationalen Organisationen vorgesehen werden, deren Abkommen über den Sitz der Organisation nicht die Anwendung der genannten nationalen Gesetzgebung ausschließt, sowie für die nichtstaatlichen internationalen Organisationen, für welche dieses Gesetz Anwendung findet.

## II. GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES

adopted by the General Assembly on 14 December 1990

The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations:

### A. Principles concerning the minimum guarantees that should be provided in national legislations

1. PRINCIPLE OF LAWFULNESS AND FAIRNESS

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. PRINCIPLE OF ACCURACY

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. PRINCIPLE OF THE PURPOSE-SPECIFICATION

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

4. PRINCIPLE OF INTERESTED-PERSON ACCESS

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

5. PRINCIPLE OF NON-DISCRIMINATION

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

6. POWER TO MAKE EXCEPTIONS

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. PRINCIPLE OF SECURITY

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. SUPERVISION AND SANCTIONS

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. TRANSBORDER DATA FLOWS

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. lf there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.





10. FIELD OF APPLICATION

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

**B. Application of the guidelines to personal data files kept by governmental international organizations**

The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

Humanitarian clause: a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

A similar derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.

# B. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

# Organisation for Economic Co-operation and Development (OECD)

## I. Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten

vom 23. September 1980 OECD-Dokument C (80) 58 (Final)

**Der Rat –**

gestützt auf Artikel 1 Buchstabe c, Artikel 3 Buchstabe a und Artikel 5 Buchstabe b des Übereinkommens vom 14. Dezember 1960 über die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung;

**In Anerkennung der Tatsache,**

daß die Mitgliedstaaten, obwohl ihr innerstaatliches Recht und ihre Politik unterschiedlich sein mögen, ein gemeinsames Interesse haben am Schutz des Persönlichkeitsbereichs und der Grundfreiheiten sowie an der Herstellung eines Ausgleichs zwischen grundlegenden, jedoch miteinander konkurrierenden Werten, wie der Achtung des Persönlichkeitsbereichs und dem freien Informationsaustausch;

daß die automatische Verarbeitung und der grenzüberschreitende Verkehr personenbezogener Daten neue Formen gegenseitiger Beziehungen zwischen den Ländem schaffen und die Einführung von Vorschriften und Praktiken erfordern, die miteinander vereinbar sind;

daß der grenzüberschreitende Verkehr personenbezogener Daten zur wirtschaftlichen und sozialen Entwicklung beiträgt; daß innerstaatliche Rechtsvorschriften über, den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten diesen grenzüberschreitenden Verkehr behindern könnten;

entschlossen, den freien Informationsaustausch zwischen den Mitgliedstaaten zu fördern und der Schaffung ungerechtfertigter Hindernisse für die Entwicklung wirtschaftlicher und sozialer Beziehungen unter den Mitgliedstaaten entgegenzuwirken –

**Empfiehlt** den Mitgliedstaaten,

1. in ihrer innerstaatlichen Gesetzgebung die Grundsätze für den Schutz des Persönlichkeitsbereichs und der Grundfreiheiten zu berücksichtigen, wie sie in den Leitlinien in der Anlage zu dieser Empfehlung dargelegt sind, die Bestandteil der Empfehlung ist;
2. sich zu bemühen, bestehende ungerechtfertigte Hindernisse für den grenzüberschreitenden Verkehr personenbezogener Daten abzubauen und nicht im Namen des Schutzes des Persönlichkeitsbereichs neue solche Hindernisse zu schaffen;

3. bei der Verwirklichung der in der Anlage enthaltenen Leitlinien zusammenzuarbeiten;
4. sich so bald wie möglich auf spezifische Konsultations- und Kooperationsverfahren für die Anwendung dieser Leitlinien zu einigen.

**Anlage**

**Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten**

**TEIL 1 - Allgemeines**

**Begriffsbestimmungen**

1. In diesen Leitlinien bedeutet
   a) »Verantwortlicher für die Datei/Datensammlung« eine natürliche oder juristische Person, die nach dem innerstaatlichen Recht zuständig ist, über Auswahl und Verwendung personenbezogener Daten unabhängig davon zu entscheiden, ob solche Daten von dieser Person oder in ihrem Namen von einem Beauftragten erfaßt, gespeichert, verarbeitet oder bekanntgegeben werden;
   b) »personenbezogene Daten« jede Information über eine bestimmte oder bestimmbare natürliche Person (»Betroffener«);
   c) »grenzüberschreitender Verkehr personenbezogener Daten« die Bewegung personenbezogener Daten über Staatsgrenzen hinweg.

**Geltungsbereich der Leitlinien**

2. Diese Leitlinien gelten sowohl im öffentlichen als auch im privaten Bereich für personenbezogene Daten, die wegen der Art und Weise, in der sie verarbeitet werden, oder wegen ihres Charakters oder wegen des Zusammenhangs, in dem sie verwendet werden, eine Gefahr für den Persönlichkeitsbereich und die Grundfreiheiten bedeuten.
3. Diese Leitlinien sollen nicht so ausgelegt werden, als verhinderten sie
   a) daß auf verschiedene Arten personenbezogener Daten je nach ihrem Charakter und dem Zusammenhang, in dem sie erfaßt, gespeichert, verarbeitet oder bekanntgegeben werden, unterschiedliche Schutzmaßnahmen angewendet werden;
   b) daß personenbezogene Daten, die offensichtlich keine Gefahr für den Persönlichkeitsbereich und die Grundfreiheiten bedeuten, von der Anwendung der Leitlinien ausgeschlossen werden;
   c) daß die Leitlinien ausschließlich auf die automatische Verarbeitung personenbezogener Daten angewendet werden.
4. Ausnahmen von den in den Teilen Zwei und Drei dieser Leitlinien enthaltenen Grundsätzen einschließlich der Ausnahmen in bezug auf die nationale Souveränität, die nationale Sicherheit und die öffentliche Ordnung sollen
   a) zahlenmäßig möglichst gering sein und
   b) der Öffentlichkeit bekanntgemacht werden.





5. Im besonderen Fall von Staaten mit föderativem Aufbau kann die Anwendung dieser Leitlinien von der Kompetenzverteilung im föderativen Staat beeinflußt werden.
6. Diese Leitlinien sollen als Mindestnorm angesehen werden, die durch zusätzliche Maßnahmen zum Schutz des Persönlichkeitsbereichs und der Grundfreiheiten ergänzt werden können.

**TEIL 2 – Grundsätze für die Anwendung im innerstaatlichen Bereich**

**Der Grundsatz der Beschränkung der Datenbeschaffung**

7. Für die Beschaffung personenbezogener Daten sollen Beschränkungen festgelegt werden; solche Daten sollen mit rechtmäßigen Mitteln und nach Treu und Glauben sowie gegebenenfalls mit Wissen oder Zustimmung des Betroffenen erhoben werden.

**Der Grundsatz der Qualität der Daten**

8. Personenbezogene Daten sollen im Hinblick auf ihren Verwendungszweck erheblich und, soweit es der Verwendungszweck erfordert, sachlich richtig, vollständig und auf den neuesten Stand gebracht sein.

**Der Grundsatz der Angabe des Zweckes**

9. Die Zwecke, für die personenbezogene Daten beschafft werden, sollen spätestens bei der Datenbeschaffung im einzelnen angegeben werden, und die Daten sollen danach nur für diese Zwecke oder für solche anderen Zwecke verwendet werden, die mit den angegebenen nicht unvereinbar sind und die jeweils bei der Zweckänderung angegeben werden.

**Der Grundsatz der Beschränkung der Verwendung**

10. Personenbezogene Daten sollen nicht für andere als die nach Punkt 9 angegebenen Zwecke preisgegeben, zur Verfügung gestellt oder sonst verwendet werden, es sei denn
    a) mit Zustimmung des Betroffenen oder
    b) aufgrund gesetzlicher Ermächtigung.

**Der Grundsatz der Sicherungsmaßnahmen**

11. Personenbezogene Daten sollen durch angemessene Sicherungsmaßnahmen gegen Gefahren wie Verlust, unbefugten Zugang sowie unbefugte Zerstörung, Verwendung, Änderung oder Preisgabe geschützt werden.

**Der Grundsatz der Transparenz**

12. Es soll allgemein gewährleistet werden, daß Entwicklung, Praxis und Politik hinsichtlich personenbezogener Daten durchschaubar sind. Die Mittel sollen leicht zu beschaffen sein, mit denen das Vorhandensein personenbezogener Daten, ihr Charakter und ihre Hauptverwendungszwecke sowie die Identität und der gewöhnliche Aufenthaltsort des Verantwortlichen für die Datei/Datensammlung festgestellt werden können.

**Der Grundsatz der Beteiligung des einzelnen**

13. Der einzelne soll das Recht haben,

    a) von dem Verantwortlichen für eine Datei/Datensammlung oder auf andere Weise die Bestätigung zu erhalten, ob dieser Daten über ihn hat oder nicht;

    b) zu verlangen, daß ihm die Daten, die ihn betreffen,

        i) innerhalb einer angemessenen Frist;

        ii) kostenlos oder gegen eine nicht übermäßige Gebühr;

        iii) in angemessener Weise und

        iv) in einer für ihn leicht verständlichen Form mitgeteilt werden;

    c) über die Gründe einer Ablehnung eines Ersuchens nach den Buchstaben a und b unterrichtet zu werden; eine solche Ablehnung anfechten zu können, und

    d) ihn betreffende Daten anzufechten und, wenn die Anfechtung begründet ist, zu verlangen, daß diese Daten gelöscht, berichtigt, vervollständigt oder geändert werden.

**Der Grundsatz der Verantwortlichkeit**

14. Ein Verantwortlicher für eine Datei/Datensammlung soll für die Beachtung der Maßnahmen verantwortlich sein, welche die oben genannten Grundsätze verwirklichen.

**TEIL 3 – Grundsätze für die Anwendung im internationalen Bereich – Freier Datenverkehr und rechtmäßige Beschränkungen**

15. Die Mitgliedstaaten sollen die Folgen der inländischen Verarbeitung und der Wiederausfuhr personenbezogener Daten für andere Mitgliedstaaten berücksichtigen.

16. Die Mitgliedstaaten sollen alle zumutbaren und angemessenen Maßnahmen ergreifen, um zu gewährleisten, daß der grenzüberschreitende Verkehr personenbezogener Daten einschließlich der Durchfuhr durch einen Mitgliedstaat ohne Unterbrechung und sicher abläuft.

17. Ein Mitgliedstaat soll den grenzüberschreitenden Verkehr personenbezogener Daten zwischen seinem Hoheitsgebiet und dem eines anderen Mitgliedstaats nicht beschränken, es sei denn, daß der letztere diese Leitlinien in wesentlichen Punkten noch nicht einhält, oder daß die Wiederausfuhr solcher Daten eine Umgehung seiner innerstaatlichen Rechtsvorschriften über den Schutz des Persönlichkeitsbereichs und der Grundfreiheiten ermöglichen würde. Ein Mitgliedstaat kann auch Einschränkungen in bezug auf bestimmte Arten personenbezogener Daten einführen, für die seine innerstaatlichen Rechtsvorschriften über den Schutz des Persönlichkeitsbereichs und der Grundfreiheiten wegen des Charakters dieser Daten besondere Regelungen umfassen und für die der andere Mitgliedstaat keinen gleichwertigen Schutz vorsieht.





18. Die Mitgliedstaaten sollen nicht im Namen des Schutzes des Persönlichkeitsbereichs und der Grundfreiheiten Rechtsvorschriften, Grundsätze und Praktiken entwickeln, die für den grenzüberschreitenden Verkehr personenbezogener Daten Hindernisse schaffen würden, die über die Erfordernisse eines solchen Schutzes hinausgehen.

**TEIL 4 – Verwirklichung im nationalen Bereich**

19. Bei der Verwirklichung der in den Teilen Zwei und Drei dargelegten Grundsätze im innerstaatlichen Bereich sollen die Mitgliedstaaten Gerichts-, Verwaltungs- oder andere Verfahren oder Einrichtungen zum Schutz des Persönlichkeitsbereichs und der Grundfreiheiten im Zusammenhang mit personenbezogenen Daten schaffen. Die Mitgliedstaaten sollen sich insbesondere bemühen,

    a) angemessene innerstaatliche Rechtsvorschriften einzuführen;

    b) die Selbstregelung zu fördern und zu unterstützen, sei es in Form eines Verhaltenskodex oder in anderer Weise;

    c) dem einzelnen angemessene Mittel zur Verfügung zu stellen, damit er seine Rechte ausüben kann;

    d) ausreichende Sanktionen und Rechtsmittel für den Fall einzuführen, daß Maßnahmen, die der Verwirklichung der in den Teilen Zwei und Drei dargelegten Grundsätze dienen, nicht beachtet werden;

    e) sicherzustellen, daß es zu keiner unbilligen Diskriminierung von Betroffenen kommt.

**TEIL 5 – Internationale Zusammenarbeit**

20. Die Mitgliedstaaten sollen auf Ersuchen anderen Mitgliedstaaten Einzelheiten über die Anwendung der in diesen Leitlinien dargelegten Grundsätze zur Kenntnis bringen. Die Mitgliedstaaten sollen ferner dafür sorgen, daß die Verfahren, die auf den grenzüberschreitenden Verkehr personenbezogener Daten sowie auf den Schutz des Persönlichkeitsbereichs und der Grundfreiheiten Anwendung finden, einfach und mit denjenigen anderer Mitgliedstaaten, welche die Leitlinien einhalten, vereinbar sind.

21. Die Mitgliedstaaten sollen Verfahren festlegen, um

    i) den mit diesen Leitlinien zusammenhängenden Informationsaustausch sowie

    ii) die gegenseitige Hilfe in den dabei auftretenden Verfahrens- und Ermittlungsfragen zu erleichtern.

22. Die Mitgliedstaaten sollen auf die Entwicklung sowohl innerstaatlicher als auch internationaler Grundsätze hinarbeiten, nach denen sich das anzuwendende Recht beim grenzüberschreitenden Verkehr personenbezogener Daten bestimmt.

## II. RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

Adopted by the Council 23 September 1980

The Council,

Having regard to articles 1(c), 3(a), and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960; Recognizing: that, although national laws and policies may differ. Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information; that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices; that transborder flows of personal data contribute to economic and social development; that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows; determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

ANNEX

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
   a) “data controller” means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
   b) “personal data” means any information relating to an identified or identifiable individual (data subject);
   c) “transborder flows of personal data” means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
   c) the application of the Guidelines only to automatic processing of personal data.
4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
   a) as few as possible, and
   b) made known to the public.
5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.
6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject:

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.





Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to: (a) adopt appropriate domestic legislation; (b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise; (c) provide for reasonable means for individuals to exercise their rights; (d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and (e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate: (i) information exchange related to these Guidelines, and (ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.





# C. Europarat/Council of Europe

## I. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)

vom 28. Januar 1981

**Präambel**

Die Mitgliedstaaten des Europarats, die dieses Übereinkommen unterzeichnen –

in der Erwägung, daß es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen, die vor allem auf die Achtung des Vorranges des Rechts sowie der Menschenrechte und Grundfreiheiten beruht,

in der Erwägung, daß es angesichts des zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten wünschenswert ist, den Schutz der Rechte und Grundfreiheiten jedes Menschen, vor allem das Recht auf Achtung des Persönlichkeitsbereichs zu erweitern,

unter zugleicher Bekräftigung, für eine Informationsfreiheit ohne Rücksicht auf Staatsgrenzen einzutreten,

in Anerkennung, der Notwendigkeit, die grundlegenden Werte der Achtung des Persönlichkeitsbereichs und des freien Informationsaustausches zwischen den Völkern in Einklang zu bringen – sind wie folgt übereingekommen:

**Kapitel I – Allgemeine Bestimmungen**

**Artikel 1 – Gegenstand und Zweck**

Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf Achtung des Persönlichkeitsbereichs, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden (»Datenschutz«).

**Artikel 2 – Begriffsbestimmungen**

In diesem Übereinkommen

a) bedeutet »personenbezogene Daten« jede Information über eine bestimmte oder bestimmbare natürliche Person (»Betroffener«);

b) bedeutet »automatisierte Datei/Datensammlung« jede zur automatischen Verarbeitung erfaßte Gesamtheit von Informationen;

c) umfaßt »automatische Verarbeitung« die folgenden Tätigkeiten, wenn sie ganz oder teilweise mit Hilfe automatischer Verfahren durchgeführt werden: das Speichern von Daten Durchführung logischer und/oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten;

d) bedeutet »Verantwortlicher für die Datei/Datensammlung« die natürliche oder juristische Personen, die Behörde, die Einrichtung oder jede andere Stelle, die nach dem innerstaatlichen Recht zuständig ist, darüber zu entscheiden, welchen Zweck die automatisierte Datei/Datensammlung haben soll, welche Arten personenbezogener Daten gespeichert und welche Verarbeitungsverfahren auf sie angewendet werden sollen.

**Artikel 3 – Geltungsbereich**

(1) Die Vertragsparteien verpflichten sich, dieses Übereinkommen auf automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden.

(2) Jeder Staat kann bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde oder jederzeit danach durch Erklärung an den Generalsekretär des Europarats bekanntgeben.

a) daß er dieses Übereinkommen auf bestimmte Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten nicht anwendet, und hinterlegt ein Verzeichnis dieser Arten. In das Verzeichnis darf er jedoch Arten automatisierter Dateien/Datensammlungen nicht aufnehmen, die nach seinem innerstaatlichen Recht Datenschutzvorschriften unterliegen. Er ändert dieses Verzeichnis durch eine neue Erklärung, wenn weitere Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten seinen innerstaatlichen Datenschutzvorschriften unterstellt werden;

b) daß er dieses Übereinkommen auch auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stellen anwendet, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht;

c) daß er dieses Übereinkommen auch auf Dateien/Datensammlungen mit personenbezogenen Daten anwendet, die nicht automatisch verarbeitet werden.

(3) Jeder Staat, der den Geltungsbereich dieses Übereinkommens durch eine Erklärung nach Absatz 2 Buchstabe b oder c erweitert hat, kann in dieser Erklärung bekanntgeben, daß die Erweiterung nur für bestimmte Arten von Dateien/Datensammlungen mit personenbezogenen Daten gilt; er hinterlegt ein Verzeichnis dieser Arten.

(4) Hat eine Vertragspartei bestimmte Arten von automatisierten Dateien/Datensammlungen mit personenbezogenen Daten durch eine Erklärung nach Absatz 2 Buchstabe a ausgeschlossen, so kann sie nicht verlangen, daß eine Vertragspartei, die diese Arten nicht ausgeschlossen hat, das Übereinkommen auf diese Arten anwendet.

(5) Ebenso kann eine Vertragspartei, die keine Erweiterung nach Absatz 2 Buchstabe b oder c vorgenommen hat, in diesen Punkten die Anwendung dieses Übereinkommens nicht verlangen von einer Vertragspartei, die eine solche Erweiterung vorgenommen hat.





(6) Die Erklärungen nach Absatz 2 werden mit Inkrafttreten des Übereinkommens für den Staat wirksam, der sie abgegeben hat, wenn sie im Zeitpunkt der Unterzeichnung oder der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde abgegeben worden sind, oder drei Monate nach ihrem Eingang beim Generalsekretär des Europarats, wenn sie später abgegeben worden sind. Diese Erklärungen können ganz oder teilweise durch Notifikation an den Generalsekretär zurückgenommen werden. Die Zurücknahme wird drei Monate nach Eingang der Notifikation wirksam.

**Kapitel II – Grundsätze für den Datenschutz**

**Artikel 4 – Pflichten der Vertragsparteien**

(1) Jede Vertragspartei trifft in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen, die in diesem Kapitel aufgestellten Grundsätze für den datenschutz zu verwirklichen.

(2) Jede Vertragspartei trifft diese Maßnahme spätestens zu dem Zeitpunkt, zu dem dieses Übereinkommen für sie in Kraft tritt.

**Artikel 5 – Qualität der Daten**

Personenbezogene Daten, die automatisch verarbeitet werden,

a) müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;

b) müssen für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so vewendet werden, daß es mit diesen Zwecken unvereinbar ist,

c) müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;

d) müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein;

e) müssen so aufbewahrt werden, daß der Betroffene nicht länger indentifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.

**Artikel 6 – Besondere Arten von Daten**

Personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen, dürfen nur automatisch verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet. Dasselbe gilt für personenbezogene Daten über Strafurteile.

**Artikel 7 – Datensicherung**

Für den Schutz personenbezogener Daten, die in automatisierten Dateien/Datensammlungen gespeichert sind, werden geeignete Sicherungsmaßnahmen getroffen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben.

**Artikel 8 – Zusätzlicher Schutz für den Betroffenen**

Jedermann muß die Möglichkeit haben,

a) das Vorhandensein einer automatisierten Datei/Datensammlung mit personenbezogenen Daten, ihre Hauptzwecke sowie die Bezeichnung, den gewöhnlichen Aufenthaltsort oder den Sitz des Verantwortlichen für die Datei/Datensammlung festzustellen;

b) in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten die Bestätigung zu erhalten, ob Daten über ihn in einer automatisierten Datei/Datensammlung mit personenbezogenen Daten gespeichert sind, sowie zu erwirken, daß ihm diese Daten in verständlicher Form mitgeteilt werden;

c) gegebenenfalls diese Daten berichtigen oder löschen lassen, wenn sie entgegen den Vorschriften des innerstaatlichen Rechts verarbeitet worden sind, welche die Grundsätze der Artikel 5 und 6 verwirklichen;

d) über ein Rechtsmittel zu verfügen, wenn seiner Forderung nach Bestätigung oder gegebenenfalls nach Mitteilung, Berichtigung oder Löschung im Sinne der Buchstaben b und c nicht entsprochen wird.

**Artikel 9 – Ausnahmen und Einschränkungen**

(1) Ausnahmen von den Artikeln 5, 6 und 8 sind nicht zulässig, abgesehen von den in diesem Artikel vorgesehenen.

(2) Eine Abweichung von den Artikeln 5, 6 und 8 ist zulässig, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist

a) zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b) zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter.

(3) Die Ausübung der Rechte nach Artikel 8 Buchstabe b, c und d kann durch Gesetz für automatisierte Dateien/Datensammlungen mit personenbezogenen Daten eingeschränkt werden, die Zwecken der Statistik oder der wissenschaftlichen Forschung dienen, wenn offensichtlich keine Gefahr besteht, daß der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird.

**Artikel 10 – Sanktionen und Rechtsmittel**

Jede Vertragspartei verpflichtet sich, geeignete Sanktionen und Rechtsmittel für Verletzungen der Vorschriften des innerstaatlichen Rechts, welche die in diesem Kapitel aufgestellten Grundsätze für den Datenschutz verwirklichen, festzulegen.

**Artikel 11 – Weitergehender Schutz**

Dieses Kapitel ist nicht so auszulegen, als ob es die Möglichkeit begrenze oder auf andere Weise beeinträchtige, daß eine Vertragspartei den Betroffenen ein größeres Maß an Schutz als das in diesem Übereinkommen vorgeschriebene gewährt.





**Kapitel III – Grenzüberschreitender Datenverkehr**

**Artikel 12 – Grenzüberschreitender Verkehr personenbezogener Daten und innerstaatliches Recht**

(1) Werden personenbezogene Daten, die automatisch verarbeitet werden oder für eine solche Verarbeitung beschafft worden sind – mittels welcher Datenträger auch immer – über die Staatsgrenzen hinweg weitergegeben, so finden die folgenden Bestimmungen Anwendung.

(2) Eine Vertragspartei darf allein zum Zweck des Schutzes des Persönlichkeitsbereichs von Betroffenen den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen.

