Federal Ministry of Education, Science, Research and Technology

# Federal Act
# Establishing the General Conditions
# for Information and Communication Services
# - Information and Communication Services Act -

(*Informations- und Kommunikationsdienste-Gesetz - IuKDG*)

August 1 1997

*The text of this act and further documents can be found under the URL:*

*http://www.iid.de*

T a b l e o f C o n t e n t s

## Article 1

## Act on the Utilization of Teleservices
## (Teleservices Act - *Teledienstegesetz TDG*)

### § 1: Purpose of the Act

The purpose of this Act is to establish uniform economic conditions for the various applications of electronic information and communication services.

### § 2: Scope

(1) The following provisions shall apply to all electronic information and communication services which are designed for the individual use of combinable data such as characters, images or sounds and are based on transmission by means of telecommunication (teleservices).

(2) Teleservices within the meaning of § 2 (1) shall include in particular:

1. services offered in the field of individual communication (e.g. telebanking, data exchange),

2. services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environmental and stock exchange data, the dissemination of information on goods and services),

3. services providing access to the Internet or other networks,

4. services offering access to telegames,

5. goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order.

(3) § 2 (1) shall apply irrespective of whether the use of the teleservices is free of charge either wholly or partially.

(4) This Act shall not apply to

1. telecommunications services and the commercial provision of telecommunications services under § 3 of the Telecommunications Act of 25 July 1996 (*Telekommunikationsgesetz* , Federal Law Gazette *BGBl.* I, page 1120),

2. broadcasting as defined in § 2 of the Interstate Agreement on Broadcasting (*Rundfunkstaatsvertrag*),

3. content provided by distribution and on-demand services if the emphasis is an editorial arrangement to form public opinion pursuant to § 2 of the Interstate Agreement on Media Services *(Mediendienste-Staatsvertrag)* signed between 20 January and 7 February 1997.

(5) Legal provisions concerning press law remain unaffected.

**§ 3: Definitions**

For the purposes of this Act

1. the term "providers" means natural or legal persons or associations of persons who make available either their own or third-party teleservices or who provide access to the use of teleservices,

2. the term "users" means natural or legal persons or associations of persons requesting teleservices.

**§ 4: Freedom of access**

Within the scope of the law, teleservices shall not be subject to licensing or registration.

**§ 5: Responsibility**

(1) Providers shall be responsible in accordance with general laws for their own content, which they make available for use.

(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.

(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.

(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telecommunications Act (*Telekommunikationsgesetz*) and if blocking is technically feasible and can reasonably be expected.

**§ 6: Identification of providers**

Concerning commercial offers, providers shall indicate:

1. their name and address as well as,

2. in case of associations and groups of persons, the name and address of their authorized representative.

## Article 2
## Act on the Protection of Personal Data Used in Teleservices
## (Teleservices Data Protection Act - *Teledienstedatenschutzgesetz TDDSG*)

### § 1: Scope

(1) The following provisions shall apply to the protection of personal data used in teleservices within the meaning of the Teleservices Act.

(2) Unless otherwise provided in this Act, the relevant provisions concerning the protection of personal data shall be applicable even if the data are not processed or used in data files.

### § 2: Definitions

For the purposes of this Act

1. the term "providers" means natural or legal persons or associations of persons who make available teleservices or who provide access to the use of teleservices,

2. the term "users" means natural or legal persons or associations of persons requesting teleservices.

### § 3: Principles for the processing of personal data

(1) Personal data may be collected, processed and used by providers for performing teleservices only if permitted by this Act or some other regulation or if the user has given his consent.

(2) The provider may use the data collected for performing teleservices for other purposes only if permitted by this Act or some other regulation or if the user has given his consent.

(3) The provider shall not make the rendering of teleservices conditional upon the consent of the user to the effect that his data may be processed or used for other purposes if other access to these teleservices is not or not reasonably provided to the user.

(4) The design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible.

(5) The user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data. In case of automated processing, which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure. The content of such information shall be accessible to the user at any time. The user may waive such information. A record shall be made of the information and the waiver. The waiver shall not constitute consent within the meaning of § 3 (1) and (2).

(6) Before giving his consent, the user shall be informed about his right to withdraw his consent at any time with effect for the future. Sentence 3 of § 3 (5) shall apply mutatis mutandis.

(7) Consent can also be declared electronically if the provider ensures that

1. such consent can be given only through an unambigious and deliberate act by the user,

2. consent cannot be modified without detection,

3. the creator can be identified,

4. the consent is recorded and

5. the text of the consent can be obtained by the user on request at any time.

**§ 4: Obligations of the provider**

(1) The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options.

(2) The provider shall take technical and organizational precautions to ensure that

1. the user can break off his connection with the provider at any time,

2. the personal data generated in connection with the process of requesting, accessing or otherwise using teleservices are erased immediately upon conclusion of the procedure unless further storage is required for accounting purposes,

3. the user is protected against third parties obtaining knowledge of his use of teleservices,

4. personal data relating to the use of several teleservices by one user are processed separately; a combination of such data is not permitted unless it is necessary for accounting purposes.