(3) Jede Vertragsparlei ist jedoch berechtigt, von Absatz 2 abzuweichen,

a) soweit ihr Recht für bestimmte Arten von personenbezogenen Daten oder automatisierten Dateien/Datensammlungen mit personenbezogenen Daten wegen der Beschaffenheit dieser Arten besondere Vorschriften enthält, es sei denn, die Vorschriften der anderen Vertragspartei sehen einen gleichwertigen Schutz vor;

b) um zu verhindern, daß ihr Recht dadurch umgangen wird, daß eine Weitergabe aus ihrem Hoheitsgebiet in das Hoheitsgebiet einer Nichtvertragspartei auf dem Weg über das Hoheitsgebiet einer anderen Vertragspartei erfolgt.

**Kapitel IV – Gegenseitige Hilfeleistung**

**Artikel 13 – Zusammenarbeit zwischen den Vertragsparteien**

(1) Die Vertragsparteien verpflichten sich, einander bei der Durchführung dieses Übereinkommens Hilfe zu leisten,

(2) Zu diesem Zweck

a) bezeichnet jede Vertragspartei eine oder mehrere Behörden und teilt deren amtliche Bezeichnung und Anschrift dem Generalsekretär des Europarats mit;

b) legt jede Vertragspartei, die mehrere Behörden bezeichnet hat, die Zuständigkeit jeder Behörde fest und gibt sie in ihrer Mitteilung nach Buchstabe a an.

(3) Eine bezeichnete Behörde einer Vertragspartei wird auf Ersuchen einer bezeichneten Behörde einer anderen Vertragspartei

a) Auskünfte über Recht und Verwaltungspraxis im Bereich des Datenschutzes erteilen;

b) in Übereinstimmung mit dem innerstaatlichen Recht und allein zum Zweck des Schutzes des Persönlichkeitsbereichs alle geeigneten Maßnahmen treffen, um Sachauskünfte über eine bestimmte automatische Verarbeitung, die in ihrem Hoheitsgebiet durchgeführt wird, zu erteilen, jedoch mit Ausnahme der dabei verarbeiteten personenbezogenen Daten.

**Artikel 14 – Unterstützung von Betroffenen, die im Ausland wohnen**

(1) Jede Vertragspartei unterstützt Personen, die im Ausland wohnen, bei der Ausübung der Rechte, die ihnen nach dem innerstaatlichen Recht zustehen, das die in Artikel 8 aufgestellten Grundsätze verwirklicht.

(2) Eine im Hoheitsgebiet einer anderen Vertragspartei wohnende Person kann ihren Antrag über die bezeichnete Behörde dieser Vertragspartei stellen.

(3) Der Antrag auf Unterstützung muß alle erforderlichen Angaben enthalten, insbesondere über

a) den Namen, die Anschrift und alle anderen für die Identifizierung des Antragstellers erheblichen Einzelheiten;

b) die automatisierte Datei/Datensammlung mit personenbezogenen Daten oder den dafür Verantwortlichen, auf die sich der Antrag bezieht;

c) den Zweck des Antrags.

**Artikel 15 – Sicherheiten bei Hilfeleistung durch bezeichnete Behörden**

(1) Hat eine bezeichnete Behörde einer Vertragspartei von einer bezeichneten Behörde einer anderen Vertragspartei Auskünfte erhalten, die einem Antrag auf Unterstützung dienen oder Antwort auf ein eigenes Ersuchen geben, so darf sie diese Auskünfte nur zu den Zwecken verwenden, die dem Antrag oder Ersuchen zugrunde liegen.

(2) Jede Vertragspartei sorgt dafür, daß die Personen, die der bezeichneten Behörde angehören oder in ihrem Namen handeln, durch entsprechende Verpflichtungen zur Geheimhaltung oder zur vertraulichen Behandlung dieser Auskünfte gebunden werden.

(3) Es ist einer bezeichneten Behörde in keinem Fall erlaubt, nach Artikel 14 Absatz 2 im Namen eines im Ausland wohnenden Betroffenen von sich aus und ohne seine ausdrückliche Zustimmung einen Antrag auf Unterstützung zu stellen.

**Artikel 16 – Ablehnung von Ersuchen und Anträgen**

Eine bezeichnete Behörde, an die nach Artikel 13 ein Ersuchen oder nach Artikel 14 ein Antrag gerichtet wird, kann nur ablehnen, ihnen stattzugeben, wenn

a) sie mit den Befugnissen der für die Beantwortung zuständigen Behörden auf dem Gebiet des Datenschutzes nicht vereinbar sind;

b) sie den Bestimmungen dieses Übereinkommens nicht entsprechen;

c) ihre Erfüllung mit der Souveränität, der Sicherheit oder der öffentlichen Ordnung der Vertragspartei, die sie bezeichnet hat, oder mit den Rechten und Grundfreiheiten der Personen, die der Gerichtsbarkeit dieser Vertragspartei unterstehen, nicht vereinbar wäre.

**Artikel 17 – Kosten und Verfahren**

(1) Für Hilfe, welche die Vertragsparteien einander nach Artikel 13 leisten, oder für Unterstützung, die sie Betroffenen im Ausland nach Artikel 14 leisten, werden keine Auslagen oder Gebühren außer für Sachverständige und Dolmetscher erhoben. Diese Auslagen oder Gebühren werden von der Vertragspartei getragen, welche die ersuchende Behörde bezeichnet hat.

(2) Der Betroffene kann nicht verpflichtet werden, für Schritte, die im Hoheitsgebiet einer anderen Vertragspartei für ihn unternommen werden, höhere Auslagen oder Gebühren zu zahlen, als von Personen erhoben werden können, die im Hoheitsgebiet der betreffenden Vertragspartei wohnen.

(3) Die sonstigen Einzelheiten im Zusammenhang mit der Hilfeleistung oder Unterstützung, insbesondere hinsichtlich der Form und der Verfahren sowie der zu verwendenden Sprachen, werden unmittelbar zwischen den beteiligten Vertragsparteien festgelegt.

**Kapitel V – Beratender Ausschuß**

**Artikel 18 – Zusammensetzung des Ausschusses**

(1) Nach dem Inkrafttreten dieses Übereinkommens wird ein Beratender Ausschuß eingesetzt.

(2) Jede Vertragspartei ernennt einen Vertreter und einen Stellvertreter für diesen Ausschuß. Jeder Mitgliedstaat des Europarats, der nicht Vertragspartei des Übereinkommens ist, hat das Recht, sich im Ausschuß durch einen Beobachter vertreten zu lassen.

(3) Der Beratende Ausschuß kann durch einstimmigen Beschluß jeden Nichtmitgliedstaat des Europarats, der nicht Vertragspartei des Übereinkommens ist, einladen, sich durch einen Beobachter in einer seiner Sitzungen vertreten zu lassen.

**Artikel 19 – Aufgaben des Ausschusses**

Der Beratende Ausschuß

a) kann Vorschläge zur Erleichterung oder Verbesserung der Anwendung des Übereinkommens machen;

b) kann in Übereinstimmung mit Artikel 21 Änderungen dieses Übereinkommens vorschlagen;

c) nimmt zu jeder vorgeschlagenen Änderung, dieses Übereinkommens Stellung, die ihm nach Artikel 21 Absatz 3 unterbreitet wird;

d) kann auf Ersuchen einer Vertragspartei zu allen Fragen im Zusammenhang mit der Anwendung dieses Übereinkommens Stellung nehmen.

**Artikel 20 – Verfahren**

(1) Der Beratende Ausschuß wird vom Generalsekretär des Europarats einberufen. Seine erste Sitzung findet innerhalb von zwölf Monaten nach Inkrafttreten dieses Übereinkommens statt. Danach tritt er mindestens alle zwei Jahre sowie immer dann zusammen, wenn ein Drittel der Vertreter der Vertragsparteien dies verlangt.

(2) Der Beratende Ausschuß ist in einer Sitzung beschlußfähig, wenn die Mehrheit der Vertreter der Vertragspartei anwesend ist.

(3) Im Anschluß an jede Sitzung unterbreitet der Beratende Ausschuß dem Ministerkomitee des Europarats einen Bericht über seine Arbeit und die Wirksamkeit des Übereinkommens.

(4) In Übereinstimmung mit diesem Übereinkommen gibt sich der Beratende Ausschuß eine Geschäftsordnung.

**Kapitel VI –Änderungen**

**Artikel 21 – Änderungen**

(1) Änderungen dieses Übereinkommens können von einer Vertragspartei, vom Ministerkomitee des Europarats oder vom Beratenden Ausschuß vorgeschlagen werden.

(2) Der Generalsekretär des Europarats teilt jeden Änderungsvorschlag den Mitgliedstaaten des Europarats sowie jedem Nichtmitgliedstaat mit, der diesem Übereinkommen beigetreten ist oder der nach Artikel 23 eingeladen worden ist, ihm beizutreten.

(3) Darüber hinaus wird jede von einer Vertragspartei oder vom Ministerkomitee vorgeschlagene Änderung dem Beratenden Ausschuß übermittelt; dieser teilt dem Ministerkomitee seine Stellungnahme zu der vorgeschlagenen Änderung mit.

(4) Das Ministerkomitee prüft die vorgeschlagene Änderung und die Stellungnahme des Beratenden Ausschusses und kann die Änderung genehmigen.

(5) Der Wortlaut einer Änderung, die das Ministerkomitee nach Absatz 4 genehmigt hat, wird den Vertragsparteien zur Annahme zugeleitet.

(6) Eine nach Absatz 4 genehmigte Änderung tritt am dreißigsten Tag nach dem Zeitpunkt in Kraft, zu dem alle Vertragsparteien dem Generalsekretär ihre Annahme mitgeteilt haben.

**Kapitel VII – Schlußklauseln**

**Artikel 22 – Inkrafttreten**

(1) Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

(2) Das Übereinkommen tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Mitgliedstaaten des Europarats nach Absatz 1 ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein.

(3) Für jeden Mitgliedstaat, der später seine Zustimmung ausdrückt, durch das Übereinkommen gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Ratifikations-, Annahme- oder Genehmigungsurkunde folgt.





**Artikel 23 – Beitritt von Nichtmitgliedstaaten**

(1) Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats durch einen mit der in Artikel 20 Buchstabe d der Satzung vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Komitee haben, gefaßten Beschluß jeden Nichtmitgliedstaat des Rates einladen, dem Übereinkommen beizutreten.

(2) Für jeden beitretenden Staat tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Beitrittsurkunde beim Generalsekretär des Europarats folgt.

**Artikel 24 – Räumlicher Geltungsbereich**

(1) Jeder Staat kann bei der Unterzeichnung, oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

(2) Jeder Staat kann jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt.

(3) Jede nach den Absätzen 1 und 2 abgegebene Erklärung kann in bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Zurücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

**Artikel 25 – Vorbehalte**

Vorbehalte zu diesem Übereinkommen sind nicht zulässig.

**Artikel 26 – Kündigung**

(1) Jede Vertragspartei kann dieses Übereinkommen jederzeit durch eine an den Generalsekretär des Europarats gerichtete Notifikation kündigen.

(2) Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

**Artikel 27 – Notifikation**

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Rates und jedem Staat, der diesem Übereinkommen beigetreten ist,

a) jede Unterzeichnung;

b) jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;

c) jeden Zeitpunkt des Inkrafttretens dieses Übereinkommens nach den Artikeln 22, 23 und 24;

d) jede andere Handlung, Notifikation oder Mitteilung im Zusammenhang mit diesem Übereinkommen.

Zu Urkunde dessen haben die hierzu befugten Unterzeichneten dieses Übereinkommen unterschrieben.

Geschehen zu Straßburg am 28. Januar 1981 in englischer und französischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats und allen zum Beitritt zu diesem Übereinkommen eingeladenen Staaten beglaubigte Abschriften.





## II. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

**Council of Europe, European Treaty Series No. 108.**
**Signed January 28, 1981**

The Member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

### CHAPTER I – GENERAL PROVISIONS

#### Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

#### Article 2 – Definitions

For the purposes of this convention:

a) "personal data" means any information relating to an identified or identifiable individual ("data subject");

b) "automated data file" means any set of data undergoing automatic processing;

c) "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

d) "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 – Scope

(1) The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

(2) Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a) that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b) that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c) that it will also apply this convention to personal data files which are not processed automatically.

(3) Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

(4) Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

(5) Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraph 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

(6) The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

## CHAPTER II – BASIC PRINCIPLES FOR DATA PROTECTION

Article 4 – Duties of the Parties

(1) Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

(2) These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.





Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

d) accurate and, where necessary, kept up to date;

e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 – Additional safeguards for the data subject

Any person shall be enabled:

a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 – Exceptions and restrictions

(1) No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

(2) Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b) protecting the data subject or the rights and freedoms of others.

(3) Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 – Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 – Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects of wider measure of protection than that stipulated in this convention.

CHAPTER III – TRANSBORDER DATA FLOWS

Article 12 – Transborder flows of personal data and domestic law

(1) The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

(2) A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

(3) Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.





CHAPTER IV – MUTUAL ASSISTANCE

Article 13 – Co-operation between Parties

(1) The Parties agree to render each other mutual assistance in order to implement this convention.

(2) For that purpose:

a) each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

b) each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

(3) An authority designated by a Party shall at the request of an authority designated by another Party:

a) furnish information on its law and administrative practice in the field of data protection;

b) take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 – Assistance to data subjects resident abroad

(1) Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

(2) When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

(3) The request for assistance shall contain all the necessary particulars, relating inter alia to:

a) the name, address and any other relevant particulars identifying the person making the request;

b) the automated personal data file to which the request pertains, or its controller;

c) the purpose of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities

(1) An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

(2) Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

(3) In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 – Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

a) the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

b) the request does not comply with the provisions of this convention;

c) compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 – Costs and procedures of assistance

(1) Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

(2) The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

(3) Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

## CHAPTER V – CONSULTATIVE COMMITTEE

Article 18 – Composition of the committee

(1) A Consultative Committee shall be set up after the entry into force of this convention.

(2) Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

(3) The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19 – Functions of the committee

The Consultative Committee:

a) may make proposals with a view to facilitating or improving the application of the convention;





b) may make proposals for amendment of this convention in accordance with Article 21;

c) shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;

d) may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20 – Procedure

(1) The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

(2) A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

(3) After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.

(4) Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

## CHAPTER VI – AMENDMENTS

Article 21 – Amendments

(1) Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

(2) Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

(3) Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

(4) The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

(5) The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

(6) Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII – FINAL CLAUSES

Article 22 – Entry into force

(1) This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

(2) This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

(3) In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-member States

(1) After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

(2) In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24 – Territorial clause

(1) Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

(2) Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

(3) Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 – Reservations

No reservation may be made in respect of the provisions of this convention.





Article 26 – Denunciation

(1) Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

(2) Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 – Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of

a) any signature;

b) the deposit of any instrument of ratification, acceptance, approval or accession

c) any date of entry into force of this convention in accordance with Articles 22, 23 and 24;

d) any other act, notification or communication relating to this convention.

In witness where of the undersigned, being duly authorised there to, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

# D. Europäische Union/European Union

## I. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Dies ist ein inoffizieller Text. Der rechtsverbindliche Text ist im Amtsblatt der Europäischen Gemeinschaften abgedruckt (Nr. L 281 vom 23. November 1995 S. 31).

**Inhalt**

**Erwägungsgründe**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 100 a,

auf Vorschlag der Kommission[1],

nach Stellungnahme des Wirtschafts- und Sozialausschusses[2],

gemäß dem Verfahren des Artikels 189 b des Vertrags[3],

in Erwägung nachstehender Gründe:

(1) Die Ziele der Gemeinschaft, wie sie in dem durch den Vertrag über die Europäische Union geänderten Vertrag festgelegt sind, bestehen darin, einen immer engeren Zusammenschluß der europäischen Völker zu schaffen, engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossenen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.

(3) Für die Errichtung und das Funktionieren des Binnenmarktes, der gemäß Artikel 7 a des Vertrags den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleisten soll, ist es nicht nur erforderlich, daß personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können, sondern auch, daß die Grundrechte der Personen gewahrt werden.

(4) Immer häufiger werden personenbezogene Daten in der Gemeinschaft in den verschiedenen Bereichen wirtschaftlicher und sozialer Tätigkeiten verarbeitet. Die Fortschritte der Informationstechnik erleichtern die Verarbeitung und den Austausch dieser Daten beträchtlich.

(5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Artikel 7 a des Vertrags ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen

1 ABl. Nr. C 277 vom 5. November 1990, S. 3, und ABl. Nr. C 311 vom 27. November 1992, S. 30.
2 ABl. Nr. C 159 vom 17. Juni 1991, S. 38.
3 Stellungnahme des Europäischen Parlaments vom 11. März 1992 (ABl. Nr. C 94 vom 13. April 1992, S. 198), bestätigt am 2. Dezember 1993 (ABl. Nr. C 342 vom 20. Dezember 1993, S. 30). Gemeinsamer Standpunkt des Rates vom 20. Februar 1995 (ABl. Nr. C 93 vom 13. April 1995, S. 1) und Beschluß des Europäischen Parlaments vom 15. Juni 1995 (ABl. Nr. C 166 vom 3. Juli 1995).

Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschaftsrechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaats durchführen zu können.

(6) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Telekommunikationsnetze in der Gemeinschaft erfordern und erleichtern den grenzüberschreitenden Verkehr personenbezogener Daten.

(7) Das unterschiedliche Niveau des Schutzes der Rechte und Freiheiten von Personen, insbesondere der Privatsphäre, bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaats in das Gebiet eines anderen Mitgliedstaats verhindern. Dieses unterschiedliche Schutzniveau kann somit ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und die Erfüllung des Auftrags der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden verhindern. Dieses unterschiedliche Schutzniveau ergibt sich aus der Verschiedenartigkeit der einzelstaatlichen Rechts- und Verwaltungsvorschriften.

(8) Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerläßlich. Insbesondere unter Berücksichtigung der großen Unterschiede, die gegenwärtig zwischen den einschlägigen einzelstaatlichen Rechtsvorschriften bestehen, und der Notwendigkeit, die Rechtsvorschriften der Mitgliedstaaten zu koordinieren, damit der grenzüberschreitende Fluß personenbezogener Daten kohärent und in Übereinstimmung mit dem Ziel des Binnenmarktes im Sinne des Artikels 7 a des Vertrags geregelt wird, läßt sich dieses für den Binnenmarkt grundlegende Ziel nicht allein durch das Vorgehen der Mitgliedstaaten verwirklichen. Deshalb ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich.

(9) Die Mitgliedstaaten dürfen aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen. Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an. Innerhalb dieses Spielraums können unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann.

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muß im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.





(11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

(12) Die Schutzprinzipien müssen für alle Verarbeitungen personenbezogener Daten gelten, sobald die Tätigkeiten des für die Verarbeitung Verantwortlichen in den Anwendungsbereich des Gemeinschaftsrechts fallen. Auszunehmen ist die Datenverarbeitung, die von einer natürlichen Person in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten – wie zum Beispiel Schriftverkehr oder Führung von Anschriftenverzeichnissen – vorgenommen wird.

(13) Die in den Titeln V und VI des Vertrags über die Europäische Union genannten Tätigkeiten, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im Bereich des Strafrechts betreffen, fallen unbeschadet der Verpflichtungen der Mitgliedstaaten gemäß Artikel 56 Absatz 2 sowie gemäß den Artikeln 57 und 100 a des Vertrags zur Gründung der Europäischen Gemeinschaft nicht in den Anwendungsbereich des Gemeinschaftsrechts. Die Verarbeitung personenbezogener Daten, die zum Schutz des wirtschaftlichen Wohls des Staates erforderlich ist, fällt nicht unter diese Richtlinie, wenn sie mit Fragen der Sicherheit des Staates zusammenhängt.

(14) In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muß diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden.

(15) Die Verarbeitung solcher Daten wird von dieser Richtlinie nur erfaßt, wenn sie automatisiert erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen.

(16) Die Verarbeitung von Ton- und Bilddaten, wie bei der Videoüberwachung, fällt nicht unter diese Richtlinie, wenn sie für Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder der Tätigkeiten des Staates im Bereich des Strafrechts oder anderen Tätigkeiten erfolgt, die nicht unter das Gemeinschaftsrecht fallen.

(17) Bezüglich der Verarbeitung von Ton- und Bilddaten für journalistische, literarische oder künstlerische Zwecke, insbesondere im audiovisuellen Bereich, finden die Grundsätze dieser Richtlinie gemäß Artikel 9 eingeschränkt Anwendung.

(18) Um zu vermeiden, daß einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird, müssen auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaats angewandt werden. Es ist angebracht, auf die Verarbeitung, die von einer Person, die dem in dem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen unterstellt ist, vorgenommen werden, die Rechtsvorschriften dieses Staates anzuwenden.

(19) Eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich. Wenn der Verantwortliche im Hoheitsgebiet mehrerer

Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muß er vor allem zur Vermeidung von Umgehungen sicherstellen, daß jede dieser Niederlassungen die Verpflichtungen einhält, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, das auf ihre jeweiligen Tätigkeiten anwendbar ist.

(20) Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, daß die in dieser Richtlinie vorgesehenen Richte und Pflichten tatsächlich eingehalten werden.

(21) Diese Richtlinie berührt nicht die im Strafrecht geltenden Territorialitätsregeln.

(22) Die Mitgliedstaaten können in ihren Rechtsvorschriften oder bei der Durchführung der Vorschriften zur Umsetzung dieser Richtlinie die allgemeinen Bedingungen präzisieren, unter denen die Verarbeitungen rechtmäßig sind. Insbesondere nach Artikel 5 in Verbindung mit den Artikeln 7 und 8 können die Mitgliedstaaten neben den allgemeinen Regeln besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen und für die verschiedenen Datenkategorien gemäß Artikel 8 vorsehen.

(23) Die Mitgliedstaaten können den Schutz von Personen sowohl durch ein allgemeines Gesetz zum Schutz von Personen bei der Verarbeitung personenbezogener Daten als auch durch gesetzliche Regelungen für bestimmte Bereiche, wie zum Beispiel die statistischen Ämter, sicherstellen.

(24) Diese Richtlinie berührt nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen.

(25) Die Schutzprinzipien finden zum einen ihren Niederschlag in den Pflichten, die den Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung verantwortlichen Stellen obliegen; diese Pflichten betreffen insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Datenzu erhalten, ihre Berichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können.

(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, daß die betroffene Person nicht mehr identifizierbar ist. Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht.

(27) Datenschutz muß sowohl für automatisierte als auch für nichtautomatisierte Verarbeitungen gelten. In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden. Bei manuellen Verarbeitungen erfaßt diese Richtlinie lediglich Dateien, nicht jedoch unstrukturierte





Akten. Insbesondere muß der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein, die einen leichten Zugriff auf die Daten ermöglichen. Nach der Definition in Artikel 2 Buchstabe c können die Mitgliedstaaten die Kriterien zur Bestimmung der Elemente einer strukturierten Sammlung personenbezogener Daten sowie die verschiedenen Kriterien zur Regelung des Zugriffs zu einer solchen Sammlung festlegen. Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich dieser Richtlinie.

(28) Die Verarbeitung personenbezogener Daten muß gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Sie hat den angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein.

(29) Die Weiterverarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, wenn der Mitgliedstaat geeignete Garantien vorsieht. Diese Garantien müssen insbesondere ausschließen, daß die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.

(30) Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf der Einwilligung der betroffenen Person beruht oder notwendig ist im Hinblick auf den Abschluß oder die Erfüllung eines für die betroffene Person bindenden Vertrags, zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder wenn sie im Interesse einer anderen Person erforderlich ist, vorausgesetzt, daß die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Um den Ausgleich der in Frage stehenden Interessen unter Gewährleistung eines effektiven Wettbewerbs sicherzustellen, können die Mitgliedstaaten insbesondere die Bedingungen näher bestimmen, unter denen personenbezogene Daten bei rechtmäßigen Tätigkeiten im Rahmen laufender Geschäfte von Unternehmen und anderen Einrichtungen an Dritte weitergegeben werden können. Ebenso können sie die Bedingungen festlegen, unter denen personenbezogene Daten an Dritte zum Zweck der kommerziellen Werbung oder der Werbung von Wohltätigkeitsverbänden oder anderen Vereinigungen oder Stiftungen, z. B. mit politischer Ausrichtung, weitergegeben werden können, und zwar unter Berücksichtigung der Bestimmungen dieser Richtlinie, nach denen betroffene Personen ohne Angabe von Gründen und ohne Kosten Widerspruch gegen die Verarbeitung von Daten, die sie betreffen, erheben können.

(31) Die Verarbeitung personenbezogener Daten ist ebenfalls als rechtmäßig anzusehen, wenn sie erfolgt, um ein für das Leben der betroffenen Person wesentliches Interesse zu schützen.

(32) Es ist nach einzelstaatlichem Recht festzulegen, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht oder das Privatrecht fallende Person, wie beispielsweise eine Berufsvereinigung, handeln soll.

(33) Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen, dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot müssen ausdrücklich vorgesehen werden bei spezifischen Notwendigkeiten, insbesondere wenn die Verarbeitung dieser Daten für gewisse auf das Gesundheitswesen bezogene Zwecke von Personen vorgenommen wird, die nach dem einzelstaatlichen Recht dem Berufsgeheimnis unterliegen, oder wenn die Verarbeitung für berechtigte Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, deren Ziel es ist, die Ausübung von Grundfreiheiten zu ermöglichen.

(34) Die Mitgliedstaaten können, wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien vorsehen in Bereichen wie dem öffentlichen Gesundheitswesen und der sozialen Sicherheit – insbesondere hinsichtlichder Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zurAbrechnung von Leistungen in den sozialen Krankenversicherungssystemen –, der wissenschaftlichen Forschung und der öffentlichen Statistik. Die Mitgliedstaaten müssen jedoch geeignete besondere Garantien zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.

(35) Die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im Völkerrecht niedergelegte Zwecke von staatlich anerkannten Religionsgesellschaften erfolgt ebenfalls im Hinblick auf ein wichtiges öffentliches Interesse.

(36) Wenn es in bestimmten Mitgliedstaaten zum Funktionieren des demokratischen Systems gehört, daß die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen eines wichtigen öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.

(37) Für die Verarbeitung personenbezogener Daten zu journalistischen, literarischen oder künstlerischen Zwecken, insbesondere im audiovisuellen Bereich, sind Ausnahmen von bestimmten Vorschriften dieser Richtlinie vorzusehen, soweit sie erforderlich sind, um die Grundrechte der Person mit der Freiheit der Meinungsäußerung und insbesondere der Freiheit, Informationen zu erhalten oder weiterzugeben, die insbesondere in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und der Grundfreiheiten garantiert ist, in Einklang zu bringen. Es obliegt deshalb den Mitgliedstaaten, unter Abwägung der Grundrechte Ausnahmen und Einschränkungen festzulegen, die bei den allgemeinen Maßnahmen zur Rechtmäßigkeit der Verarbeitung von Daten, bei den Maßnahmen zur Übermittlung der Daten in Drittländer sowie hinsichtlich der Zuständigkeiten der Kontrollstellen erforderlich sind, ohne daß jedoch Ausnahmen bei den Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorzusehen sind. Ferner sollte mindestens die in diesem Bereich zuständige Kontrollstelle bestimmte nachträgliche Zuständigkeiten erhalten, beispielsweise zur regelmäßigen Veröffentlichung eines Berichts oder zur Befassung der Justizbehörden.

(38) Datenverarbeitung nach Treu und Glauben setzt voraus, daß die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.

(39) Bestimmte Verarbeitungen betreffen Daten, die der Verantwortliche nicht unmittelbar bei der betroffenen Person erhoben hat. Des weiteren können Daten rechtmäßig an Dritte weitergegeben werden, auch wenn die Weitergabe bei der Erhebung der Daten bei





der betroffenen Person nicht vorgesehen war. In diesen Fällen muß die betroffene Person zum Zeitpunkt der Speicherung der Daten oder spätestens bei der erstmaligen Weitergabe der Daten an Dritte unterrichtet werden.

(40) Diese Verpflichtung erübrigt sich jedoch, wenn die betroffene Person bereits unterrichtet ist. Sie besteht auch nicht, wenn die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist oder wenn die Unterrichtung der betroffenen Person unmöglich ist oder unverhältnismäßigen Aufwand erfordert, was bei Verarbeitungen für historische, statistische oder wissenschaftliche Zwecke der Fall sein kann. Diesbezüglich können die Zahl der betroffenen Personen, das Alter der Daten und etwaige Ausgleichsmaßnahmen in Betracht gezogen werden.

(41) Jede Person muß ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, haben, damit sie sich insbesondere von der Richtigkeit dieser Daten und der Zulässigkeit ihrer Verarbeitung überzeugen kann. Aus denselben Gründen muß jede Person außerdem das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne des Artikels 15 Absatz 1, besitzen. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insbesondere das Urheberrecht zum Schutz von Software, berühren. Dies darf allerdings nicht dazu führen, daß der betroffenen Person jegliche Auskunft verweigert wird.

(42) Die Mitgliedstaaten können die Auskunfts- und Informationsrechte im Interesse der betroffenen Person oder zum Schutz der Rechte und Freiheiten Dritter einschränken. Zum Beispiel können sie vorsehen, daß Auskunft über medizinische Daten nur über ärztliches Personal erhalten werden kann.

(43) Die Mitgliedstaaten können Beschränkungen des Auskunfts- und Informationsrechts sowie bestimmter Pflichten des für die Verarbeitung Verantwortlichen vorsehen, soweit dies beispielsweise für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, für zwingende wirtschaftliche oder finanzielle Interessen eines Mitgliedstaats oder der Union oder für die Ermittlung und Verfolgung von Straftaten oder von Verstößen gegen Standesregeln bei reglementierten Berufen erforderlich ist. Als Ausnahmen und Beschränkungen sind Kontroll-, Überwachungs- und Ordnungsfunktionen zu nennen, die in den drei letztgenannten Bereichen in bezug auf öffentliche Sicherheit, wirtschaftliches oder finanzielles Interesse und Strafverfolgung erforderlich sind. Die Erwähnung der Aufgaben in diesen drei Bereichen läßt die Zulässigkeit von Ausnahmen und Einschränkungen aus Gründen der Sicherheit des Staates und der Landesverteidigung unberührt.

(44) Die Mitgliedstaaten können aufgrund gemeinschaftlicher Vorschriften gehalten sein, von den das Auskunftsrecht, die Information der Personen und die Qualität der Daten betreffenden Bestimmungen dieser Richtlinie abzuweichen, um bestimmte der oben genannten Zweckbestimmungen zu schützen.

(45) Auch wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung aufgrund eines öffentlichen Interesses, der Ausübung hoheitlicher Gewalt oder der Interessen eines einzelnen sein können, sollte doch jede betroffene Person das Recht besitzen, aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch dagegen einzulegen, daß die sie betreffenden Daten verarbeitet werden. Die Mitgliedstaaten können allerdings innerstaatliche Bestimmungen vorsehen, die dem entgegenstehen.

(46) Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern. Die Mitgliedstaaten haben dafür Sorge zu tragen, daß der für die Verarbeitung Verantwortliche diese Maßnahmen einhält. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(47) Wird eine Nachricht, die personenbezogene Daten enthält, über Telekommunikationsdienste oder durch elektronische Post übermittelt, deren einziger Zweck darin besteht, Nachrichten dieser Art zu übermitteln, so gilt in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Vearbeitung der in der Nachricht enthaltenen personenbezogenen Daten. Jedoch gelten die Personen, die diese Dienste anbieten, in der Regel als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind.

(48) Die Meldeverfahren dienen der Offenlegung der Zweckbestimmungen der Verarbeitungen sowie ihrer wichtigsten Merkmale mit dem Zweck der Überprüfung ihrer Vereinbarkeit mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

(49) Um unangemessene Verwaltungsformalitäten zu vermeiden, können die Mitgliedstaaten bei Verarbeitungen, bei denen eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht zu erwarten ist, von der Meldepflicht absehen oder sie vereinfachen, vorausgesetzt, daß diese Verarbeitungen den Bestimmungen entsprechen, mit denen der Mitgliedstaat die Grenzen solcher Verarbeitungen festgelegt hat. Eine Befreiung oder eine Vereinfachung kann ebenso vorgesehen werden, wenn ein vom für die Verarbeitung Verantwortlichen benannten Datenschutzbeauftragter sicherstellt, daß eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen durch die Verarbeitung nicht zu erwarten ist. Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muß seine Aufgaben in vollständiger Unabhängigkeit ausüben können.

(50) Die Befreiung oder Vereinfachung kann vorgesehen werden für Verarbeitungen, deren einziger Zweck das Führen eines Registers ist, das gemäß einzelstaatlichem Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht.

(51) Die Vereinfachung oder Befreiung von der Meldepflicht entbindet jedoch den für die Verarbeitung Verantwortlichen von keiner der anderen sich aus dieser Richtlinie ergebenden Verpflichtungen.

(52) In diesem Zusammenhang ist die nachträgliche Kontrolle durch die zuständigen Stellen im allgemeinen als ausreichende Maßnahme anzusehen.

(53) Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung – wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen – oder





aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen. Es obliegt den Mitgliedstaaten, derartige Risiken in ihren Rechtsvorschriftren aufzuführen, wenn sie dies wünschen.

(54) Bei allen in der Gesellschaft durchgeführten Verarbeitungen sollte die Zahl der Verarbeitungen mit solchen besonderen Risiken sehr beschränkt sein. Die Mitgliedstaaten müssen für diese Verarbeitungen vorsehen, daß vor ihrer Durchführung eine Vorabprüfung durch die Kontrollstelle oder in Zusammenarbeit mit ihr durch den Datenschutzbeauftragten vorgenommen wird. Als Ergebnis dieser Vorabprüfung kann die Kontrollstelle gemäß einzelstaatlichem Recht eine Stellungnahme abgeben oder die Verarbeitung genehmigen. Diese Prüfung kann auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

(55) Für den Fall der Mißachtung der Rechte der betroffenen Personen durch den für die Verarbeitung Verantwortlichen ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen. Mögliche Schäden, die den Personen aufgrund einer unzulässigen Verarbeitung entstehen, sind von dem für die Verarbeitung Verantwortlichen zu ersetzen, der von seiner Haftung befreit werden kann, wenn er nachweist, daß der Schaden ihm nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt. Unabhängig davon, ob es sich um eine Person des Privatrechts oder des öffentlichen Rechts handelt, müssen Sanktionen jede Person treffen, die die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht einhält.

(56) Grenzüberschreitender Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels notwendig. Der in der Gemeinschaft durch diese Richtlinie gewährte Schutz von Personen steht der Übermittlung personenbezogener Daten in Drittländer, die ein angemessenes Schutzniveau aufweisen, nicht entgegen. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlungen oder eine Kategorie von Übermittlung zu beurteilen.

(57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.

(58) Ausnahmen von diesem Verbot sind unter bestimmten Voraussetzungen vorzusehen, wenn die betroffene Person ihre Einwilligung erteilt hat oder die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel bei internationalem Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind. Ebenso kann eine Übermittlung aus einem gesetzlich vorgesehenen Register erfolgen, das der öffentlichen Einsichtnahme oder der Einsichtnahme durch Personen mit berechtigtem Interesse dient. In diesem Fall sollte eine solche Übermittlung nicht die Gesamtheit oder ganze Kategorien der im Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, so sollte die Übermittlung nur auf Antrag dieser Person oder nur dann erfolgen, wenn diese Person die Adressaten der Übermittlung sind.

(59) Besondere Maßnahmen können getroffen werden, um das unzureichende Schutzniveau in einem Drittland auszugleichen, wenn der für die Verarbeitung Verantwortliche geeignete Sicherheiten nachweist. Außerdem sind Verfahren für die Verhandlungen zwischen der Gemeinschaft und den betreffenden Drittländern vorzusehen.

(60) Übermittlungen in Drittstaaten dürfen auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften erfolgen, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gemäß Artikel 8, erlassen haben.

(61) Die Mitgliedstaaten und die Kommission müssen in ihren jeweiligen Zuständigkeitsbereichen die betroffenen Wirtschaftskreise ermutigen, Verhaltensregeln auszuarbeiten, um unter Berücksichtigung der Besonderheiten der Verarbeitung in besimmten Bereichen die Durchführung dieser Richtlinie im Einklang mit den hierfür vorgesehenen einzelstaatlichen Bestimmungen zu fördern.

(62) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung pesonenbezogener Daten.

(63) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden, sowie Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in dem Mitgliedstaat beizutragen, dem sie unterstehen.

(64) Die Behörden der verschiedenen Mitgliedstaaten werden einander bei der Wahrnehmung ihrer Aufgaben unterstützen müssen, um sicherzustellen, daß die Schutzregeln in der ganzen Europäischen Union beachtet werden.

(65) Auf Gemeinschaftsebene ist eine Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten einzusetzen, die ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Unter Berücksichtigung dieses besonderen Charakters hat sie die Kommission zu beraten und insbesondere zur einheitlichen Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften beizutragen.

(66) Für die Übermittlung von Daten an Drittländer ist es zur Anwendung dieser Richtlinie erforderlich, der Kommission Durchführungsbefugnisse zu übertragen und ein Verfahren gemäß den Bestimmungen des Beschlusses 87/373/EWG des Rates[1] festzulegen.

(67) Am 20. Dezember 1994 wurde zwischen dem Europäischen Parlament, dem Rat und der Kommission ein Modus vivendi betreffend die Maßnahmen zur Durchführung der nach dem Verfahren des Artikels 189 b des EG-Vertrags erlassenen Rechtsakte vereinbart.

(68) Die in dieser Richtlinie enthaltenen Grundsätze des Schutzes der Rechte und Freiheiten der Personen und insbesondere der Achtung der Privatsphäre bei der Verarbeitung personenbezogener Daten können – besonders für bestimmte Bereiche – durch spezifische Regeln ergänzt oder präzisiert werden, die mit diesen Grundsätzen in Einklang stehen.

(69) Den Mitgliedstaatesn sollte eine Frist von längstens drei Jahren ab Inkrafttreten ihrer Vorschriften zur Umsetzung dieser Richtlinie eingeräumt werden, damit sie die neuen einzelstaatlichen Vorschriften fortschreitend auf alle bereits laufenden Verarbeitungen anwenden können. Um eine kosteneffiziente Durchführung dieser Vorschriften zu erleichtern, wird den Mitgliedstaaten eine weitere Frist von zwölf Jahren nach Annahme dieser Richtlinie eingeräumt, um die Anpassung bestehender manueller Dateien an bestimmte Vorschriften dieser Richtlinie sicherzustellen. Werden in solchen Dateien enthaltene Daten während dieser erweiterten Umsetzungsfrist manuell verarbeitet, so sollten die Dateien zum Zeitpunkt der Verarbeitung mit diesen Vorschriften in Einklag gebracht werden.

(70) Die betroffene Person braucht nicht erneut ihre Einwilligung zu geben, damit der Verantwortliche nach Inkrafttreten der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie eine Verarbeitung sensibler Daten fortführen kann, die für die Erfüllung eines in freier Willenserklärung geschlossenen Vertrags erforderlich ist, und vor Inkrafttreten der genannten Vorschriften mitgeteilt wurde.

(71) Diese Richtlinie steht den gesetzlichen Regelungen eines Mitgliedstaats im Bereich der geschäftsmäßigen Werbung gegenüber in seinem Hoheitsgebiet ansässigen Verbrauchern nicht entgegen, sofern sich diese gesetzlichen Regelungen nicht auf den Schutz der Person bei der Verarbeitung personenbezogener Daten beziehen.

(72) Diese Richtlinie erlaubt bei der Umsetzung der mit ihr festgelegten Grundsätze die Berücksichtigung des Grundsatzes des öffentlichen Zugangs zu amtlichen Dokumenten –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

## KAPITEL I – ALLGEMEINE BESTIMMUNGEN

### Artikel 1 – Gegenstand der Richtlinie

(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.

### Artikel 2 – Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

b) „Verarbeitung personenbezogener Daten" („Verarbeitung") jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

1 ABl. Nr. L 197 vom 18. 7. 1987 S. 33.

c) „Datei mit personenbezogenen Daten“ („Datei“) jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;

d) „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;

e) „Auftragsverarbeiter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

f) „Dritter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

g) „Empfänger“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;

h) „Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, daß personenbezogene Daten, die sie betreffen, verarbeitet werden.

Artikel 3 – Anwendungsbereich

(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

- die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;
- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.





Artikel 4 – Anwendbares einzelstaatliches Recht

(1) Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erläßt, auf alle Verarbeitungen personenbezogener Daten an,

a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;

b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;

c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, daß diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

(2) In dem in Absatz 1 Buchstabe c genannten Fall hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

## KAPITEL II – ALLGEMEINE BEDINGUNGEN FÜR DIE RECHTMÄSSIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 5

Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

### ABSCHNITT I – GRUNDSÄTZE IN BEZUG AUF DIE QUALITÄT DER DATEN

Artikel 6

(1) Die Mitgliedstaaten sehen vor, daß personenbezogene Daten

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

d) sachlich richtig und, wenn nötig, auf den neusten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

## ABSCHNITT II – GRUNDSÄTZE IN BEZUG AUF DIE ZULÄSSIGKEIT DER VERARBEITUNG VON DATEN

### Artikel 7

Die Mitgliedstaaten sehen vor, daß die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;

e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;

f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

## ABSCHNITT III – BESONDERE KATEGORIEN DER VERARBEITUNG

### Artikel 8 – Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.





(2) Absatz 1 findet in folgenden Fällen keine Anwendung:

a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden;

oder

b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist;

oder

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;

oder

d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, daß sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden;

oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

(3) Absatz 1 gilt nicht, wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

(4) Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.

(5) Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.

Die Mitgliedstaaten können vorsehen, daß Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.

(6) Die in den Absätzen 4 und 5 vorgesehenen Abweichungen von Absatz 1 sind der Kommission mitzuteilen.

(7) Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.

Artikel 9 – Verarbeitung personenbezogener Daten und Meinungsfreiheit

Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.

## ABSCHNITT IV – INFORMATION DER BETROFFENEN PERSON

Artikel 10 – Information bei der Erhebung personenbezogener Daten bei der betroffenen Person

Die Mitgliedstaaten sehen vor, daß die Person, bei der die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls eines Vertreters,

b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,

c) weitere Informationen, beispielsweise betreffend

- die Empfänger oder Kategorien der Empfänger der Daten,
- die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,
- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Artikel 11 – Informationen für den Fall, daß die Daten nicht bei der betroffenen Person erhoben wurden

(1) Für den Fall, daß die Daten nicht bei der betroffenen Person erhoben wurden, sehen die Mitgliedstaaten vor, daß die betroffene Person bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:





a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls eines Vertreters,

b) Zweckbestimmungen der Verarbeitung,

c) weitere Informationen, beispielsweise betreffend

- die Datenkategorien, die verarbeitet werden,
- die Empfänger oder Kategorien der Empfänger der Daten,
- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(2) Absatz 1 findet – insbesondere bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung – keine Anwendung, wenn die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. In diesen Fällen sehen die Mitgliedstaaten geeignete Garantien vor.

## ABSCHNITT V – AUSKUNFTSRECHT DER BETROFFENEN PERSON

Artikel 12 – Auskunftsrecht

Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen folgendes zu erhalten:

a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten

- die Bestätigung, daß es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;
- eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;
- Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne von Artikel 15 Absatz 1;

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;

c) die Gewähr, daß jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

## ABSCHNITT VI – AUSNAHMEN UND EINSCHRÄNKUNGEN

### Artikel 13 – Ausnahmen und Einschränkungen

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

a) die Sicherheit des Staates;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;

e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;

f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c, d und e genannten Zwecke verbunden sind;

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

(2) Vorbehaltlich angemessener rechtlicher Garantien, mit denen insbesondere ausgeschlossen wird, daß die Daten für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden, können die Mitgliedstaaten in Fällen, in denen offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht, die in Artikel 12 vorgesehenen Rechte gesetzlich einschränken, wenn die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet werden oder personenbezogen nicht länger als erforderlich lediglich zur Erstellung von Statistiken aufbewahrt werden.

## ABSCHNITT VII – WIDERSPRUCHSRECHT DER BETROFFENEN PERSON

### Artikel 14 – Widerspruchsrecht der betroffenen Person

Die Mitgliedstaaten erkennen das Recht der betroffenen Person an,

a) zumindest in den Fällen von Artikel 7 Buchstaben e und f jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen Widerspruch einlegen zu können, daß sie betreffende Daten verarbeitet werden; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen;

b) auf Antrag kostenfrei gegen eine vom für die Verarbeitung Verantwortlichen beabsichtigte Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen oder vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor deren erstmaliger Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden und ausdrücklich auf das Recht hingewiesen zu





werden, kostenfrei gegen eine solche Weitergabe oder Nutzung Widerspruch einlegen zu können. Die Mitgliedstaaten ergreifen die erforderlichen Maßnahmen, um sicherzustellen, daß die betroffenen Personen vom Bestehen des unter Buchstabe b Unterabsatz 1 vorgesehenen Rechts Kenntnis haben.

### Artikel 15 – Automatisierte Einzelentscheidungen

(1) Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

(2) Die Mitgliedstaaten sehen unbeschadet der sonstigen Bestimmungen dieser Richtlinie vor, daß eine Person einer Entscheidung nach Absatz 1 unterworfen werden kann, sofern diese

a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags ergeht und dem Ersuchen der betroffenen Person auf Abschluß oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen – beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen – garantiert wird

oder

b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

## ABSCHNITT VIII – VERTRAULICHKEIT UND SICHERHEIT DER VERARBEITUNG

### Artikel 16 – Vertraulichkeit der Verarbeitung

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

### Artikel 17 – Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(2) Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.

(3) Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere folgendes vorgesehen ist:

- der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen;
- die in Absatz 1 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

(4) Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in bezug auf Maßnahmen nach Absatz 1 schriftlich oder in einer anderen Form zu dokumentieren.

## ABSCHNITT IX – MELDUNG

### Artikel 18 – Pflicht zur Meldung bei der Kontrollstelle

(1) Die Mitgliedstaaten sehen eine Meldung durch den für die Verarbeitung Verantwortlichen oder gegebenenfalls seinen Vertreter bei der in Artikel 28 genannten Kontrollstelle vor, bevor eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen durchgeführt wird.

(2) Die Mitgliedstaaten können eine Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht nur in den folgenden Fällen und unter folgenden Bedingungen vorsehen:

- sie legen für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung fest, und/oder
- der für die Verarbeitung Verantwortliche bestellt entsprechend dem einzelstaatlichen Recht, dem er unterliegt, einen Datenschutzbeauftragten, dem insbesondere folgendes obliegt:
- die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen,
- die Führung eines Verzeichnisses mit den in Artikel 21 Absatz 2 vorgesehenen Informationen über die durch den für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung, um auf diese Weise sicherzustellen, daß die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht beeinträchtigt werden.





(3) Die Mitgliedstaaten können vorsehen, daß Absatz 1 keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines Registers ist, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht.

(4) Die Mitgliedstaaten können die in Artikel 8 Absatz 2 Buchstabe d) genannten Verarbeitungen von der Meldepflicht ausnehmen oder die Meldung vereinfachen.

(5) Die Mitgliedstaaten können die Meldepflicht für nicht automatisierte Verarbeitungen von personenbezogenen Daten generell oder in Einzelfällen vorsehen oder sie einer vereinfachten Meldung unterwerfen.

### Artikel 19 – Inhalt der Meldung

(1) Die Mitgliedstaaten legen fest, welche Angaben die Meldung zu enthalten hat. Hierzu gehört zumindest folgendes:

a) Name und Anschrift des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

b) die Zweckbestimmung(en) der Verarbeitung;

c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

d) die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;

e) eine geplante Datenübermittlung in Drittländer;

f) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

(2) Die Mitgliedstaaten legen die Verfahren fest, nach denen Änderungen der in Absatz 1 genannten Angaben der Kontrollstelle zu melden sind.

### Artikel 20 – Vorabkontrolle

(1) Die Mitgliedstaaten legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, daß diese Verarbeitungen vor ihrem Beginn geprüft werden.

(2) Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muß.

(3) Die Mitgliedstaaten können eine solche Prüfung auch im Zuge der Ausarbeitung einer Maßnahme ihres Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchführen, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

Artikel 21 – Öffentlichkeit der Verarbeitungen

(1) Die Mitgliedstaaten erlassen Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird.

(2) Die Mitgliedstaaten sehen vor, daß die Kontrollstelle ein Register der gemäß Artikel 18 gemeldeten Verarbeitungen führt. Das Register enthält mindestens die Angaben nach Artikel 19 Absatz 1 Buchstaben a bis e. Das Register kann von jedermann eingesehen werden.

(3) Die Mitgliedstaaten sehen vor, daß für Verarbeitungen, die von der Meldung ausgenommen sind, der für die Verarbeitung Verantwortliche oder eine andere von den Mitgliedstaaten benannte Stelle zumindest die in Artikel 19 Absatz 1 Buchstaben a) bis e) vorgesehenen Angaben auf Antrag jedermann in geeigneter Weise verfügbar macht. Die Mitgliedstaaten können vorsehen, daß diese Bestimmungen keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen von Registern ist, die gemäß den Rechts- und Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt sind und die entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offenstehen.

## KAPITEL III – RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 22 – Rechtsbehelfe

Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, daß jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.

Artikel 23 – Haftung

(1) Die Mitgliedstaaten sehen vor, daß jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.

(2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

Artikel 24 – Sanktionen

Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind.





## KAPITEL IV – ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Artikel 25 – Grundsätze

(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

(4) Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, daß ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.

(5) Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gemäß Absatz 4 festgestellte Lage zu schaffen.

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, daß ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet. Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

Artikel 26 – Ausnahmen

(1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, daß eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern

a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder

b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder

c) die Übermittlung zum Abschluß oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder

e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder

f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.

(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten über die von ihm nach Absatz 2 erteilten Genehmigungen. Legt ein anderer Mitgliedstaat oder die Kommission einen in bezug auf den Schutz der Privatsphäre, der Grundrechte und der Personen hinreichend begründeten Widerspruch ein, so erläßt die Kommission die geeigneten Maßnahmen nach dem Verfahren des Artikels 31 Absatz 2. Die Mitgliedstaaten treffen die aufgrund des Beschlusses der Kommission gebotenen Maßnahmen.

(4) Befindet die Kommission nach dem Verfahren des Artikels 31 Absatz 2, daß bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Absatz 2 bieten, so treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

## KAPITEL V – VERHALTENSREGELN

### Artikel 27

(1) Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

(2) Die Mitgliedstaaten sehen vor, daß die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können. Die Mitgliedstaaten sehen vor, daß sich diese Stelle insbesondere davon überzeugt, daß die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Die Stelle





holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint.

(3) Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, daß die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.

## KAPITEL VI – KONTROLLSTELLE UND GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

### Artikel 28 – Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, daß eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, daß die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;
- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;
- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie. Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde. Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befaßt werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, daß eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden. Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, daß die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

Artikel 29 – Datenschutzgruppe

(1) Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend „Gruppe“ genannt). Die Gruppe ist unabhängig und hat beratende Funktion.

(2) Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission. Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.

(3) Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.

(4) Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

(5) Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

(6) Die Gruppe gibt sich eine Geschäftsordnung.

(7) Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.

Artikel 30

(1) Die Gruppe hat die Aufgabe,

a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;

b) zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;





c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;

d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.

(2) Stellt die Gruppe fest, daß sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen könnten, so teilt sie dies der Kommission mit.

(3) Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.

(4) Die Stellungnahmen und Empfehlungen der Gruppe werden der Kommission und dem in Artikel 31 genannten Ausschuß übermittelt.

(5) Die Kommission teilt der Gruppe mit, welche Konsequenzen sie aus den Stellungnahmen und Empfehlungen gezogen hat. Sie erstellt hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht.

(6) Die Gruppe erstellt jährlich einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, den sie der Kommission, dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht.

KAPITEL VII – GEMEINSCHAFTLICHE DURCHFÜHRUNGSMASSNAHMEN

Artikel 31 – Ausschußverfahren

(1) Die Kommission wird von einem Ausschuß unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

(2) Der Vertreter der Kommission unterbreitet dem Ausschuß einen Entwurf der zu treffenden Maßnahmen. Der Ausschuß gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann. Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 148 Absatz 2 des Vertrags vorgesehen ist. Bei der Abstimmung im Ausschuß werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil. Die Kommission erläßt Maßnahmen, die unmittelbar gelten. Stimmen sie jedoch mit der Stellungnahme des Ausschusses nicht überein, werden sie von der Kommission unverzüglich dem Rat mitgeteilt. In diesem Fall gilt folgendes:

- Die Kommission verschiebt die Durchführung der von ihr beschlossenen Maßnahmen um drei Monate vom Zeitpunkt der Mitteilung an;
- der Rat kann innerhalb des im ersten Gedankenstrich genannten Zeitraums mit qualifizierter Mehrheit einen anderslautenden Beschluß fassen.

SCHLUSSBESTIMMUNGEN

Artikel 32

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen. Wenn die Mitgliedstaaten derartige Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß Verarbeitungen, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits begonnen wurden, binnen drei Jahren nach diesem Zeitpunkt mit diesen Bestimmungen in Einklang gebracht werden. Abweichend von Unterabsatz 1 können die Mitgliedstaaten vorsehen, daß die Verarbeitungen von Daten, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits in manuellen Dateien enthalten sind, binnen zwölf Jahren nach Annahme dieser Richtlinie mit den Artikeln 6, 7 und 8 in Einklang zu bringen sind. Die Mitgliedstaaten gestatten jedoch, daß die betroffene Person auf Antrag und insbesondere bei Ausübung des Zugangsrechts die Berichtigung, Löschung oder Sperrung von Daten erreichen kann, die unvollständig, unzutreffend oder auf eine Art und Weise aufbewahrt sind, die mit den vom für die Verarbeitung Verantwortlichen verfolgten rechtmäßigen Zwecken unvereinbar ist.

(3) Abweichend von Absatz 2 können die Mitgliedstaaten vorbehaltlich geeigneter Garantien vorsehen, daß Daten, die ausschließlich zum Zwecke der historischen Forschung aufbewahrt werden, nicht mit den Artikeln 6, 7 und 8 in Einklang gebracht werden müssen.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 33

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig, und zwar erstmals drei Jahre nach dem in Artikel 32 Absatz 1 genannten Zeitpunkt, einen Bericht über die Durchführung dieser Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei. Dieser Bericht wird veröffentlicht. Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten.

Artikel 34

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.





## II. 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

This is an unofficial text. For the authoritative text of the Directive, reference should be made to the Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

**Contents**

**Recitals**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and inparticular Article 100 a thereof,

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the Economic and Social Committee[2],

Acting in accordance with the procedure referred to in Article 189 b of the Treaty[3].

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress bycommon action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and thewell-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7 a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7 a of the Treaty will necessarily lead to a substantial increase incross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform theirduties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted bythe internal market;

1 OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.
2 OJ No C 159, 17. 6. 1991, p. 38.
3 Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(6) Whereas, furthermore, the increase in scientific and technical co-operation and the co-ordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community-level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a highlevel of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by anatural person in the exercise of activities





which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on the European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100 a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection,processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, inparticular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can becarried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, none the less, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the differentcriteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;





(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certainhealth-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection – especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system – scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e. g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data ist to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy ot the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;





(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exeptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, *ex post facto* verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in co-operation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of *force majeure;* whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a





transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third contries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC[1];

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189 b of the EC Treary was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and feedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

1 OJ No. 1, 197, 18. 7. 1987, p. 33.

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

## CHAPTER I GENERAL PROVISIONS

### Article 1 Object of the Directive

(1) In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

(2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

### Article 2 Definitions

For the purposes of this Directive:

a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;





c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

h) 'the data subject's consent' shall mean 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.

### Article 3 Scope

(1) This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise 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 Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

### Article 4 National law applicable

(1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

(2) In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

## CHAPTER II – GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

### Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

## SECTION I – PRINCIPLES RELATING TO DATA QUALITY

### Article 6

(1) Member States shall provide that personal data must be:

a) processed fairly and lawfully;

b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

(2) It shall be for the controller to ensure that paragraph 1 is complied with.

## SECTION II – CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

### Article 7

Member States shall provide that personal data may be processed only if:

a) the data subject has unambiguously given his consent; or





b) 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; or

c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

d) processing is necessary in order to protect the vital interests of the data subject; or

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

## SECTION III – SPECIAL CATEGORIES OF PROCESSING

### Article 8 The processing of special categories of data

(1) Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

(2) Paragraph 1 shall not apply where:

a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

(3) Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

(4) Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

(5) Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

(6) Derogations from paragraph I provided for in paragraphs 4 and 5 shall be notified to the Commission.

(7) Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9 Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV – INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10 Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

a) the identity of the controller and of his representative, if any;

b) the purposes of the processing for which the data are intended;

c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 Information where the data have not been obtained from the data subject

(1) Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:





a) the identity of the controller and of his representative, if any;

b) the purposes of the processing;

c) any further information such as

- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(2) Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V – THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12 Right of access

Member States shall guarantee every data right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI – EXEMPTIONS AND RESTRICTIONS

Article 13

(1) Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred toin (c), (d) and (e);

g) the protection of the data subject or of the rights and freedoms of others.

(2) Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

## SECTION VII – THE DATA SUBJECT'S RIGHT TO OBJECT

### Article 14 The data subject's right to object

Member States shall grant the data subject the right:

a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

### Article 15 Automated individual decisions

(1) Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, credit-worthiness, reliability, conduct, etc.

(2) Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:





a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

## SECTION VIII – CONFIDENTIALITY AND SECURITY OF PROCESSING

### Article 16 Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

### Article 17 Security of processing

(1) Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

(2) The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

(3) The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

(4) For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

## SECTION IX – NOTIFICATION

### Article 18 – Obligation to notify the supervisory authority

(1) Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

(2) Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

(3) Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

(4) Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

(5) Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19 – Contents of notification

(1) Member States shall specify the information to be given in the notification. It shall include at least:

a) the name and address of the controller and of his representative, if any;

b) the purpose or purposes of the processing;

c) a description of the category or categories of data subject and of the data or categories of data relating to them;

d) the recipients or categories of recipient to whom the data might be disclosed;

e) proposed transfers of data to third countries;

f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

(2) Member States shall specify the procedures under which any change affecting the information referred to in paragraph I must be notified to the supervisory authority.





Article 20 Prior checking

(1) Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

(2) Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

(3) Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21 – Publicizing of processing operations

(1) Member States shall take measures to ensure that processing operations are publicized.

(2) Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

(3) Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide provide of a legitimate interest.

## CHAPTER III – JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22 Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23 Liability

(1) Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

(2) The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

## CHAPTER IV – TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 Principles

(1) The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures anadequate level of protection,

(2) The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose 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.

(3) The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

(4) Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

(5) At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

(6) The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 Derogations

(1) By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

a) the data subject has given his consent unambiguously to the proposed transfer; or





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; or

c) the transfer is necessary for the conclusion or performance of acontract concluded in the interest of the data subject between the controller and a third party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or

f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

(2) Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

(3) The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary to comply with the Commission's decision.

(4) Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

## CHAPTER V – CODES OF CONDUCT

Article 27

(1) The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

(2) Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

(3) Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

## CHAPTER VI – SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

### Article 28 Supervisory authority

(1) Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

(2) Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

(3) Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

(4) Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.





(5) Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

(6) Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

(7) Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

### Article 29 – Working Party on the Protection of Individuals with regard to the Processing of Personal Data

(1) A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

(2) The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a join trepresentative. The same shall apply to the authorities established for Community institutions and bodies.

(3) The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

(4) The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

(5) The Working Party's secretariat shall be provided by the Commission.

(6) The Working Party shall adopt its own rules of procedure.

(7) The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of are presentative of the supervisory authorities or at the Commission's request.

### Article 30

(1) The Working Party shall:

a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

b) give the Commission an opinion on the level of protection in the Community and in third countries;

c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

d) give an opinion on codes of conduct drawn up at Community level.

(2) If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

(3) The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

(4) The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

(5) The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

(6) The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

## CHAPTER VII – COMMUNITY IMPLEMENTING MEASURES

### Article 31 – The Committee

(1) The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

(2) The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.





## FINAL PROVISIONS

### Article 32

(1) Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

(2) Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

(3) By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

(4) Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

### Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

### Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

# E. Vereinigte Staaten von Amerika / United States of America

## I. Privatsphäre und Nationale Informations-Infrastruktur: Grundsätze für die Bereitstellung und Nutzung personenbezogener Informationen

– Übersetzung –

Privacy Working Group
Information Policy Committee
Information Infrastructure Task Force

Endgültige Fassung
6. Juni 1995

### Einleitung

Die Nationale Informations-Infrastruktur (NII), die eine nahtlose Vernetzung von Kommunikationsnetzen, Computern, Datenbanken und Unterhaltungselektronik verspricht, kündigt das Herannahen des Informationszeitalters an. Die Möglichkeit, Informationen zu akzeptablen Kosten zu erwerben, zu verarbeiten, zu übermitteln und zu speichern, ist niemals größer gewesen; die fortdauernde Verbesserung der Computer- und Telekommunikationstechnologien wird zu einem fortlaufenden Anwachsen der Erzeugung, Nutzung und Speicherung von Informationen führen.

Die Nationale Informations-Infrastruktur verspricht enorme Vorteile. Sie eröffnet – um nur einige davon zu nennen – Möglichkeiten einer größeren Bürgerbeteiligung in der diskursorientierten Demokratie, Fortschritte in der Medizin und der medizinischen Forschung und die schnelle Verifikation von sensiblen Informationen, wie z. B. dem Vorstrafenregister eines Waffenkäufers. Diese Vorteile haben jedoch ihren Preis: den Verlust der Privatsphäre. Privatsphäre bedeutet in diesem Zusammenhang „informationelle Privatsphäre“, also den Anspruch des einzelnen, die Bedingungen zu kontrollieren, unter denen persönliche Informationen – Informationen, die einem Individuum zugeordnet werden können – erworben, übermittelt und genutzt werden.

Zwei konvergierende Trends – der eine ein sozialer, der andere ein technologischer Trend – führen zu einer verstärkten Gefährdung der Privatsphäre in der sich entwickelnden NII. Als sozialer Trend werden die einzelnen die NII nutzen, um miteinander zu kommunizieren, Waren und Dienstleistungen zu bestellen und Informationen zu beziehen. Die Nutzung der NII für solche Zwecke wird jedoch, anders als die Barzahlung beim Kauf einer Zeitschrift, zum Entstehen von Daten führen, die die Transaktion dokumentieren und die leicht gespeichert, ausgewertet, analysiert und wiederverwendet werden können. Tatsächlich könnte aus den Verbindungsdaten der NII sowohl darauf geschlossen werden, wer wann und für wie lange kommuniziert hat, als auch, wer was und für welchen Preis

gekauft hat. Typischerweise wird diese Art von persönlichen Informationen automatisch in elektronischer Form generiert und kann daher zu sehr geringen Kosten gespeichert und verarbeitet werden.

Der technologische Trend besteht darin, daß die Fähigkeiten von Hardware, Software und Kommunikationsnetzen kontinuierlich zunehmen, während die Kosten dafür kontinuierlich zurückgehen und eine Nutzung von Information in einer Art erlauben, die vorher unmöglich oder unwirtschaftlich war. Ohne die NII mußte man z. B., um ein Benutzerprofil einer Person zu erstellen, die in verschiedenen Bundesstaaten gewohnt hat, von Bundesstaat zu Bundesstaat fahren und öffentliche Register nach Informationen über diese Person durchsuchen. Dieser Vorgang erfordert das Ausfüllen von Formularen, die Zahlung von Gebühren und das Schlangestehen für die Akteneinsicht bei kommunalen Behörden, Landes- und Bundesbehörden, wie der Kfz-Zulassungsstelle, den Grundbuchämtern, den Wahlkommissionen und den Bezirksarchiven. Obwohl man auf diese Art manuell ein Persönlichkeitsprofil zusammenstellen könnte, wäre dies ein zeitaufwendiger und teurer Vorgang, der nicht unternommen werden würde, wenn man sich nicht einen angemessenen Erfolg versprechen würde. Im Gegensatz dazu kann heute, da mehr und mehr persönliche Informationen elektronisch lesbar zur Verfügung stehen, ein solches Profil zu geringen Kosten in wenigen Minuten erstellt werden.

Diese beiden zusammenhängenden Trends werden mit Sicherheit dazu führen, daß im Zusammenhang mit der Entwicklung der NII mehr personenbezogene Informationen entstehen und in größerem Maße genutzt werden. Hierin liegt das zunehmende Risiko für die Privatsphäre. Dieses Risiko muß angesprochen werden, sowohl um den Wert der Privatsphäre für den einzelnen und die Gesellschaft sicherzustellen, als auch, um dafür zu sorgen, daß die NII ihr volles Potential erreichen wird. Wenn dies nicht getan wird, könnten die Bürger aus Angst, daß die Nachteile für den Schutz ihrer personenbezogenen Daten die Vorteile der NII überwiegen könnten, nicht daran teilnehmen. Die Einführung von Prinzipien für den fairen Umgang mit Informationen ist ein wichtiger erster Schritt, um dieser Besorgnis entgegenzuwirken.

Obwohl entsprechende gesetzliche Regelungen und Prinzipien bereits existieren, müssen diese angepaßt werden, um die sich entwickelnde Informationsumgebung (information environment) abzudecken. Diese sich verändernden Rahmenbedingungen sind mit neuen Gefährdungen verbunden.

- Die Sammlung und Nutzung großer Mengen von personenbezogenen Informationen erfolgt nicht mehr durch Regierungsstellen allein; der private Bereich fängt an, im Hinblick auf die Sammlung und die Nutzung personenbezogener Informationen mit der Regierung zu konkurrieren. Neue Prinzipien würden damit unvollständig bleiben, falls sie nicht sowohl auf den öffentlichen als auch auf den privaten Bereich anwendbar wären.

- Die NII verspricht wirkliche Interaktivität. Die einzelnen werden zu aktiven Teilnehmern, die sowohl große Mengen von Inhalts- als auch von Verbindungsdaten erzeugen werden.

- Die Transporteinrichtungen für persönliche Information – die Netze – können mißbraucht werden; daher ist die Sicherheit der Netze selbst für den zukünftigen Erfolg der NII entscheidend.





- Die sich schnell entwickelnde Informationsumgebung macht in manchen Fällen die Anwendung traditioneller ehtischer Regeln schwierig, selbst wenn es sich um solche handelt, die beim Umgang mit greifbaren Akten und Dokumenten allgemein verstanden und akzeptiert werden. Man denke z. B. nur daran, wie jemand, der niemals in das Haus eines anderen eindringen würde, das Einbrechen in dessen Computer als eine intellektuelle Übung betrachten könnte. Zusätzlich kann die heutige Informationsumgebung Fragen über die Nutzung persönlicher Informationen aufwerfen, die in traditionellen Regelungen nicht einmal erwähnt werden.

Diese „Prinzipien für die Bereitstellung und Nutzung personenbezogener Informationen“ („die Prinzipien“) werden als Antwort auf diese neue Informationsumgebung angeboten. Die Prinzipien, angesiedelt zwischen abstrakten Begriffen und detaillierten Regelungen, sollen eine sinnvolle Linie bieten. Sie sind für alle Teilnehmer an der NII gedacht und sollten von denen genutzt werden, die Gesetze und Vorschriften entwerfen, Regelungen für faire Informationspraktiken in der Industrie schaffen und Vorhaben im öffentlichen und privaten Bereich planen, bei denen personenbezogene Informationen genutzt werden.

Man muß sich über die dieser Art von Prinzipien innewohnenden Grenzen klar sein. Die Prinzipien haben keine Gesetzeskraft und schaffen kein materielles oder prozedurales Recht, das gerichtlich durchgesetzt werden kann. Sie sind weder dazu gedacht, spezifische Antworten auf alle denkbaren Fragen zu geben, noch als pauschale Regelung für die verschiedenen Sektoren, in denen personenbezogene Informationen genutzt werden. Die Prinzipien sollten als Ganzes pragmatisch und vernünftig verstanden und angewandt werden. Zum Beispiel sollten die, die diese Prinzipien anwenden, folgendes in Erwägung ziehen:

- den Nutzen, den die Gesellschaft durch die Nutzung personenbezogener Informationen hat, unter der Berücksichtigung der Tatsache, daß der Schutz der Privatsphäre des einzelnen nicht absolut ist und mit der Notwendigkeit einer gesetzlichen Haftung, der Anwendung des ersten Zusatzes (der amerikanischen Verfassung betreffend die Meinungs- und Pressefreiheit; Anm. d. Übers.), den Erfordernissen der Strafverfolgung und anderem in Gesetzen anerkannten gesellschaftlichen Nutzen abgewogen werden;

- das Ausmaß, bis zu dem die Entscheidung, personenbezogene Informationen preiszugeben, freiwillig ist, und die Erwartungen des einzelnen bezüglich der Nutzung dieser Informationen (unter Berücksichtigung der Aufklärung und des Umfangs der gegebenen Einwilligung);

- die Sensibilität der Information und das Schadenspotential für den einzelnen, das aus einer bestimmten Weitergabe oder Nutzung der Information entstehen könnte;

- den Aufwand und die Kosten, die notwendig sind, um Schäden für den Einzelnen vorzubeugen, unter Berücksichtigung der Tatsache, daß ein Mehr an sensiblen Informationen teurere und aufwendigere Schutzmaßnahmen als weniger sensible Informationen notwendig machen könnte.

Dort, wo eine allzu mechanische Anwendung der Prinzipien besonders ungerechtfertigt erscheint, enthält der Text Formulierungen, die die Worte „angemessen“ oder „berechtigt“ enthalten. Diese Unbestimmtheit, die in die Prinzipien eingefügt wurde, um schwierige oder unvorhergesehene Fälle zu behandeln, bedeutet nicht, daß die Prinzipien nicht

strikt eingehalten werden sollen. Schließlich sollen die Prinzipien dem Geist von gegenwärtig existierenden internationalen Regelungen, wie den Richtlinien der OECD über die Nutzung personenbezogener Informationen[1], entsprechen. Die Prinzipien sollen zu weiterer internationaler Kooperation über die Entwicklung und Harmonisierung von globalen Datenschutzregelungen anregen, deren Einhaltung die weitere Entwicklung der globalen Informations-Infrastruktur voranbringen wird.

**Präambel**

Die Vereinigten Staaten engagieren sich für die Errichtung einer Nationalen Informations-Infrastruktur (NII), um den Informationsbedürfnissen ihrer Bevölkerung zu entsprechen. Diese Infrastruktur, die durch technologische Fortschritte möglich wird, erweitert den Grad der Interaktivität, verbessert die Kommunikation und erlaubt einen einfacheren Zugriff auf Dienstleistungen. Als Ergebnis dessen werden viel mehr Nutzer neue, früher unvorstellbare Möglichkeiten entdecken, personenbezogene Informationen zu beschaffen und zu nutzen. In diesem Umfeld sind wir aufgefordert, neue Prinzipien zu entwickeln, um alle neuen Teilnehmer der NII beim fairen Gebrauch personenbezogener Informationen anzuleiten.

Existierende Regelungen über faire Informationspraktiken müssen in ein neues Umfeld umgesetzt werden, in dem Informationen und Nachrichten von Benutzern über Netzwerke gesendet und empfangen werden, die sehr verschiedene Möglichkeiten, Zielvorstellungen und Interessen haben. In dieser interaktiven und vernetzten Umgebung werden viele neue Beziehungen zwischen Individuen, Anbietern von Kommunikationsdienstleistungen und anderen Teilnehmern an der NII geknüpft. Neue Prinzipien müssen berücksichtigen, daß jeder Beteiligte unterschiedliche Beziehungen mit den Einzelpersonen hat und unterschiedlichen Gebrauch von personenbezogenen Informationen macht.

Neue Prinzipien sollen nicht die bestehenden verfassungsmäßigen und gesetzlichen Grenzen für den Zugang zu Informationen, Nachrichten und Transaktionen wie die Notwendigkeit von Durchsuchungsbefehlen und Beschlagnahmeanordnungen aufweichen. Derartige Prinzipien sollten sicherstellen, daß die Begrenzung des Zugriffs mit der technologischen Entwicklung Schritt hält. Die Prinzipien sollten berücksichtigen, daß alle Teile unserer Gesellschaft Verantwortung für die faire Behandlung von Einzelpersonen im Hinblick auf die Nutzung von personenbezogenen Informationen tragen, unabhängig davon, ob auf Papier oder in elektronischer Form. Darüber hinaus sollten die Prinzipien berücksichtigen, daß die Interaktivität der NII die einzelnen in die Lage versetzen kann, selbst am Schutz ihrer personenbezogenen Informationen teilzunehmen. Die neuen Prinzipien sollten außerdem herausstellen, daß diese Verantwortung nur mit einer Aufgeschlossenheit für den Verfahrensablauf einer Verpflichtung zu Fairneß und Verantwortlichkeit und einer fortdauernden Aufmerksamkeit für die Sicherheit wahrgenommen werden kann. Schließlich sollten die Prinzipien die Notwendigkeit anerkennen, alle Beteiligten über die neue Informations-Infrastruktur aufzuklären und darüber, welche Auswirkungen sie auf ihr Leben haben wird.

1 S. o. S. 15.





Diese „Prinzipien für die Bereitstellung und Nutzung personenbezogener Informationen“ („die Prinzipien“) erkennen die sich verändernde Rolle der Regierung und der Industrie in bezug auf die Erhebung und die Nutzung von Informationen an. Sie sind daher für die Anwendung sowohl auf öffentliche als auch auf private Stellen gedacht. Die Prinzipien sollen sowohl alle Teilnehmer an der NII als auch jene, die Gesetze und Regelungen bezüglich der Nutzung personenbezogener Informationen schaffen, anleiten. Sie stellen einen Rahmen dar, aus dem bei Bedarf bereichsspezifische Prinzipien entwickelt werden können.

Bei der Umsetzung der Prinzipien werden Zielkonflikte unvermeidbar sein, da Belange des Schutzes der Privatsphäre nicht absolut gesetzt werden können und mit der Notwendigkeit für eine Verantwortlichkeit, dem Wert des ungehinderten Flusses von Informationen und anderen vom Gesetz anerkannten Nutzen wie Erfordernissen der Strafverfolgung in Einklang gebracht werden müssen. Beispielsweise sind bestimmte Entscheidungen über den Fluß personenbezogener Informationen bereits durch den ersten Zusatz (der amerikanischen Verfassung; Anm. d. Übers.) getroffen worden, und die Prinzipien sollen nichts enthalten, was Maßnahmen erforderlich machen würde, die die verfassungsmäßig geschützte Meinungs- und Pressefreiheit schmälern könnten. Angesichts dieser manchmal entgegengesetzten Interessen und öffentlichen Belange müssen die Prinzipien pragmatisch und gewissenhaft umgesetzt werden unter angemessener Berücksichtigung beispielsweise des Ausmaßes, in dem die Preisgabe personenbezogener Informationen auf freiwilliger Basis erfolgt, der Angemessenheit der Aufklärung darüber, in welcher Weise die personenbezogene Information genutzt werden soll, des Umfangs der Einwilligung des einzelnen und des Verhältnisses der Kosten für den Schutz von Information zu deren Sensibilität.

**Prinzipien und Erläuterungen**

**I. Allgemeine Prinzipien für alle NII-Teilnehmer**

1. Drei grundlegende Prinzipien sollten von allen Beteiligten der NII berücksichtigt werden. Diese drei Prinzipien – Vertraulichkeit der Information, Integrität der Information, Qualität der Information – bilden die fundamentalen Anforderungen für die richtige Nutzung personenbezogener Informationen und damit für die erfolgreiche Implementierung der NII. Alle Beteiligten an der NII sollen angemessene Maßnahmen treffen, um sicherzustellen, daß diesen Prinzipien Genüge getan wird.

**I. A. Datenschutzprinzip (Information Privacy Principle)**

**Personenbezogene Informationen sollen nur in einer Weise erhoben, offenbart und genutzt werden, die den Datenschutz des einzelnen respektieren.**

2. Die NII kann nur erfolgreich sein, wenn alle Beteiligten den Datenschutz respektieren. Datenschutz ist der Anspruch des einzelnen, die Bedingungen zu bestimmen, unter denen personenbezogene Informationen – d. h. Informationen, die auf eine einzelne Person bezogen werden können – erhoben, offenbart und genutzt werden. Das Niveau des zu gewährleistenden Datenschutzes bestimmt sich nach der berechtigten Erwartung des einzelnen, einer subjektiven Erwartung des einzel-

nen, die von der Gesellschaft als objektiv berechtigt erachtet wird. Nicht alle subjektiven Erwartungen werden als berechtigt gelten können. Eine Einzelperson, die beispielsweise eine unverschlüsselte persönliche Mitteilung in einem Mitteilungsbrett für öffentliche Mitteilungen aufgibt, kann nicht berechtigterweise erwarten, daß diese persönliche Mitteilung nur von dem, an den sie adressiert ist, gelesen wird.

3. Was im Sinne der Prinzipien als berechtigte Erwartung gilt, ist nicht dadurch beschränkt, was als eine berechtigte Erwartung an den Datenschutz hinsichtlich des vierten Änderungszusatzes der Verfassung der Vereinigten Staaten von Amerika gilt. In vielen Fällen hat die Gesellschaft es für angemessen gehalten, den Datenschutz auf einem höheren Level, als von dem vierten Änderungszusatz gefordert, zu gewährleisten. Vgl. z. B. Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1988); Privacy Act, 5 U.S.C. § 552 a (1988). Das Datenschutzprinzip unterstützt solche Möglichkeiten.

4. Wie in den späteren Prinzipien und dem Kommentar erklärt wird, kann der Datenschutz des einzelnen oft am besten berücksichtigt werden, wenn die Betroffenen und die Nutzer von Informationen zu einem gegenseitigen Einverständnis darüber kommen, wie personenbezogene Informationen erhoben, offenbart und genutzt werden sollen. Allerdings können ausschließlich vertragliche Regelungen zwischen dem Betroffenen und den Nutzern von Informationen in bestimmten Fällen für die Gewährleistung des Datenschutzes nicht ausreichend sein, z. B. wenn dem Betroffenen die notwendige Kaufkraft fehlt. Für solche Fälle sollte die Gesellschaft ein bestimmtes Grundniveau an Datenschutz sicherstellen, um dem Datenschutzprinzip zu genügen.

### I. B. Integritätsprinzip (Information Integrity Principle)

**Personenbezogene Informationen dürfen nicht unsachgemäß verändert oder gelöscht werden.**

5. Die Teilnehmer an der NII sollten sich auf die Integrität der personenbezogenen Daten, die in der NII enthalten sind, verlassen können. Daher sollten personenbezogene Informationen gegen unsachgemäße Veränderung oder Löschung geschützt werden.

### I. C. Qualitätsprinzip (Information Quality Principle)

**Personenbezogene Informationen sollen richtig, aktuell, vollständig und erforderlich für den Zweck sein, für den sie bereitgestellt und genutzt werden.**

6. Personenbezogene Informationen sollten eine hinreichende, verläßliche Qualität haben. Dies bedeutet, daß personenbezogene Informationen richtig, aktuell, vollständig und erforderlich für den Zweck sein sollten, für den sie bereitgestellt und genutzt werden.





## II. Prinzipien für Nutzer personenbezogener Daten

### II. A. Erhebungsprinzipien

**Die Nutzer von Informationen sollten:**

1. **die Auswirkungen auf den Datenschutz bei der Entscheidung über die Erhebung, Weitergabe oder Nutzung personenbezogener Informationen abschätzen;**
2. **nur solche Informationen erheben und speichern, die vernünftigerweise als geeignet für gegenwärtige oder zukünftige Aktivitäten angesehen werden.**

7. Der Vorteil von Informationen liegt in ihrer Nutzung, aber damit sind oft nicht bedachte Kosten verbunden: die Gefährdung des Datenschutzes. Eine entscheidende Eigenschaft des Datenschutzes liegt darin, daß er kaum wiederhergestellt werden kann, wenn er einmal durchbrochen worden ist. Man denke z. B. daran, bis zu welchem Ausmaß die unangemessene Veröffentlichung sensibler medizinischer Informationen durch eine öffentliche Entschuldigung zurückgenommen werden kann.

8. Aufgrund dieser Eigenschaft sollte Datenschutz nicht als nachgeordnet behandelt werden, sobald personenbezogene Daten erhoben worden sind. Die Nutzer von Informationen sollten vielmehr ausdrücklich bereits beim Entwurf von Informationssystemen und bei der Entscheidung darüber, ob personenbezogene Daten erhoben oder genutzt werden sollen, zuerst die Auswirkung auf den Datenschutz bedenken. Bei der Abschätzung dieser Auswirkung sollten die Nutzer von Informationen nicht nur den Effekt abschätzen, den ihre Aktivitäten auf die Einzelpersonen haben, über die personenbezogene Informationen erhoben, weitergegeben und genutzt werden; sie sollten auch andere Faktoren bedenken, wie die öffentliche Meinung und die Kräfte des Marktes, aus denen Hinweise für die Angemessenheit einer möglichen Aktivität gewonnen werden können.

9. Nachdem die Auswirkungen auf den Datenschutz abgeschätzt worden sind, könnte ein Nutzer von Informationen zu dem Schluß kommen, daß es im Hinblick auf eine gegenwärtige oder geplante Aktivität angemessen ist, personenbezogene Daten zu erheben. Eine geplante Aktivität ist eine Aktivität, die von dem Nutzer der Informationen mit der Absicht erwogen wird, eine solche Aktivität in der Zukunft durchzuführen. In jedem Fall sollte ein Nutzer von Informationen nur solche Informationen erheben, deren Verwendung zur Unterstützung dieser Aktivitäten vernünftigerweise erwartet werden kann. Obwohl die Kosten für die Speicherung von Informationen kontinuierlich zurückgehen, ist es unangemessen, große Mengen personenbezogener Informationen nur deswegen zu speichern, weil die Informationen sich in der Zukunft als von einem unerwartetem Wert herausstellen können. Auch personenbezogene Informationen, die ihren Zweck erfüllt haben und von denen nicht vernünftigerweise erwartet werden kann, daß sie irgendwelche gegenwärtigen oder geplanten Aktivitäten unterstützen können, sollten nicht weitergespeichert werden.

10. Die Fähigkeit, bestimmte personenbezogene Informationen zu erheben, bedeutet nicht, daß es auch richtig ist, dies zu tun. In bestimmten Fällen haben Einzelpersonen keine Wahl, personenbezogene Daten zu offenbaren oder dies nicht zu tun. Wenn z. B. eine Einzelperson eine Transaktion auf der NII ausführt, werden typi-

scherweise personenbezogene Informationen in Form von Transaktionsdaten erzeugt. In anderen Fällen mag eine Wahlmöglichkeit nur theoretisch gegeben sein. Von einer bestimmten Wahlmöglichkeit Gebrauch zu machen, kann zur Verweigerung von Leistungen führen, die die Einzelpersonen brauchen, um an der Gesellschaft in vollem Umfang teilnehmen zu können – z. B. die Erteilung eines Führerscheins, um ein Fahrzeug führen zu können. In diesen Fällen sollte die Gesellschaft ein Grundniveau für den Datenschutz im Einklang mit dem Datenschutzprinzip (I. A.) schaffen.

## II. B. Aufklärungsprinzip (Notice Principle)

**Nutzer von Informationen, die personenbezogene Informationen direkt vom Betroffenen erheben, sollten angemessene, erforderliche Informationen darüber zur Verfügung stellen,**

1. **warum sie die Information erheben;**
2. **wofür die Informationen voraussichtlich gebraucht werden;**
3. **welche Schritte unternommen werden, um die Vertraulichkeit, Integrität und Qualität der Informationen zu schützen;**
4. **welche Konsequenzen die Offenbarung bzw. Zurückhaltung der Informationen haben würde und**
5. **welche Rechte die betroffene Person hat.**

11. Personenbezogene Informationen können auf zwei Arten erhoben werden: sie können direkt bei der Einzelperson erhoben oder von einer Sekundärquelle beschafft werden. Notwendigerweise unterscheiden sich die Prinzipien, die diese zwei Methoden der Erhebung von personenbezogenen Informationen regeln. Während die Verpflichtung zur Aufklärung all denen auferlegt werden kann, die Informationen direkt von dem einzelnen erheben, können diese nicht in gleicher Weise auf Einrichtungen angewandt werden, die keine solche direkte Beziehung haben. Wenn alle Empfänger personenbezogener Informationen verpflichtet werden, jeden einzelnen, über den sie Daten erhalten, zu benachrichtigen, würde der Austausch personenbezogener Daten entscheidend erschwert werden und viele der Vorteile der NII würden verlorengehen.

12. Für diejenigen, die personenbezogene Informationen direkt vom einzelnen erheben, fordert das Aufklärungsprinzip, dem einzelnen hinreichende Informationen zu geben, um eine informierte Entscheidung über seinen oder ihren Datenschutz treffen zu können. Die Wichtigkeit dieser Aufklärung kann nicht überbetont werden, da die Bedingungen der Aufklärung das Verständnis des einzelnen darüber, wie personenbezogene Informationen genutzt werden sollen, in substantieller Weise bestimmt, ein Verständnis, das von allen nachfolgenden Nutzern dieser Informationen respektiert werden muß.

13. Das Aufklärungsprinzip bezieht sich insbesondere auf personenbezogene Informationen, die durch Gesetz als öffentliche Akten bestimmt sind, und auf Transaktionsdaten, die als Nebenprodukt einer Transaktion entstehen. Im Hinblick auf die Transaktionsdaten bezieht sich das Aufklärungsprinzip auf alle Parteien, nicht nur auf die Partei, die prinzipiell mit dem einzelnen in Verbindung steht, um ein Produkt zu liefern oder einen Dienst zu erbringen, sondern auch auf die, die diese Transaktion ermöglichen, wie Anbieter von Kommunikationsdiensten und elektronischen Zahlungsdiensten, die dabei helfen, diese Transaktionen zu vollziehen. Wenn z. B. ein einzelner mit einer Kreditkarte in einem On-line-Kaufhaus Blumen kauft, auf das er über ein Modem zugreift, ist das Aufklärungsprinzip auf alle Parteien anwendbar, die in Verbindung mit diesem Kauf Transaktionsdaten erheben, nicht nur auf den Blumenhändler, sondern auch auf die Telefon- und die Kreditkartengesellschaften. Transaktionsvermittler sollten normalerweise in dem Augenblick Aufklärung leisten, in dem sie ein Konto einrichten oder dem Benutzer eine Rechnung stellen.

14. Was als angemessene, erforderliche Information angesehen wird, um dem Aufklärungsprinzip zu genügen, hängt von den Umständen der Erhebung der Information ab. In manchen Fällen – insbesondere wenn es eine kontinuierliche Beziehung zwischen dem einzelnen und der die Information erhebenden Stelle gibt – muß eine Aufklärung nicht vor der Erhebung personenbezogener Daten in jedem Einzelfall gegeben werden. Beispielsweise sollte ein Anbieter von Informations- oder Kommunikationsdiensten normalerweise den Benutzer in dem Augenblick aufklären, in dem er einen bestimmten Dienst abonniert und möglicherweise danach in periodischen Abständen, aber nicht jedesmal, wenn der einzelne diesen Dienst benutzt. In anderen Fällen ist der gewöhnliche und bestätigte Gebrauch personenbezogener Informationen von den einzelnen so klar vorauszusehen, daß eine formelle Aufklärung nicht notwendig ist. Wenn beispielsweise der Name und die Adresse eines einzelnen erhoben wird, um der richtigen Person die richtige Medizin unter der richtigen Adresse zu liefern, braucht der Bestellung keine ausführliche Aufklärung vorauszugehen. Sollte jedoch das pharmazeutische Unternehmen die Informationen in einer Weise nutzen, die vom Betroffenen nicht klar vorhergesehen werden kann – z. B. um eine Liste mit von Bluthochdruck betroffenen Personen zu erstellen und diese an Krankenversicherungen zu verkaufen –, sollte eine gewisse Aufklärung erfolgen.

15. Während das Aufklärungsprinzip erkennen läßt, aus welchen Elementen eine angemessene Aufklärung zusammengesetzt sein könnte, schreibt es keine bestimmte Form dieser Aufklärung vor. Das Ziel dieses Prinzips ist eher, sicherzustellen, daß der einzelne hinreichende Informationen in einer verständlichen Form erhält, um eine informierte Entscheidung treffen zu können. Daher sollten die Entwickler von Aufklärungstexten erfinderisch im Hinblick darauf sein, auf eine Art aufzuklären, die jeden einzelnen, unabhängig von Alter, der Fähigkeit zum Lesen und Schreiben und von Bildung dabei unterstützen kann, dieses Ziel zu erreichen.

16. Obwohl das Aufklärungsprinzip die Stellen, die Informationen erheben, auffordert, jeden einzelnen darüber zu informieren, welche Schritte zum Schutz der personenbezogenen Informationen unternommen werden, sind sie nicht verpflichtet, überwiegend technische Beschreibungen solcher Sicherheitsmaßnahmen zur Verfügung zu stellen. Tatsächlich können solche Beschreibungen für den einzelnen unwillkommen oder nicht hilfreich sein. Darüber hinaus können sie sich im Gegensatz zu den Anforderungen des Schutzprinzips (II.C.) kontraproduktiv auswirken, da die breitgestreute Veröffentlichung technischer Sicherheitsmaßnahmen Schwachstellen von Systemen offenlegen könnte.

**II. C. Schutzprinzip (Protection Principle)**

**Nutzer von Informationen sollen angemessene technische und organisatorische Maßnahmen ergreifen, um die Vertraulichkeit und Integrität von personenbezogenen Informationen zu schützen.**

17. In der NII werden personenbezogene Informationen in einer Netzwerkumgebung verarbeitet, die enorme Risiken im Hinblick auf unbefugten Zugriff, unbefugte Weitergabe, Veränderung und Löschung aufwirft. Sowohl Personen innerhalb der datenverarbeitenden Stelle als auch Außenstehende könnten Zugriff auf Informationen erhalten, die nicht für sie bestimmt sind, oder schwer nachzuvollziehende Veränderungen an Daten vornehmen, die dann für wichtige Entscheidungen herangezogen werden.

18. Unsere Gesundheitsdienstleistungsunternehmen erwarten beispielsweise, intensive Nutzer der NII zu werden. Mit Hilfe der NII wird eine abgelegene Klinik in der Lage sein, Röntgenaufnahmen zur Untersuchung durch einen Radiologen an eine Universitätsklinik in einem anderen Teil des Landes zu senden. Die möglichen Vorteile einer solchen Maßnahme sind offensichtlich. Jedoch können diese Vorteile nicht genutzt werden, wenn die einzelnen sich weigern, solche sensiblen Daten zu übertragen, weil sie fürchten, daß die NII nicht sicherstellen kann, daß sensible medizinische Daten vertraulich und unverändert bleiben werden.

19. Bei der Entscheidung darüber, welche Maßnahmen angemessen sind, sollten die Nutzer von Informationen anerkennen, daß personenbezogene Informationen im Einklang mit den Annahmen der einzelnen und in einer Weise geschützt werden, die dem Schaden entspricht, der entstehen könnte, wenn die Informationen unbefugt weitergegeben oder verändert würden.

20. Beim Schutz personenbezogener Informationen sollten die Nutzer von Informationen einen mehrseitigen Ansatz wählen, der sowohl technische als auch organisatorische Maßnahmen umfaßt. Im Hinblick auf technische Maßnahmen sollten die Nutzer von Informationen die Verschlüsselung personenbezogener Informationen einschließlich des Inhalts und der Verbindungsdaten bei Transaktionen in Erwägung ziehen. Zusätzlich sollten sie die Schaffung automatisierter Überwachungsmechanismen in Erwägung ziehen, die bei der Aufdeckung von unbefugten Zugriffen sowohl von Beschäftigten als auch von Außenstehenden helfen können. Im Hinblick auf organisatorische Maßnahmen könnte man z. B. die Schaffung einer Organisationskultur anstreben, in der die einzelnen über faire Informationspraktiken informiert werden und diese Praktiken anwenden. Organisationen können auch eine Politik einführen, die eine Nutzung von Informationen, die im Zusammenhang mit einer bestimmten Aktivität erhoben worden sind, für andere nicht dazu in Beziehung stehende Zwecke verbietet.

**II. D. Fairneß-Prinzip (Fairness Principle)**

**Nutzer von Informationen sollten personenbezogene Informationen nicht in einer Weise nutzen, die nicht mit den Erwartungen des einzelnen darüber vereinbar ist, wie diese Information genutzt werden wird, soweit nicht ein zwingendes öffentliches Interesse an einer solchen Nutzung besteht.**





21. Die Erwartung des einzelnen umfaßt das objektive, vernünftige Verständnis des einzelnen und den Umfang der Einwilligung zum Zeitpunkt der Erhebung der Information. Wie bereits vorher ausgeführt, richtet sich die Erwartung des einzelnen prinzipiell nach der Art der Aufklärung durch denjenigen, der die Daten erhebt, nach dem Aufklärungprinzip (II. B.), die der einzelne nach dem Bewußtseinsprinzip (III. A.) erhalten hat. Ohne ein Fairneß-Prinzip wäre eine unbeschränkte Nutzung der Informationen möglich, die über die Erwartung des einzelnen hinausgehen könnte.

22. Wenn ein Informationsnutzer personenbezogene Informationen in einer unvereinbaren Art nutzen will, muß er zunächst den einzelnen darüber aufklären und seine oder ihre explizite oder implizite Einwilligung einholen. Die Art der unangemessenen Nutzung bestimmt, ob eine solche Einwilligung explizit oder implizit gegeben werden muß. In einigen Fällen können die Folgen für den einzelnen von solcher Tragweite sein, daß der zukünftige Nutzer die Daten nur nutzen sollte, nachdem der einzelne dieser Nutzung ausdrücklich zugestimmt hat. In anderen Fällen kann eine Aufklärung des einzelnen angemessen sein, die ihm die Möglichkeit gibt, der Nutzung innerhalb einer bestimmten Zeitspanne zu widersprechen. Das Prinzip enthält die Anforderung, daß, wenn personenbezogene Informationen von einem Informationsnutzer an einen anderen Informationsnutzer übertragen werden, auch die Erwartungen des einzelnen, wie diese personenbezogenen Informationen genutzt werden, weitergegeben werden müssen. Da sich alle Nutzer von Informationen an das Fairneß-Prinzip halten müssen, tragen sowohl Übermittler als auch Empfänger die Verantwortung dafür, sicherzustellen, daß die Erwartungen des einzelnen zusammen mit der Information übertragen werden.

23. Bei der Entscheidung darüber, ob eine bestimmte Nutzung von Informationen nicht mit den Erwartungen des einzelnen vereinbar ist, sollten die Nutzer von Informationen abwägen, ob die Nutzung bei der Aufklärung ausdrücklich gestattet wurde oder in anderer Hinsicht mit der Aufklärung in Einklang steht. Jede Nutzung von Information jenseits dieser Bedingungen ist mit den Erwartungen des einzelnen nicht vereinbar. Was im Rahmen dieses Prinzips als unvereinbar gilt, ist nicht beschränkt durch das, was im Rahmen des Datenschutzgesetzes (Privacy Act) als unvereinbar gilt (vgl. 5 U.S.C. § 552 a).

24. Das Fairneß-Prinzip kann nicht in jeder Situation in gleicher Weise angewandt werden. Eine zweckfremde Nutzung ist nicht notwendigerweise auch eine schädliche Nutzung; tatsächlich kann eine solche Nutzung sehr vorteilhaft für den einzelnen und die Gesellschaft sein. Es gibt einige zweckfremde Nutzungen, die zu erheblichen Vorteilen führen werden und die meistenteils zu vernachlässigende Auswirkungen auf die Datenschutzinteressen des einzelnen haben. Beispiele hierfür bilden Forschung und Statistik, bei denen die Informationen ohne Auswirkung auf den einzelnen genutzt werden. Das Einholen der Einwilligung des einzelnen, um eine erneute statistische Nutzung existierender Daten zu erlauben, führt zu zusätzlichen Kosten und zusätzlichem Verwaltungsaufwand und kann damit zu einer Behinderung eines Forschungsprojekts führen. In anderen Fällen können personenbezogene Informationen für ein wichtiges öffentliches Erfordernis genutzt werden, das von der Gesellschaft in einer formalen, offenen Weise anerkannt wird (typischerweise durch Gesetzgebung), das verhindert werden würde, wenn man dem einzelnen die Möglichkeit geben würde, die Nutzung zu begren-

zen. Ein Beispiel bildet die Nutzung personenbezogener Informationen in einem Ermittlungsverfahren, für die die Einwilligung des Verdächtigen unwahrscheinlich wäre und sogar die Frage nach einer solchen Einwilligung kontraproduktiv für die Untersuchung sein könnte. Ein weiteres Beispiel wäre eine zweckfremde Nutzung personenbezogener Informationen durch die investigative Presse, die durch den ersten Zusatz (der amerikanischen Verfassung; Anm. d. Übers.) besonders geschützt und sanktioniert ist.

**II. E. Unterrichtungsprinzip (Education Principle)**

**Nutzer von Informationen sollten sich selbst und die Öffentlichkeit darüber unterrichten, wie der Datenschutz gewährleistet werden kann.**

25. Das Unterrichtungsprinzip bildet eine wichtige Ergänzung zu den traditionellen Prinzipien des fairen Umgangs mit Informationen. Es gibt viele Nutzungsmöglichkeiten der NII, für die der einzelne sich nicht vollständig auf Kontrollen durch die Regierung oder andere Organisationen zum Schutz seiner personenbezogenen Daten verlassen kann. Obwohl die einzelnen zum Schutz ihrer personenbezogenen Daten oftmals auf solche gesetzlichen und institutionellen Kontrollen angewiesen sind, werden viele Personen Aktivitäten außerhalb dieser Kontrollen beginnen, insbesondere, wenn sie sich am informellen Austausch von Informationen auf der NII beteiligen. Daher müssen sich die einzelnen der Gefahren bei der Offenbarung personenbezogener Daten bewußt sein und abwägen, ob die Offenbarung personenbezogener Daten ihrem Vorteil dient.

26. Die gesamten Auswirkungen der NII auf die Nutzung personenbezogener Daten sind noch nicht absehbar, und die einzelnen können nicht erkennen, welche Auswirkungen die Vernetzung von Informationen auf ihr Leben haben könnte. Da es von Bedeutung ist, daß die einzelnen und die Nutzer von Informationen sich darüber bewußt sind, in welcher Weise die NII sich auf den Schutz personenbezogener Daten auswirkt, sollten alle Nutzer von Informationen an der Unterrichtung über den Umgang und die Nutzung personenbezogener Informationen teilnehmen. Traditionell haben die Regierungen und die Schulen die Öffentlichkeit in Angelegenheiten von sozialen Rechten und Pflichten unterrichtet, und sie sollen auch weiterhin eine führende Rolle spielen. Jedoch muß auch der private Bereich als ein wichtiger Erbauer der NII eine entscheidende Rolle spielen. Eine Unterrichtung, die den einzelnen helfen würde, die Risiken für den Schutz ihrer personenbezogenen Daten zu minimieren, könnte in Datenschutz-Telefon-Hotlines, Datenschutzberatungseinrichtungen auf dem Internet und vergleichbaren Marketing- und Öffentlichkeitsarbeitskampagnen bestehen.

## III. Prinzipien für die Betroffenen als Informationslieferanten

**III. A. Bewußtseinsprinzip (Awareness Principle)**

**Die einzelnen sollen angemessene und relevante Informationen darüber erhalten,**

1. **warum die Information erhoben wird;**
2. **wofür die Information voraussichtlich genutzt wird;**





3. **welche Schritte zum Schutz ihrer Vertraulichkeit, Integrität und Qualität unternommen werden;**
4. **welche Konsequenzen die Offenbarung bzw. Zurückhaltung der Information haben würde und**
5. **welche Rechte sie haben.**

27. In zunehmenden Maße werden Einzelpersonen gebeten, personenbezogene Informationen über sich zu offenbaren. Manchmal sind diese Anfragen einfach; beispielsweise wird eine Bank vor der Bearbeitung eines Darlehensantrags personenbezogene Daten erbitten. In diesem Fall ist eine Nutzung der Information offensichtlich – die Bearbeitung des Darlehensantrags. Es könnte jedoch andere Nutzungen geben, die nicht so offensichtlich sind, wie die Nutzung eines Teils dieser Information zur Werbung für eine Kreditkarte. Tatsächlich offenbaren Einzelpersonen regelmäßig personenbezogene Daten, ohne sich vollständig über die unterschiedlichen Arten bewußt zu sein, auf die diese Informationen letzten Endes benutzt werden. Beispielsweise könnte ein einzelner nicht bemerken, daß die Bezahlung medizinischer Dienstleistungen mit einer Kreditkarte zum Entstehen von Transaktionsdaten führt, die seinen Gesundheitszustand offenlegen können.

28. Das Bewußtseinsprinzip erkennt an, daß, obwohl die Stellen, die Daten erheben, Verantwortung dafür tragen, die einzelnen darüber zu informieren, warum sie die personenbezogenen Informationen brauchen, auch die einzelnen eine Verantwortung haben, die Konsequenzen der Offenbarung personenbezogener Daten an andere zu verstehen. Dies gilt insbesondere in einer interaktiven Umgebung wie der NII, in der die einzelnen die Bedingungen ihrer Teilnahme aktiv bestimmen können. Wenn die einzelnen beispielsweise eine wirkliche Wahlmöglichkeit haben, ob und in welchem Maße personenbezogene Informationen offenbart werden sollen, sollten sie eine aktive Rolle bei der Entscheidung darüber spielen, ob überhaupt und unter welchen Bedingungen personenbezogene Informationen offenbart werden sollen.

29. Natürlich muß den einzelnen, wenn sie für die Auswahl aus diesen Möglichkeiten verantwortlich gemacht werden sollen, genug Information gegeben werden, um eine intelligente Wahl treffen zu können. Auf diese Weise wirkt das Bewußtseinsprinzip im Zusammenhang mit dem Aufklärungsprinzip (II. B.) und in geringerem Maße mit dem Unterrichtungsprinzip (II. E.) zusammen, um die einzelnen zu befähigen, die Verantwortung dafür zu übernehmen, wie personenbezogene Informationen offenbart und genutzt werden sollen.

**III. B. Durchsetzungsprinzipien (Empowerment Principles)**

**Die Einzelnen sollten in der Lage sein, den Schutz ihrer personenbezogenen Daten zu sichern durch**

1. **Mittel, die sie betreffenden Informationen zu erhalten;**
2. **Mittel, sie betreffende Informationen, die eine ungenügende Qualität haben, zu korrigieren, um die Fairneß bei ihrer Nutzung zu sichern;**

**3. die Möglichkeit zur Nutzung angemessener technischer Kontrollen, wie z. B. Verschlüsselung, um die Vertraulichkeit und die Integrität von Nachrichten und Transaktionen zu schützen, und**

**4. die Möglichkeit, anonym zu bleiben, wenn dies angemessen ist.**

30. Die einzelnen sollten die Möglichkeit haben, von den Nutzern von Informationen eine Kopie ihrer personenbezogenen Informationen zu erhalten und Informationen über sich zu korrigieren, die eine hinreichende Qualität vermissen lassen, um die Fairneß bei ihrer Nutzung sicherzustellen. In welchem Ausmaß solche Mittel angeboten werden, hängt von verschiedenen Faktoren ab, einschließlich der Reichweite der Konsequenzen der Nutzung der personenbezogenen Informationen für den einzelnen und jeglicher Rechte aus dem ersten Zusatz (der amerikanischen Verfassung; Anm. d. Übers.), die dem Nutzer der Information zustehen.

31. Darüber hinaus sollte der einzelne verschiedene selbstinitiierte Maßnahmen zur Sicherung des Schutzes seiner personenbezogenen Daten in Betracht ziehen, wenn die Bedingungen bei der Erhebung der Information unbefriedigend sind. Um beispielsweise die Vertraulichkeit oder die Integrität einer Kommunikation zu sichern, sollte der einzelne die Möglichkeit haben, angemessene Werkzeuge, wie z. B. Verschlüsselung, zu benutzen. Um zu vermeiden, eine Datenspur von Transaktionsdatensätzen zu hinterlassen, sollte der einzelne auch die Möglichkeit haben, anonym zu bleiben, wenn dies angemessen ist. Anonymität würde z. B. angemessen sein, wenn der einzelne eine öffentliche elektronische Bibliothek durchsucht oder wenn ein einzelner sich an der anonymen politischen Äußerung, die von der Verfassung geschützt ist, beteiligt (S. McIntyre v. Ohio Elections Commission, 131 L. Ed. 2d 426 [1995]). In einer idealen Welt würde das Angebot nichtentschlüsselbarer Verschlüsselungsverfahren oder absoluter Anonymität dem Schutz personenbezogener Daten ohne negative Auswirkungen dienen. Unglücklicherweise werden in der realen Welt einige dieser Technologien mißbraucht und schaden dabei anderen. Es liegt außerhalb des Geltungsbereichs der Prinzipien, in welcher Weise den einzelnen Verschlüsselung oder Anonymität für berechtigte Nutzungen bei gleichzeitiger Minimierung ihres Mißbrauchs angeboten werden kann. Diese Dinge müssen jedoch angesprochen werden, wenn die NII ihr volles Potential erreichen soll.

### III. C. Wiedergutmachungsprinzip (Redress Principle)

**Die einzelnen sollten, soweit dies angemessen ist, Mittel zur Wiedergutmachung (Rechte) haben, wenn sie durch eine unsachgemäße Offenbarung oder Nutzung personenbezogener Informationen beeinträchtigt werden.**

32. Wiedergutmachung ist nur notwendig, wenn ein einzelner in seinen Rechten verletzt wird. Da das Wiedergutmachungsprinzip für eine generelle Anwendung entworfen worden ist, beantwortet es nicht in jedem Einzelfall, ob überhaupt ein Schaden entstanden ist oder ob genug Schaden entstanden ist, um eine bestimmte Art der Wiedergutmachung zu rechtfertigen. Diese Fragen müssen während der sektoralen Implementierung der Prinzipien beantwortet werden.





33. Eine unsachgemäße Nutzung schließt insbesondere eine Entscheidung ein, die auf personenbezogene Daten von nicht hinreichender Qualität gestützt wird – Information, die nicht richtig, aktuell, vollständig oder erforderlich für den Zweck ist, für den sie offenbart und genutzt wird. Das Wiedergutmachungsprinzip setzt jedoch keinen bestimmten Verschuldensgrad des Nutzers von Informationen zur Rechtfertigung einer bestimmten Form der Wiedergutmachung voraus.

34. Wenn eine Wiedergutmachung angemessen ist, sind nach den Prinzipien verschiedene Formen vorstellbar, einschließlich, aber nicht beschränkt auf informelle Beschwerde, Vermittlung, Schlichtung, zivilen Rechtsstreit, gesetzliche Zwangsmaßnahmen und Strafverfolgung in verschiedenen privaten, kommunalen, einzel- und bundesstaatlichen Foren mit dem Ziel, Abhilfe möglichst effektiv und kostengünstig zu schaffen.

# II. PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION

Privacy Working Group
Information Policy Committee
Information Infrastructure Task Force

Final Version
June 6, 1995

## INTRODUCTION

The National Information Infrastructure ("NII"), with its promise of a seamless web of communications networks, computers, databases, and consumer electronics, heralds the arrival of the information age. The ability to acquire, process, send, and store information at an acceptable cost has never been greater, and continuing advances in computer and telecommunications technologies will result in ever-increasing creation, use, and storage of information.

The NII promises enormous benefits. To name just a few, the NII offers the possibilities of greater citizen participation in a deliberative democracy, advances in medical treatment and research, and quick verification of critical information such as a gun purchaser's criminal record. These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means "information privacy," an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed, and used.

Two converging trends – one social, the other technological – lead to an increased risk to privacy in the evolving NII. As a social trend, individuals will use the NII to communicate, order goods and services, and obtain information. But, unlike paying cash to buy a magazine, using the NII for such purposes will generate data documenting the transaction that can be easily stored, retrieved, analyzed, and reused. Indeed, NII transactional data may reveal who communicated with whom, when, and for how long, as well as who bought what, for what price. Significantly, this type of personal information is automatically generated, in electronic form, and is therefore especially inexpensive to store and process.

The technological trend is that the capabilities of hardware, software, and communications networks are continually increasing, while costs are continually decreasing, allowing information to be used in ways that were previously impossible or economically impractical. For example, before the NII, in order to build a profile of an individual who had lived in various states, one would have to travel from state to state and search public records for information about the individual. This process would have required filling out forms, paying fees, and waiting in line for record searches at local, state, and federal agencies, such as the departments of motor vehicles, deed record offices, electoral commissions, and county record offices. Although one could manually compile a personal profile in this manner, it would be a time-consuming and costly exercise, one that would not be undertaken unless the offsetting rewards were considerable. In sharp contrast, today, as more and more personal information appears on-line, such a profile can be built in a matter of minutes, at minimal cost.

These two converging trends guarantee that as the NII evolves, more personal information will be generated and more will be done with that information. Here lies the increased risk to privacy. This risk must be addressed both to secure the value of privacy for individuals and society and to ensure that the NII will achieve its full potential. Unless this is done, individuals may not participate in the NII for fear that the costs to their privacy will outweigh the benefits. The adoption of principles of fair information practice is a critical first step in addressing this concern. While guidance can be found in existing laws and principles, these need to be adapted to accommodate the evolving information environment. This changing environment presents new concerns.

- No longer do governments alone acquire and use large amounts of personal information; the private sector now rivals the government in acquiring and using personal information. New principles would thus be incomplete unless they applied to both the governmental and private sectors.
- The NII promises true interactivity. Individuals will become active participants who will create volumes of data containing the content of communications as well as transactional data.
- The transport vehicles for personal information – the networks – are vulnerable to abuse; thus, the security of the network itself is critical to the NII's future success.
- The rapidly evolving information environment makes it difficult at times to know how to apply traditional ethical rules, even ones that are well understood and accepted when dealing with tangible records and documents. Consider, for example, how an individual who would never trespass into someone's home might rationalize cracking into someone's computer as an intellectual exercise. In addition, today's information environment may present questions about the use of personal information that traditional rules do not even address.

These "Principles for Providing and Using Personal Information" ("the Principles") are offered to respond to this new information environment. The Principles attempt to provide meaningful guidance, striking a balance between abstract concepts and a detailed code. They are intended to guide all NII participants and should be used by those who are drafting laws and regulations, creating industry codes of fair information practices, and designing private sector and government programs that use personal information.

The limitations inherent in any such principles must be recognized. The Principles do not have the force of law and do not create any substantive or procedural right enforceable at law. They are not designed to produce specific answers to all possible questions; nor to single-handedly govern the various sectors that use personal information. The Principles should be interpreted and applied as a whole, pragmatically and reasonably. For example, those applying these principles should consider:

- the benefits to society from the use of personal information, recognizing that privacy interests are not absolute and must be balanced by the need for legal accountability, adherence to the First Amendment, law enforcement needs, and other societal benefits recognized in law;
- the extent to which the decision to provide personal information is voluntary, and the individual's expectations regarding the use of the information (taking into account the notice and the scope of consent provided);





- the sensitivity of the information and the potential for harm to the individual that could result from a particular disclosure or use of the information;
- the cost and effort required to protect against harm to individuals, recognizing that more sensitive information may require more costly and elaborate protection procedures than less sensitive information.

Where an overly mechanical application of the Principles would be particularly unwarranted, phrases with the words "appropriate" or "reasonable" appear in the text. This flexibility, built into the Principles to address hard or unexpected cases, does not mean that the Principles need not be adhered to rigorously. Finally, the Principles are intended to be consistent with the spirit of current international guidelines, such as the OECD Guidelines,[1] regarding the use of personal information. The Principles invite further international cooperation over the development and harmonization of global privacy policies, adherence to which will bolster the ongoing development of the Global Information Infrastructure.

**PREAMBLE**

The United States is committed to building a National Information Infrastructure ("NII") to meet the information needs of its people. This infrastructure, created by advances in technology, is expanding the level of interactivity, enhancing communication, and allowing easier access to services. As a result, many more users are discovering new, previously unimagined ways to acquire and use personal information. In this environment, we are challenged to develop new principles to guide all NII participants in the fair use of personal information.

Existing codes of fair information practice must be adapted to a new environment in which information and communications are sent and received over networks by users who have very different capabilities, objectives, and perspectives. In this interactive, networked environment, many new relationships are being formed among individuals, communication providers, and other NII participants. New principles must acknowledge that each party has a different relationship with the individual and has different uses for personal information.

New principles should not diminish existing constitutional and statutory limitations on access to information, communications, and transactions, such as requirements for warrants and subpoenas. Such principles should ensure that access limitations keep pace with technological developments. These principles should acknowledge that all elements of our society share responsibility for ensuring the fair treatment of individuals in the use of personal information, whether on paper or in electronic form. Moreover, the principles should recognize that the interactive nature of the NII can empower individuals to participate in protecting information about themselves. The new principles should also make clear that this responsibility can be exercised only with openness about the process, a commitment to fairness and accountability, and continued attention to security. Finally, the principles should recognize the need to educate all participants about the new information infrastructure and how it will affect their lives.

1 See above p. 21.

These "Principles for Providing and Using Personal Information" ("the Principles") recognize the changing roles of government and industry in information acquisition and use. Thus, they are intended to apply to both public and private entities. The Principles are designed to guide all NII participants as well as those who are drafting legislation and crafting policy regarding the use of personal information. They provide the basic framework from which specialized principles can be developed as needed.

Trade-offs will be inevitable in implementing the Principles because privacy interests are not absolute and must be balanced against the need for accountability, the value of an unabridged flow of information, and other societal benefits recognized in law, such as lawful law enforcement activities. For example, certain decisions about the flow of personal information have already been made for us by the First Amendment, and nothing in the Principles should be read to require policies derogating the constitutionally protected freedom of speech and the press. Given these sometimes conflicting interests and public policies, the Principles must be implemented pragmatically yet conscientiously, giving due consideration to issues such as the extent to which providing personal information is voluntary, the adequacy of the notice regarding how the personal information may be used, the scope of the individual's consent, and the cost of protecting information in light of the information's sensitivity.

## PRINCIPLES AND COMMENTARY

### I. General Principles for All NII Participants

1. Three fundamental principles should guide all NII participants. These three principles – information privacy, information integrity, and information quality – identify the fundamental requirements necessary for the proper use of personal information, and in turn the successful implementation of the NII. All NII participants should use appropriate means to ensure that these principles are satisfied.

#### I. A. Information Privacy Principle

**Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.**

2. The NII can flourish only if all participants respect information privacy. Information privacy is an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed, and used. The level of privacy that must be respected is an individual's reasonable expectation, an expectation subjectively held by the individual and deemed objectively reasonable by society. Not all subjectively held expectations will be honored as reasonable. For example, an individual who posts an unencrypted personal message on a bulletin board for public postings cannot reasonably expect that personal message to be read only by the addressee.

3. What counts as a reasonable expectation of privacy under the Principles is not limited by what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. In many instances, society has deemed it reasonable to protect privacy at a level higher than that required by the Fourth Amendment. See, e.g., Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1988); Privacy Act, 5 U.S.C. § 552a (1988). The Information Privacy Principle fully supports such possibilities.

4. As explained in later principles and commentary, an individual's privacy can often be best respected when individuals and information users come to some mutually agreeable understanding of how personal information will be acquired, disclosed, and used. However, in certain cases – for example, if the individual lacks sufficient bargaining power – purely contractual arrangements between individuals and information users may fail to respect privacy adequately. In such instances, society should ensure privacy at some basic level in order to satisfy the Information Privacy Principle.

#### I. B. Information Integrity Principle

**Personal information should not be improperly altered or destroyed.**

5. NII participants should be able to rely on the integrity of the personal information the NII contains. Thus, personal information should be protected against improper alteration or destruction.

#### I. C. Information Quality Principle

**Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.**

6. Personal information should have sufficient quality to be relied upon. This means that personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

### II. Principles for Users of Personal Information

#### II. A. Acquisition Principles

**Information users should:**

1. **Assess the impact on privacy in deciding whether to acquire, disclose, or use personal information.**
2. **Acquire and keep only information reasonably expected to support current or planned activities.**

7. The benefit of information lies in its use, but therein lies an often unconsidered cost: the threat to information privacy. A critical characteristic of privacy is that once it is lost, it can rarely be restored. Consider, for example, the extent to which the inappropriate release of sensitive medical information could ever be rectified by public apology.

8. Given this characteristic, privacy should not be addressed as a mere afterthought, once personal information has been acquired. Rather, information users should explicitly consider the impact on privacy in the very process of designing informa-

tion systems and in deciding whether to acquire or use personal information in the first place. In assessing this impact, information users should gauge not just the effect their activities may have on the individuals about whom personal information is acquired, disclosed, and used; they should also consider other factors, such as public opinion and market forces, that may provide guidance on the appropriateness of any given activity.

9. After assessing the impact on information privacy, an information user may conclude that it is appropriate to acquire personal information in pursuit of a current or planned activity. A planned activity is one that is contemplated by the information user, with the intent to pursue such activity in the future. In all cases, the information user should acquire only that information reasonably expected to support those activities. Although information storage costs decrease continually, it is inappropriate to collect volumes of personal information simply because some of the information may, in the future, prove to be of some unanticipated value. Also, personal information that has served its purpose and is no longer reasonably expected to support any current or planned activities should not be kept.

10. The ability to acquire certain kinds of personal information does not mean that it is proper to do so. In certain cases, individuals have no choice whether to disclose personal information. For example, if the individual executes a transaction on the NII, personal information in the form of transactional data will typically be generated. In other cases, the choice may exist in theory only. Exercising certain choices may result in the denial of a benefit that individuals need to participate fully in society – for example, obtaining a license to drive an automobile. In such cases, society should establish some basic level of privacy protection in accordance with the Information Privacy Principle (I. A.).

## II. B. Notice Principle

**Information users who collect personal information directly from the individual should provide adequate, relevant information about:**

1. **Why they are collecting the information;**
2. **What the information is expected to be used for;**
3. **What steps will be taken to protect its confidentiality, integrity, and quality;**
4. **The consequences of providing or withholding information; and**
5. **Any rights of redress.**

11. Personal information can be acquired in one of two ways: it can be collected directly from the individual or obtained from some secondary source. By necessity, the principles governing these two methods of acquiring personal information differ. While notice obligations can be placed on all those who collect information directly from the individual, they cannot be imposed uniformly on entities that have no such direct relationship. If all recipients of personal information were required to notify every individual about whom they receive data, the exchange of personal information would become prohibitively burdensome, and many of the benefits of the NII would be lost.





12. For those who collect personal information directly from the individual, the Notice Principle requires the individual to be given sufficient information to make an informed decision about his or her privacy. The importance of providing this notice cannot be overstated because the terms of the notice substantially determine the individual's understanding of how personal information will be used, an understanding that must be respected by all subsequent users of that information.

13. The Notice Principle specifically applies to personal information designated by law as a public record and to transactional data generated as a byproduct of a transaction. With respect to transactional data, this principle applies to all parties, including not only the party principally transacting with the individual in order to provide some product or service, but also to those transaction facilitators such as communication providers and electronic payment providers who help to consummate these transactions. For example, if an individual purchases flowers with a credit card through an on-line shopping mall accessed via modem, the Notice Principle applies to all parties who collect transactional data related to the purchase, not only to the florist, but also to the telephone and credit card companies. Transaction facilitators would ordinarily provide notice at the time they establish an account, or when billing the customer.

14. What counts as adequate, relevant information to satisfy the Notice Principle depends on the circumstances surrounding the collection of information. In some cases – especially where there is a continuing relationship between the individual and the information collector – notice need not be given before each instance that personal information is collected. For example, an information or communication service provider should ordinarily give notice when the individual subscribes to a particular service and perhaps periodically thereafter, not each time the individual uses the service. In other cases, the ordinary and acknowledged use of personal information is so clearly contemplated by the individual that providing formal notice is not necessary. For example, if an individual's name and address is collected by a pharmaceutical company that takes the order over interactive television simply to deliver the right medicine to the right person at the right address, no elaborate notice need precede taking the individual's order. However, should the pharmaceutical company use the information in a manner not clearly contemplated by the individual – for example, to create and sell a list of people afflicted with high blood pressure to health insurance companies – then some form of notice should be provided.

15. While the Notice Principle indicates what might constitute the elements of adequate notice, it does not prescribe a particular form for that notice. Rather, the goal of the Principle is to ensure that the individual has sufficient information in an understandable form to make an informed decision. Thus the drafters of notices should be creative about informing in ways that will help all individuals, regardless of age, literacy, and education to achieve this goal.

16. Finally, although the Notice Principle requires information collectors to inform individuals what steps will be taken to protect personal information, they are not required to provide overly technical descriptions of such security measures. Indeed, such descriptions might be unwelcome or unhelpful to the individual. Furthermore, they may be counterproductive since widespread disclosure of the technical security measures might expose system vulnerabilities, in conflict with the Protection Principle (II. C.).

**II. C. Protection Principle**

**Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.**

17. On the NII, personal information is maintained in a networked environment, an environment that poses tremendous risk of unauthorized access, disclosure, alteration, and destruction. Both insiders and outsiders may gain access to information they have no right to see or may make hard-to-detect changes in data that will then be relied upon in making critical decisions.

18. For example, our health care providers expect to become intensive participants in the NII. Through the NII, a hospital in a remote locale will be able to send x-rays for review by a radiologist at a teaching hospital in another part of the country. The potential benefits are obvious. Yet, such benefits will not be realized if individuals refuse to send such sensitive data because they fear that the NII cannot ensure that sensitive medical data will remain confidential and unaltered.

19. In deciding what controls are appropriate, information users should recognize that personal information should be protected in accordance with the individual's understanding and in a manner commensurate with the harm that might occur if it were improperly disclosed or altered.

20. In protecting personal information, information users should adopt a multi-faceted approach that includes both technical and managerial controls. As for technical controls, information users should, for example, consider encrypting personal information, including the contents of communications and information generated from transactions. In addition, they should consider computerized audit trails, which help detect improper access by both insiders and outsiders. As for management controls, one could strive, for example, to create an organizational culture in which individuals learn about fair information practices and adopt these practices as the norm. Also, organizations could establish policies to forbid information acquired for one activity from being used for another unrelated activity.

**II. D. Fairness Principle**

**Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.**

21. An individual's understanding encompasses the individual's objectively reasonable contemplation and scope of consent when the information was collected. As explained earlier, an individual's understanding depends principally on the notice provided by the information collector pursuant to the Notice Principle (II. B.) and obtained by the individual pursuant to the Awareness Principle (III. A.). Without a Fairness Principle, information use may know no boundaries and thus go beyond the individual's understanding.

22. If an information user seeks to use personal information in an incompatible manner, the user must first notify the individual and obtain his or her explicit or implicit consent. The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate. Inherent in this principle is the requirement that whenever personal information is transferred from information user to user, the individual's understanding of how that personal information will be used must also be conveyed. Because all information users must abide by the Fairness principle, both information transferor and transferee bear a responsibility to ensure that the individual's understanding is transferred along with the information.

23. In deciding whether a particular use of information is "incompatible" with an individual's understanding, information users should evaluate whether the uses are permitted explicitly in the notice or are otherwise consistent with the notice. Any use of information beyond these conditions is incompatible with the individual's understanding. What is incompatible under this Principle is not limited to what has been interpreted as incompatible under the Privacy Act. (See 5 U.S.C. § 552 a.)

24. The Fairness Principle cannot be applied uniformly in every setting. An incompatible use is not necessarily a harmful use; in fact, it may be extremely beneficial to the individual and society. There are some incompatible uses that will produce enormous benefits and have at most a trivial effect on the individual's information privacy interest. Research and statistical studies, in which information will not be used to affect the individual, are examples. Obtaining the consent of the individual to permit new statistical uses of existing data adds cost and administrative complexity to the process and risks impairing the research project. In other cases, personal information may be used for a significant public need recognized by society in a highly formal, open way (typically in legislation) that would be thwarted by giving the individual a chance to limit its use. One example would be the use of personal information in a law enforcement investigation for which the suspect's consent would be unlikely and even asking for such consent would be counterproductive to the investigation. Another example would be an incompatible use of personal information, made by the investigatory press, that is specifically protected and sanctioned by the First Amendment.

**II. E. Education Principle**

**Information users should educate themselves and the public about how information privacy can be maintained.**

25. The Education Principle represents a significant addition to the traditional principles of fair information practice. There are many uses of the NII for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activities outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.

26. The full effect of the NII on the use of personal information is not readily apparent, and individuals may not recognize how their lives may be affected by networked information. Because it is important that individuals and information users appreciate how the NII affects information privacy, all information users should participate in education about the handling and use of personal information. Traditionally, governments and schools have educated the public on matters of social rights and responsibilities, and they must continue to play a lead role. However, as major builders of the NII, the private sector has as crucial a role to play. Such education, which would help individuals minimize the risks to their privacy, could involve privacy telephone hotlines, Internet privacy "help" sites, and comprehensive marketing and publicity campaigns.

## III. Principles for Individuals Who Provide Personal Information

### III. A. Awareness Principle

**Individuals should obtain adequate, relevant information about:**

1. **Why the information is being collected;**
2. **What the information is expected to be used for;**
3. **What steps will be taken to protect its confidentiality, integrity, and quality;**
4. **The consequences of providing or withholding information; and**
5. **Any rights of redress.**

27. Increasingly, individuals are being asked to surrender personal information about themselves. Sometimes the inquiry is straight-forward; for example, a bank will ask for personal information prior to processing a loan request. In this case, one use for the information is clear – to process the loan application. There may, however, be other uses that are not so obvious, such as using some of that information for a credit card solicitation. Indeed, individuals regularly disclose personal information without being fully aware of the many ways in which that information may ultimately be used. For example, an individual may not realize that paying for medical services with a credit card creates transactional data that could reveal the individual's state of health.

28. The Awareness Principle recognizes that although information collectors have a responsibility to inform individuals why they want personal information, individuals also have a responsibility to understand the consequences of providing personal information to others. This is especially true in an interactive realm such as the NII, in which individuals can actively shape the terms of their participation. For example, when individuals have real choices about whether and to what degree personal information should be disclosed, they should take an active role in deciding whether to disclose personal information in the first place, and under what terms.

29. Of course, if individuals are to be held responsible for making these choices, they must be given enough information to make intelligent choices. This is how the Awareness Principle works in conjunction with the Notice Principle (II. B.) and more broadly with the Education Principle (II. E) to enable individuals to take responsibility over how personal information is disclosed and used.





### III. B. Empowerment Principles

**Individuals should be able to safeguard their own privacy by having:**

1. **A means to obtain their personal information;**
2. **A means to correct their personal information that lacks sufficient quality to ensure fairness in its use;**
3. **The opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions; and**
4. **The opportunity to remain anonymous when appropriate.**

30. Individuals should have a means to obtain from information users a copy of their personal information and to correct information about them that lacks sufficient quality to ensure fairness in its use. The extent to which such means are provided depends on various factors, including the seriousness of the consequences to the individual of using the personal information and any First Amendment rights held by the information user.

31. Further, if the terms of the information collection are unsatisfactory, the individual should consider various self-initiated measures to safeguard privacy. For example, to safeguard the confidentiality or integrity of a communication, the individual should have the opportunity to use appropriate tools such as encryption. Also, to avoid leaving a data trail of transactional records, individuals should have the opportunity to remain anonymous, when appropriate. For example, anonymity would be appropriate when an individual browses a public electronic library or when an individual engages in anonymous political speech protected by the Constitution. See McIntyre v. Ohio Elections Commission, 131 L. Ed. 2d 426 (1995). In an ideal world, offering undecipherable encryption or absolute anonymity would serve to protect privacy with no negative effect. Unfortunately, in the real world, some will abuse these technologies and, in the process, harm others. It is beyond the scope of the Principles how encryption or anonymity can be offered to individuals for legitimate uses while minimizing their misuse. These issues must, however, be addressed if the NII is to achieve its full potential.

### III. C. Redress Principle

**Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.**

32. Redress is required only when an individual is harmed. Designed for general applicability, the Redress Principle does not answer in any particular case whether harm has occurred at all or whether enough harm has occurred to warrant a specific form of redress. Those questions must be answered in the sectoral implementation of the Principles.

33. An improper use specifically includes a decision based on personal information of inadequate quality – information that is not accurate, timely, complete, or relevant for the purpose for which it is provided and used. The Redress Principle does not, however, set the level of culpability on the part of the information user necessary to warrant a specific form of redress.

34. When redress is appropriate, the Principles envision various forms including, but not limited to, informal complaint resolution, mediation, arbitration, civil litigation, regulatory enforcement, and criminal prosecution, in various private, local, state, and federal forums with the goal of providing relief in the most cost-effective manner possible.





# F. Russische Föderation / Russian Federation

## I. Gesetz der Russischen Föderation über Information, Informatisierung und Informationsschutz

**Verabschiedet von der Staatlichen Duma am 25. Januar 1995**
**(Auszug)**

**– Übersetzung –**

### Teil 1

### Allgemeine Grundsätze

#### Artikel 1

#### Geltungsbereich dieses Gesetzes

1. Die Vorschriften dieses föderalen Gesetzes finden Anwendung für folgende Bereiche:
   - Gestaltung und Nutzung der Informationsressourcen, d. h.: Bildung, Sammlung, Bearbeitung, Verdichtung, Aufbewahrung, Recherche, Verbreitung und Zulieferung dokumentierter Information an die Benutzer,
   - Bildung und Nutzung der Informationstechnologien und entsprechender Schutzmaßnahmen,
   - Schutz der Informationen und Rechte der an den Informationsprozessen und an der Informatisierung beteiligten Subjekte.
2. Dieses föderale Gesetz findet Anwendung in den genannten Bereichen, soweit sie nicht unter die Vorschriften des föderalen Gesetzes über das Urheberrecht und ähnliche Rechte fallen.

#### Artikel 2

#### Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

„Information“ – Nachrichten über Personen, Objekte, Tatsachen, Ereignisse, Erscheinungen und Prozesse unabhängig von der Darstellungsform;

„Informatisierung“ – sozialökonomischer und wissenschaftstechnischer Organisationsprozeß, zwecks Schaffung von optimalen Bedingungen zur Befriedigung informationeller Bedürfnisse und Gewährung der Rechte von Bürgern, staatlichen und territorialen (kommunalen) Selbstverwaltungsorganen, gesellschaftlichen Organen, Institutionen im Zusammenhang mit der Gestaltung und Nutzung der Informationsressourcen;

„Dokumentierte Information (Dokument)“ – auf einem Informationsträger fixierte (gespeicherte) Information, zusammen mit den Identifikationsmerkmalen;

„Informationsprozesse“ – Erheben, Verarbeiten, Speichern, Aufbewahren, Aufsuchen (Recherche) und Verbreiten von Informationen;

„Informationssystem“ – organisatorisch geordnete Dokumentenmenge samt Informationstechnologien, inkl. EDV-Technik, die die Informationsprozesse ausführen;

„Informationsressourcen“ – einzelne Dokumente und Dokumentenmenge, Dokumente und Dokumentenmenge in den Informationssystemen (Bibliotheken, Archiven, Sammlungen, Datenbanken und in anderen Informationssammlungen);

„Informationen über Bürger (personenbezogene Daten)“ – Berichte über Fakten, Ereignisse und Lebensverhalten des Bürgers, die eine Identifizierung der einzelnen Bürger ermöglichen;

„Vertrauliche Informationen“ – dokumentierte Informationen, die aufgrund der geltenden Gesetzgebung nur teilweise (beschränkt) zugänglich sind;

„Mittel für die Sicherung der automatischen Informationssysteme und automatischen Informationstechnologien“ (im folgenden: „Informationssicherheitseinrichtungen“) – programmatische, technische, linguistische, rechtliche und organisatorische Einrichtungen (Software, Hardware und Nachrichtentechnik, Computerprogramme, Fachwörterbücher, Thesauren und Klassifikationen, Instruktionen und Methodiken, Pragmatika, Reglements, Schemata und ihre Beschreibungen wie auch jede andere Dokumentation), die bei der Entwicklung oder Ausnutzung der Informationssysteme entstehen und ihre Funktionsfähigkeit sichern;

„Eigentümer (Inhaber) der Informationsressourcen, Informationssysteme, -technologien und Informationssicherheitseinrichtungen“ – jedes Subjekt, welches unbegrenzt die Eigentumsrechte über diese Objekte ausüben darf;

„Besitzer der Informationsressourcen, Informationssysteme, -technologien und Informationssicherheitseinrichtungen“ – jedes Subjekt, welches über diese Objekte als Eigentümer und Besitzer verfügt und im gesetzlichen Rahmen über diese Anordnungen trifft;

„Informationsbenutzer“ – jedes Subjekt, welches seinen Informationsbedarf mit Hilfe eines Informationssystems oder eines Vermittlers befriedigt.

### Artikel 10

### Informationsressourcen, geordnet nach der Zugangsart

1. Staatliche Informationsressourcen der Russischen Föderation sind öffentlich; sie sind allgemein zugänglich. Ausnahmen betreffen die Informationsressourcen, soweit sie durch Gesetz als beschränkt zugänglich bezeichnet werden.
2. Beschränkt zugängliche dokumentierte Informationen bestehen aus den Staatsgeheimnisse betreffenden Informationen und aus den vertraulichen Informationen.
3. Es ist verboten, folgende Dokumente als Informationen mit beschränktem Zugang zu qualifizieren:
   - Gesetze und andere normative Akte, welche die rechtliche Position der Staatsorgane, territorialer Selbstverwaltungsorgane, Organisationen und gesellschaftlicher Vereine oder auch die Rechte, Freiheiten und Pflichten der Bürger und mit diesen verbundene Verfahren betreffen,





   - Dokumente, die über außergewöhnliche Ereignisse, ökologische, meteorologische, demographische, epidemiologische Fakten berichten oder auch andere Informationen beinhalten, die für das Funktionieren der Versorgungs- und Produktionseinrichtungen sowie für die Sicherheit der Bürger und Wirtschaft von Bedeutung sind;
   - Dokumente, die über die Tätigkeit der Staatsorgane und territorialer Selbstverwaltungsorgane, über die Nutzung der Haushaltsmittel oder anderer staatlicher und örtlicher Vorräte, über die Wirtschaftslage und auch über den Versorgungsbedarf berichten, ausgenommen die Staatsgeheimnisse betreffenden Dokumente;
   - Dokumente in den öffentlichen Sammlungen der Bibliotheken und Archive, Informationssysteme der Staatsorgane, Organe territorialer Selbstverwaltung, gesellschaftlicher Vereine und Organisationen, die von öffentlichem Interesse oder für die Ausübung der Bürgerrechte, -freiheiten und -pflichten unbedingt nötig sind.
4. Das föderale Gesetz „Über das Staatsgeheimnis“ bestimmt über die Bedeutung der Informationen für das Staatsgeheimnis.
5. Über die Vertraulichkeit von Informationen wird aufgrund der Gesetzgebung der Russischen Föderation entschieden; Artikel 11 dieses föderalen Gesetzes ist anzuwenden.

### Artikel 11

### Informationen über Bürger (personenbezogene Daten)

1. Die Art der personenbezogenen Daten, die in den föderalen Informationsressourcen, Informationsressourcen der territorialen Selbstverwaltungsorgane und nichtstaatlichen Organisationen gespeichert werden sollen, wird durch föderales Gesetz festgelegt.

   Personenbezogene Daten werden als vertrauliche Informationen betrachtet.

   Das Erheben, Speichern, Nutzen und Verbreiten der Informationen über das Privatleben und Verarbeiten von Informationen, welche das persönliche und familiäre Geheimnis betreffen, und Eingriffe in das Post-, Fernmelde-, Telegrammgeheimnis sowie das Geheimnis der anderen Kommunikationsarten zwischen den Personen sind nur zulässig, wenn eine Rechtsvorschrift dies vorsieht oder der Betroffene eingewilligt hat.
2. Personenbezogene Daten dürfen nicht genutzt werden, um den Bürgern wirtschaftlichen und moralischen Schaden zuzufügen oder um die Ausübung der Rechte und Freiheiten der Bürger der Russischen Föderation zu erschweren. Beschränkungen der Bürgerrechte aufgrund der Informationen über soziale Herkunft, Rasse, Nationalität, Sprache, Religion, Parteimitgliedschaft sind verboten und werden dem Gesetz entsprechend bestraft.
3. Natürliche und juristische Personen, die aufgrund ihrer Zuständigkeit die personenbezogenen Daten verarbeiten, erheben oder nutzen, tragen aufgrund der Gesetzgebung der Russischen Föderation die Verantwortung für die Verletzung der Vorschriften, die das Sammeln, Bearbeiten und Nutzen von diesen Informationen regeln.

4. Die mit der Verarbeitung und Auswertung der personenbezogenen Daten verbundene Tätigkeit nichtstaatlicher Organisationen und Privatpersonen wird obligatorisch lizenziert. Das Lizenzverfahren wird in der Gesetzgebung der Russischen Föderation festgelegt.
5. Auf Antrag der nach Artikel 14 und 15 dieses Gesetzes und entsprechenden Vorschriften des Gesetzes über personenbezogene Daten handelnden Subjekte darf die Gesetzwidrigkeit des Speicherns von personenbezogenen Daten durch Staatsorgane und Organisationen in einem Gerichtsverfahren festgestellt werden.

## Teil 3

## Nutzung der Informationsressourcen

### Artikel 12

### Verwirklichung des Zugangsrechts zu den Informationen in Informationsressourcen

1. Die Benutzer – Bürger, staatliche Organe, territoriale Selbstverwaltungsorgane, Organisationen und gesellschaftliche Vereine – verfügen über gleiche Zugangsrechte zu den staatlichen Informationsressourcen und sind nicht verpflichtet, die Notwendigkeit ihres Bedarfs nachzuweisen. Ausnahme bilden die beschränkt zugänglichen Informationen.

   Der Zugang der natürlichen und juristischen Personen zu den staatlichen Informationsressourcen stellt eine wichtige Voraussetzung für Durchführung sozialer Kontrolle aller Staatsorgane, territorialer Selbstverwaltungsorgane, gesellschaftlicher, politischer und anderer Organisationen dar; auf diese Weise werden auch die Kontrolle der ökonomischen und ökologischen Lage sowie die Kontrolle in den anderen Bereichen des gesellschaftlichen Lebens erleichtert.
2. Die Besitzer informationeller Ressourcen gewähren entsprechend den Satzungen, Dienstordnungen und Informationslieferungsverträgen den Informationsbenutzern Zugang zu den von ihnen benötigten Informationen aufgrund der geltenden Gesetzgebung.

   Informationen, welche die Bürger und Organisationen aus den staatlichen Informationsressourcen erhalten, dürfen zur Erstellung von kommerziellen Informationen genutzt werden; auf diese Weise veränderte Informationen dürfen danach nur mit Hinweis auf ihre Herkunft verbreitet werden.

   Die Gewinnquelle resultiert in diesem Fall zwar aus der Menge der bei der Schaffung der kommerziellen Informationen verwendeten Arbeit und angewandten Mittel, jedoch ist die Entstehung der Information aus den Informationsressourcen unvermeidbar.
3. Die Ordnung des Informationszugangs (Zugangsort, -zeit, verantwortliche Personen, obligatorische Verfahren) wird von den Eigentümern bzw. Besitzern der Informationsressourcen festgelegt; sie sind dabei verpflichtet, die gesetzlichen Bedingungen zu berücksichtigen.

   Verzeichnisse von Informationen und Informationsleistungen wie auch Informationen über das Verfahren und die Bedingungen des Informationszugangs stehen den Benutzern kostenlos zur Verfügung.





4. Die für das Gestalten und Nutzen der Informationsressourcen verantwortlichen Staatsorgane und Organisationen sichern den Interessenten einen effektiven und ungehinderten Zugang zu den dokumentierten Informationen gemäß den in ihren Satzungen genannten Pflichten.
5. Art und Weise der Erhebung und Speicherung dokumentierter Informationen mit beschränktem Zugang sowie diese betreffende Schutzregeln und Nutzungsbedingungen nennen die Staatsorgane, die für eine bestimmte Informationsart oder Informationsmenge verantwortlich sind. Sie dürfen auch direkt durch die Informationseigentümer entsprechend den Rechtsvorschriften festgelegt werden.

### Artikel 13

### Gewährung des Informationszugangs

1. Staatsorgane und territoriale Selbstverwaltungsorgane sind verpflichtet, allgemein zugängliche Informationssammlungen einzurichten, die Informationen über ihren Tätigkeitsbereich wie auch über die Tätigkeitsbereiche der ihnen untergeordneten Organisationen enthalten.

   Im Rahmen ihrer Zuständigkeit sichern sie auch der Öffentlichkeit den Zugang zu den Informationen über Freiheiten und Pflichten der Bürger, über ihre Sicherheit wie auch zu den anderen Informationen, die aus der Sicht der Öffentlichkeit von Bedeutung sind.
2. Gegen die Verweigerung des Zuganges zu den in Artikel 13 Absatz 1 erwähnten Informationsressourcen steht der Rechtsweg offen.
3. Das Komitee für Informatisierungspolitik beim Präsidenten der Russischen Föderation führt die Registrierung aller Informationsressourcen, Informationssysteme und diese betreffenden Veröffentlichungen durch, um auf diese Weise das Recht auf Informationszugang zu garantieren.
4. Die Regierung der Russischen Föderation stellt ein Informationsdienstleistungsverzeichnis her, welches Benutzer der staatlichen Informationsressourcen entgeltlich, unentgeltlich oder teilweise entgeltlich in Anspruch nehmen dürfen.

   Die durch diese Dienstleistungen verursachten Kosten werden aus den Haushaltsmitteln der Russischen Föderation bzw. deren Subjekte erstattet.

### Artikel 14

### Zugang der Bürger und Organisationen zu den über sie gespeicherten Informationen

1. Bürger und Organisationen haben das Recht auf Zugang zu den sie betreffenden dokumentierten Informationen, auf ihre Berichtigung und Ergänzung, zwecks Gewährleistung der Glaubwürdigkeit und Vollständigkeit dieser Informationen. Sie haben das Recht, informiert zu werden, wer und zu welchem Zweck diese Informationen nutzt oder früher genutzt hatte.

   Eine Beschränkung der Rechte von Bürgern und Organisationen auf Zugang zu den sie betreffenden Informationen kann nur aufgrund der föderalen Gesetze erfolgen.

2. Die Stellen, die den Bürger betreffende Informationen verarbeiten, sind verpflichtet, den Betroffenen diese Informationen gebührenfrei zugänglich zu machen. Begrenzungen dieser Pflicht sind nur unter den gesetzlichen Voraussetzungen zulässig.
3. Subjekte, die sie betreffende Informationen entsprechend den Artikeln 7 und 8 dieses Gesetzes zwecks Bildung der Informationsressourcen einliefern, sind berechtigt, diese Informationen gebührenfrei in Anspruch zu nehmen.
4. Verweigert der Inhaber von Informationsressourcen dem Betroffenen den Zugang zu ihn betreffenden Informationen, steht diesem der Rechtsweg offen.

**Artikel 15**

**Pflichten und Haftung des Inhabers von Infomationsressourcen**

1. Inhaber der Informationsressourcen sind verpflichtet, die durch die Gesetzgebung der Russischen Föderation oder durch den Informationsressourceneigentümer bestimmten Verarbeitungsbedingungen und Informationszugangsregeln zu erfüllen.
2. Inhaber von Informationsressourcen haften für die Verletzung des in der Gesetzgebung der Russischen Föderation vorgesehenen Informationsverfahrens.

## Teil 5

## Schutz der Informationen und subjektiven Rechte im Verlauf der Informations- und Informatisierungsprozesse

**Artikel 20**

**Ziel des Schutzes**

Ziel des Schutzes ist es:

- den Abgang, den Diebstahl, den Verlust und das Fälschen von Informationen zu verhindern;
- Gefahren für die Sicherheit der Personen, der Gesellschaft und des Staates auszuschließen;
- die unerlaubte Vernichtung, Veränderung, Fälschung, Vervielfältigung, Sperrung und andere rechtswidrige Eingriffsarten in die Informationsressourcen und Informationssysteme zu verhindern;
- die Eigentumsrechte an dokumentierten Informationen zu sichern;
- die Verfassungsrechte der Bürger auf Schutz der Privatsphäre und Vertraulichkeit der personenbezogenen Daten in den Informationssystemen zu gewähren;
- das Staatsgeheimnis und die Vertraulichkeit der dokumentierten Informationen entsprechend der geltenden Gesetzgebung zu gewähren;
- die Rechte der Subjekte im Verlaufe der Informationsprozesse und beim Entwerfen, Herstellen und Nutzen von Informationssystemen, -technologien und Informationssicherheitseinrichtungen zu schützen.





**Artikel 21**

**Informationsschutz**

1. Geschützt wird jede dokumentierte Information, die bei einem unzulässigen Umgang mit ihr zu Schäden für Eigentümer, Besitzer oder für andere Personen führen könnte.

   Das Informationsschutzregime soll für einzelne Informationskategorien durch folgende Subjekte hergestellt werden:

   - die zuständigen, im föderalen Gesetz „Über das Staatsgeheimnis“ genannten Organe bestimmen entsprechend der Schutzordnung das Staatsgeheimnis betreffende Informationen;
   - die Inhaber der Informationsressourcen bzw. die von ihnen beauftragten Personen, entsprechend dem vorliegenden föderalen Gesetz, im Falle der vertraulichen Informationen.

   Den Informationsschutz für die personenbezogenen Daten regeln die Vorschriften dieses Gesetzes.
2. Staatsorgane und Organisationen, die für Gestaltung und Nutzung der schutzbedürftigen Informationsressourcen verantwortlich sind, wie auch Organe und Organisationen, die Informationssysteme und Informationstechnologien für Verarbeitung der Informationen mit beschränktem Zugang herstellen und nutzen, unterliegen in ihrer Tätigkeit der Gesetzgebung der Russischen Föderation.
3. Die Kontrolle des Informationsschutzes, der entsprechenden Software- und Hardwaremittel wie auch der organisatorischen Regeln, nach denen die beschränkt zugänglichen Informationen in den Informationssystemen verarbeitet werden, üben die Staatsorgane aus. Diese Kontrolle wird nach den Regeln ausgeführt, die durch die Regierung der Russischen Föderation bestimmt sind.
4. Organisationen, die staatseigene Informationen mit beschränktem Zugang verarbeiten, sind auch verpflichtet, die speziellen Informationsschutzdienste einzurichten.
5. Inhaber der Informationsressourcen oder die von ihm bevollmächtigten Personen können das Beachten der Informationsschutzmaßnahmen prüfen und die Informationsverarbeitung verbieten oder einstellen, wenn die Schutzregeln nicht beachtet werden.
6. Eigentümer oder Besitzer der dokumentierten Informationen dürfen sich an die Staatsorgane wenden, um festzustellen, ob ihre Informationen unter Beachtung der Informationsschutzregeln verarbeitet sind. Entsprechende Kontrollorgane werden durch Regierung der Russischen Föderation benannt. Diese Organe sind verpflichtet, selbst die Bedingungen der Informationsvertraulichkeit zu beachten und Kontrollergebnisse vertraulich zu behandeln.

**Artikel 22**

**Rechte und Pflichten der Subjekte im Bereich des Informationsschutzes**

1. Die Eigentümer der Dokumente, Dokumentenmengen und Informationssysteme oder die von ihnen bevollmächtigten Personen bestimmen im Einklang mit dem ent-

sprechenden Föderalgesetz ein Reglement der Informationsnutzung. Im Reglement werden der Ort, die Zeit, die verantwortlichen Personen und das Verarbeitungsverfahren genannt.

2. Die Besitzer der Dokumente, Dokumentenmengen und Informationssysteme sichern ein maßgebendes Informationsschutzniveau entsprechend der Gesetzgebung der Russischen Föderation.

3. Das mit der Inanspruchnahme von nichtzertifizierten Informationssystemen und nichtzertifizierten Informationsschutzeinrichtungen verbundene Risiko trägt deren Inhaber.

   Die Nutzung einer aus nichtlizenzierten Informationssystemen entnommenen Information geschieht auf das Risiko des Informationsbenutzers.

4. Die Inhaber der Dokumente, Dokumentenmengen oder Informationssysteme dürfen sich an die mit der Zertifizierung beschäftigten Organisationen wenden und eine Prüfung des Informationszustandes in den ihm gehörenden Informationsressourcen und Informationssystemen verlangen; sie dürfen auch eine Beratung fordern.

5. Die Besitzer der Dokumente, Dokumentenmengen und Informationssysteme sind verpflichtet, den Eigentümer der Informationsressourcen und/oder Informationssysteme über alle Verletzungen der Informationsschutzvorschriften zu unterrichten.

### Artikel 23

### Schutz der subjektiven Rechte im Bereich der Informationsprozesse und Informatisierung

1. Das Gewähren von subjektiven Rechten beim Gestalten und Nutzen von Informationsressourcen, beim Entwerfen, Herstellen und Nutzen von Informationssystemen, -technologien und Informationsschutzeinrichtungen soll vor den Rechtsverletzungen und illegalen Handlungen schützen, zur Wiederherstellung der Rechtsordnung beitragen und die Entschädigung der Betroffenen sichern.

2. Den Schutz der Subjekte im genannten Bereich verwirklichen Gerichte, Schiedsgerichte, Arbitragekommissionen bei Berücksichtigung der Eigenart der dabei entstehenden Rechtsverletzungen und Schäden.

3. Die Verantwortung für Rechtsverletzungen, die bei dem Umgang mit den dokumentierten Informationen entstehen können, tragen Staatsorgane, Organisationen und verantwortliche Personen entsprechend der Gesetzgebung der Russischen Föderation und ihrer Subjekte.

   Zwecks Untersuchung der Konfliktsituationen und Gewährung der Rechte beim Gestalten von Informationsressourcen, Einrichten und Nutzen von Informationssystemen, -technologien und Informationsschutzeinrichtungen können zeitbegrenzte oder dauerhafte Schiedsgerichte gebildet werden.

   Die Schiedsgerichte entscheiden über die ihnen vorgelegten Konflikte und Streitigkeiten. Sie richten sich dabei nach der Verfahrensordnung, die durch die Gesetzgebung für das schiedsgerichtliche Verfahren bestimmt wurde.





4. Die Verantwortung für die Verletzung der internationalen Normen und Regeln bei der Gestaltung und Nutzung der Informationsressourcen, bei der Herstellung und Ausnutzung der Informationssysteme, -technologien und Informationsschutzeinrichtungen tragen die Staatsorgane, Organisationen und Bürger im Einklang mit Verträgen, die mit den ausländischen Partnern geschlossen wurden. Es sollen dabei die entsprechenden internationalen Verträge der Russischen Föderation berücksichtigt werden.

### Artikel 24

### Schutz des Informationszugangsrechts

1. Die Verweigerung des Zugangs zu den allgemein zugänglichen Informationen oder absichtliche Erteilung unvollständiger Informationen darf vor Gericht angefochten werden.

   Den Streit zwischen den Organisationen um Nichterfüllung oder nicht ausreichende Erfüllung der aus den Lieferverträgen, Kaufverträgen oder aus den anderen rechtlichen Formen folgenden Informationsverpflichtungen schlichten die Arbitragegerichte.

   Personen, denen der Zugang zu Informationen verweigert wurde oder welche nur unvollständige Informationen erhielten, dürfen entsprechende Entschädigung (Schadenswiedergutmachung) verlangen.

2. Das Gericht entscheidet im Streit über Qualifizierung bzw. Nichtqualifizierung einer Information als beschränkt zugängliche Information und über Schadenswiedergutmachung im Fall einer unbegründeten Informationsverweigerung oder anderer Rechtsverletzungen von Informationsbenutzern.

3. Leiter und andere Angestellten der Staatsorgane und Organisationen, die für die rechtswidrige Zugangsrechtsbegrenzung und Verletzung der Informationsschutzordnung verantwortlich sind, haften aufgrund des Straf-, Zivil- und Verwaltungsrechts.

### Artikel 25

### Inkrafttreten dieses föderalen Gesetzes

1. Dieses Gesetz tritt am Tage nach der offiziellen Veröffentlichung in Kraft.

2. Dem Präsidenten der Russischen Föderation wird vorgeschlagen, die von ihm erlassenen Rechtsakte mit diesem Gesetz zu koordinieren.

3. Der Regierung der Russischen Föderation wird empfohlen:

   - die von der Regierung erlassenen Rechtsakte diesem Gesetz anzupassen;
   - die entsprechenden Veränderungen in der Gesetzgebung der Russischen Föderation innerhalb der Dreimonatsfrist im vorgesehenen Verfahren der Staatlichen Duma vorzuschlagen;
   - die entsprechenden Rechtsakte zu verabschieden, die das Ausführen dieses Gesetzes ermöglichen.

# II. Russian Federation
# Law of the Russian Federation on Information, Informatisation and Information Protection

**Passed by the State Duma on 25th January 1995**
**(Extracts)**

**– Translation –**

## Part 1

## General principles

### Article 1

### Scope of this law

1. The provisions of this federal law apply to the following areas:
   - Structuring and use of the information resources, i. e. formation, collection, editing, collation, retention, official search, dissemination and supply of documented information to the users,
   - Formation and use of information techologies and corresponding protective measures,
   - Protection of information and the rights of subjects involved with the information processes and informatisation.
2. This federal law has applications in the specified areas, so far as they do not come under the provisions of the federal law “On the Copyright and similar rights”.

### Article 2

### Definition of terms

Terms in the sense of this law:

“Information” – Messages about persons, objects, facts, events, phenomena and processes independent of the form in which they are represented;

“Informatisation” – Economic and scientific organisational process for the purpose of creating optimal conditions for satisfying information requirements and granting the rights of citizens, governmental and territorial (agencies, municipal) self-governing bodies, organisations, social institutions in connection with the structuring and use of information resources;

“Documented information (Document)” – Information fixed (stored) on an information carrier, together with the identification marks;

“Information processes” – Collection, processing, storage, retention, search and dissemination of information;

“Information system” – Organisationally arranged document set together with information technologies, including computer-based techniques, which execute the information processes;

"Information resources" – Individual documents and document sets, documents and document sets in the information systems (libraries, archives, collections, databases and other information collections);

"Information about citizens (personal data)" – Reports on facts, events and lifestyles of citizens which allow for the identification of individual citizens;

"Confidential information" – Documented information which because of the applicable legislation is only partially (with restrictions) accessible;

"Means of safeguarding automated information systems and automated information technologies" (subsequently: "Information security facilities") – Programmed, technical, linguistic, legal and organisational facilities (software, hardware and telecommunications, computer programs, technical dictionaries, thesauri and classifications, instructions and methodologies, pragmatics, rules, plans and their descriptions and other documentation), which emerge in the development or exploitation of the information systems and safeguard their ability to function;

"Owner (holder) of the information resources, information systems, technologies and information security facilities" – Any subject who may exercise the proprietary rights over these objects without restriction;

"Possessor of the information resources, information systems, technologies and information security facilities" – Any subject who has these objects at his disposal as owner and possessor and disposes of them in a legal framework;

"Information user" – Any subject who satisfies his information requirements with the help of an information system or an intermediary.

**Article 10**

**Information resources arranged by type of access**

1. Government information resources of the Russian Federation are public; they are generally accessible. Exceptions relate to the information resources in so far as they have been designated by law as for restricted access.

2. Documented information for restricted access arises from the information concerning state secrecy and from confidential information.

3. It is forbidden to qualify the following documents as information with restricted access:

   - Laws and other regulations which concern the legal position of the government bodies, territorial self-governing bodies, organisations and social associations, or the rights, freedoms and duties of the citizens, and procedures involved;

   - Documents which report on unusual events, ecological, meteorological, demographic, health and epidemic-related facts, or contain other information which is of importance for the functioning of supply and production facilities or for the safety of the citizens and the economy;





   - Documents which report on activities of the government bodies and territorial self-governing bodies, on use of the budget funds or other governmental and local stocks, on economic situation and supply requirements, except for documents affecting state secrets.

   - Documents in the public collections of libraries and archives, information systems of government bodies, territorial self-governing bodies, social associations and organisations, which are of public interest or essential for the exercise of citizens' rights, freedoms and duties.

4. The federal law "On State Secrecy" determines the significance of the information for state secrecy.

5. The decision about confidentiality of information is made on the basis of the Russian Federation's legislation; Section 11 of this federal law should be applied.

**Article 11**

**Information on citizens (personal data)**

1. The nature of personal data which should be stored in the federal information resources, information resources of the territorial self-governing bodies and non-government organisations is specified by federal law.

   Personal data is regarded as confidential information.

   Collection, storage, usage and dissemination of information about private life, and processing of information which concerns personal and family secrecy, or encroaches upon post, telephone or telegram secrecy or the secrecy of other forms of communication between persons is only permissible if a legal provision provides for this, or the person affected has agreed.

2. Personal data may not be used to inflict economic or moral damage on citizens, or to impede the exercise of the rights and freedoms of the citizens of the Russian Federation. Restriction of the citizens' rights on the basis of information on social origin, race, nationality, language, religion or party membership is forbidden and is punished according to the law.

3. Natural and legal persons, who within their jurisdiction process, collect or use personal data, bear the responsibility based on the Russian Federal legislation for the violation of the provisions which govern the collection, processing and use of this information.

4. The activity of non-government organisations and private persons in the processing of personal information is compulsorily licensed. The licensing procedure is specified in the Russian Federal legislation.

5. On application by the subjects acting according to Sections 14 and 15 of this law and corresponding provisions of the law on personal data, the illegality of the storage of personal data undertaken by the government bodies and organisations may be established in legal proceedings.

## Part 3

## Use of the Information Resources

### Article 12

### Realization of the access right to the information contained in resources

1. The users – citizens, government bodies, territorial self-governing bodies, organisations and social associations – have the same rights at their disposal to the government information resources, and are not obliged to demonstrate the necessity of their requirement. The exception is the restricted access information.

   The access of the natural and legal persons to the government information resources represents an important precondition for the execution of social control of all government bodies, territorial self-governing bodies, social, political and other organisations; the control of the economic and ecological situation and control in the other areas of community life are also made easier by this means.

2. According to the statutes, official regulations and information supply agreements, the possessors of informational resources grant information users access to the information needed by them on the basis of the applicable legislation.

   Information which the citizens and organisations obtain from the government information resources may be used for preparing commercial information; information altered in this way may only be disseminated afterwards with references to its origin.

   The source of profit results in this case from the aggregate of work used in creating the commercial information and applied resources, but the emergence of the information from the information resources is unavoidable.

3. Information access arrangements (access location and time, persons responsible, obligatory procedures) are specified by the owners or possessors of the information resources; these are obliged to take into account the legal conditions.

   Directories of information and information services, as well as information about the procedures and conditions of access to information, are available to the users free of charge.

4. Government bodies and other organisations responsible for the structuring and use of the information resources assure operative and unimpeded access to the documented information for those who need it, according to the duties specified in their statutes.

5. The way of collecting and storing documented information with restricted access, and the protection rules and conditions of use relating to this, are given by the government bodies who are responsible for certain types of information or information sets. They may also be specified directly by the information owner according to the legal provisions.

### Article 13

### Granting access to information

1. Government bodies and territorial self-governing bodies are obliged to establish generally accessible information collections, which store information about their area of operation and those of their subordinate organisations.





   Within their jurisdiction they also guarantee public access to the information about citizens' freedoms and duties, and about their safety; and also to the other information which is important from the point of view of the public interest.

2. Refusal of access to the information resources mentioned in Section 13 Subsection 1 can be challenged in court.

3. The Committee for Informatisation Policy of the President of the Russian Federation is carrying out the registration of all information resources, information systems and publications concerning this, in order to guarantee thereby the right to information access.

4. The Government of the Russian Federation is setting up an information services directory, which users of the government information resources may take advantage of, against payment, without payment or partially against payment.

   Costs arising from these services are reimbursed from the budget funds of the Russian Federation or its subjects.

### Article 14

### Access of citizens and organisations to the information stored about them

1. Citizens and organisations have the right of access to the documented information about them, to correct it and supplement it, for the purpose of ensuring the credibility and completeness of this information. They have the right to be informed who is using this information or had previously used it, and for what purpose.

   Restrictions on the rights of citizens and organisations to access information concerning them can only come into being on the basis of the federal laws.

2. The processors of the documented information concerning the citizens are obliged to make the information available to those concerned without charge. Limitations of this liability are only permitted under the statutory conditions.

3. Subjects who surrender information concerning themselves according to sections 7 and 8 of this law, for the purpose of forming the information resources, are entitled to make use of this information free of charge.

4. If the holder of information resources refuses the person concerned access to the information concerning him, this person can bring proceedings in court.

### Article 15

### Obligations and liabilities of the holder of information resources

1. Holders of information resources are obliged to satisfy the processing conditions and information access rules determined by the legislation of the Russian Federation or by the owner of the information resource.

2. Holders of information resources are liable for the violation of the information procedure envisaged in the legislation of the Russian Federation.

## Part 5

## Protection of information and subjects' rights in the course of the information and informatisation processes

### Article 20

### Aim of the protection

Aim of the protection is:

- to prevent the decrease, theft, loss and falsifying of information;
- to remove dangers to the security of persons, society and the state;
- to prevent unauthorised destruction, changing, falsifying, copying, locking and other illegal forms of intervention in the information resources and information systems;
- to secure rights of ownership to documented information;
- to grant constitutional rights of citizens to privacy and confidentiality of personal data in the information systems;
- to grant state secrecy and confidentiality of the documented information according to the applicable legislation;
- to protect rights of subjects in the course of information processes and in the design, manufacture and use of information systems, technologies and information security facilities.

### Article 21

### Information protection

1. All documented information, unauthorised access to which could lead to damage for owners, possessors, or other persons, is protected.

   The information protection regime should be established for individual categories of information by the following subjects:

   - Responsible bodies, named in the federal law „On State Secrecy" to determine the corresponding protection order for information affecting state secrecy
   - The holders of information resources, or their representatives, according to the present federal law, in the case of the confidential information.

   The provisions of this law determine the information protection for the personal data.

2. Government bodies and organisations which are responsible for the structuring and use of the information resources which require protection, and similarly bodies and organisations which produce and use information systems and information technologies for processing restricted access information, are subject to the legislation of the Russian Federation in their activity.
3. The government bodies exercise control of information protection, of the corresponding software and hardware resources and also of the organisational rules by which the restricted access information is processed in the information systems. This control is executed according to the rules determined by the government of the Russian Federation.





4. Organisations which process government-owned restricted access information are also obliged to set up special information protection services.
5. The holders of information resources, or the persons authorised by them, can check the observance of the information protection measures, and forbid or suspend information processing if the protection rules are not observed.
6. The owner or possessor of the documented information may approach the government bodies to discover whether his information is processed in observance of the information protection rules. Appropriate monitoring bodies are named by the government of the Russian Federation. These bodies are obliged themselves to observe the conditions of information confidentiality, and regard monitoring results as confidential.

### Article 22

### Rights and obligations of the subjects in the area of information protection

1. The owner of documents, document sets and information systems or the persons authorised by him draw up, in accordance with the corresponding federal law, rules on information usage. The location, time, persons responsible and the processing procedure are specified in these rules.
2. The possessors of documents, document sets and information systems secure a qualifying information protection level according to the legislation of the Russian Federation.
3. The risk involved in the use of non-certified information systems and non-certified information protection facilities is borne by their holders.

   Use of information taken from non-licensed information systems is at the information user's risk.

4. The holder of documents, document sets and information systems may approach organisations concerned with certification, and request a check of the information protection in the information resources and information systems belonging to him; he may also request advice.
5. The possessor of the documents, document sets and information systems is obliged to inform the owner of the information resources and/or information systems about all violations of the information protection provisions.

### Article 23

### Protection of subjects' rights in the area of information processes and information

1. The granting of subjects' rights in the structuring and use of information resources, in designing, producing and using information systems, technologies and information protection facilities should protect against violations of law and illegal dealings, contribute to the restoration of the legal system and secure the compensation of those affected.
2. The courts, arbitration tribunals and arbitration commissions implement the protection of the subjects in the given areas, taking into account the peculiarities of violations of law and damages thereby arising.

3. Responsibility for violations of law which can arise in dealing with the documented information is borne by the government bodies, organisations and responsible persons according to the legislation of the Russian Federation and the legislation of its subjects.

   For the purpose of investigating the conflict situations and granting personal rights, in the structuring of information resources, setting up and use of information systems, technologies and information protection facilities, arbitration tribunals can be formed for a limited period or permanently.

   Arbitration tribunals decide upon conflicts and settle disputes submitted to them. They are guided by the procedural order which was determined by legislation for the procedures of arbitration tribunals.

4. Responsibility for violations of the international norms and rules in the structuring and use of the information resources, production and exploitation of the information systems, technologies and information protection facilities is borne by the government bodies, organisations and citizens in accord with agreements which were concluded with the foreign partners. The corresponding international agreements of the Russian Federation should be taken into account.

**Article 24**

**Protection of the information access right**

1. Refusal of access to the generally accessible information, or deliberate issue of incomplete information, may lead to prosecution.

   Arbitration courts settle disputes between the organisations about non-fulfilment or inadequate fulfilment of the information obligations following from the delivery contracts, purchase contracts or other legal forms.

   Persons who were denied access to information or received incomplete information only may demand corresponding compensation/reparations for damage.

2. The court decides in disputes about qualification or non-qualification of an item of information as for restricted access, and decides about reparations for damages in the case of an unjustified refusal of information or other violations of the rights of information users.

3. Managers and other staff of government bodies and organisations which are responsible for illegal restriction of access rights and violation of the information protection order are liable under the criminal, civil and administrative law.

**Article 25**

**Coming into force of this federal law**

1. This law comes into force on the day after the official publication.

2. It is proposed to the president of the Russian Federation that legal deeds passed by him are coordinated with this law.





3. The government of the Russian Federation is recommended:
   - to adapt legal deeds passed by the government to this law;
   - to propose to the State Duma the corresponding changes in the legislation of the Russian Federation within a period of three months, in the envisaged procedure;

   to pass the corresponding legal deeds.