(3) The user shall be notified of any reforwarding to another provider.

(4) User profiles are permissible under the condition that pseudonyms are used. Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym.

**§ 5: Contractual data**

(1) The provider may collect, process and use the personal data of a user to the extent necessary the data are required for concluding with him a contract on the use of teleservices and for determining or modifying the terms of such contract (contractual data).

(2) Processing and use of contractual data for the purpose of advising, advertising, market research or for the demand-oriented design of the teleservices is only permissible if the user has given his explicit consent.

**§ 6: Utilization and accounting data**

(1) The provider may collect, process and use personal data concerning the use of teleservices only to the extent necessary

1. to enable the user to utilize teleservices (utilization data) or

2. to charge the user for the use of teleservices (accounting data).

(2) The provider shall erase

1. utilization data as soon as possible, at the latest immediately after the end of each utilization, except those that are at the same time accounting data,

2. accounting data as soon as they are no longer required for accounting purposes; user-related accounting data stored by the provider for the establishment of detailed records concerning the use of particular services at the user's request in accordance with § 6 (4) below, shall be erased not later than 80 days from the date of dispatching the detailed records unless the request for payment is disputed within this period or the invoice has not been paid despite a demand for payment.

(3) Utilization or accounting data shall not be transmitted to other providers or third parties. This shall not affect the powers of criminal prosecution agencies. The provider offering access to the use of teleservices must not transmit to other providers whose teleservices have been used by the user any data other than

1. anonymised utilization data for the purposes of their market research,

2. accounting data to the extent necessary for collecting a claim.

(4) If the provider has concluded a contract with a third party concerning the provision of accounting services, he may transmit to the third party accounting data necessary for rendering such services. The third party shall be obligated to comply with telecommunications secrecy.

(5) The invoice concerning the use of teleservices must not reveal the provider, time, duration, type, content and frequency of use of any particular teleservices used unless the user requests such detailed records.

## § 7: User's right to information

The user shall be entitled at any time to inspect, free of charge, stored data concerning his person or his pseudonym at the provider’s. The information shall be given electronically if so requested by the user. If data are stored only for a short period in accordance with § 33 (2) Nr. 5 of the Federal Data Protection Act [*Bundesdatenschutzgesetz*], the user's right to information shall not be excluded by § 34 (4) of the Federal Data Protection Act.

## § 8: Control

(1) § 38 of the Federal Data Protection Act shall be applicable with the proviso that an examination may be carried out even if there are no grounds to suppose that data protection provisions have been violated.

(2) The Federal Commissioner for Data Protection shall observe the development of data protection as applied to the provision and utilization of teleservices and shall make relevant comments in the activity report he has to submit pursuant to § 26 (1) of the Federal Data Protection Act.

**Article 3**

**Digital Signature Act**[*)]

**(*Signaturgesetz - SigG*)**

**§ 1: Legislative Purpose and Scope**

(1) The purpose of this Act is to establish general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained.

(2) The application of other digital signature procedures is optional insofar as digital signatures according to this Act are not required by legal provisions.

**§ 2: Definitions**

(1) For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to §3 of this Act.

(2) For the purposes of this Act "certification authority" shall mean a natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a licence pursuant to § 4 of this Act.

(3) For the purposes of this Act "certificate" shall mean a digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate).

(4) For the purposes of this Act "time stamp" shall mean a digital declaration bearing a digital signature and issued by a certification authority confirming that specific digital data were presented to it at a particular point in time.

---

[*)] The notification requirements in Council Directive 83/189/EEC of 28 March 1983 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ No L 109, p 8), last amended by Directive 94/10/EC of the European Parliament and the Council of 23 March 1994 (OJ No L 100, p 30) have been duly observed.

### § 3: Competent Authority

The granting of licences, the issue of certificates used for the signing of certificates, and the monitoring of compliance with this Act and with the ordinance having the force of law pursuant to §16 are incumbent on the authority according to §66 of the Telecommunications Act.

### § 4: Licensing of Certification Authorities

(1) The operation of a certification authority shall require a licence from the competent authority. A licence shall be granted upon application.

(2) A licence shall be denied when facts warrant the assumption that the applicant does not possess the reliability necessary to operate a certification authority, when the applicant does not furnish proof of the specialised knowledge required to operate a certification authority or when there is reason to believe that, upon starting operation, the other requirements pertaining to the operation of the certification authority as set out in this Act and in the ordinance having the force of law pursuant to §16 will not be met.

(3) Whosoever as operator of a certification authority guarantees compliance with the legal provisions applicable to the operation of such an authority shall be deemed to possess the necessary reliability. The required specialised knowledge shall be deemed available when the persons engaged in the operation of the certification authority have the necessary knowledge, experience and skills. The other requirements pertaining to the operation of the certification authority shall be deemed met when the competent authority has been notified in a timely manner by means of a security concept of the measures ensuring compliance with the security requirements in this Act and the ordinance having the force of law pursuant to §16 and their implementation has been checked and confirmed by a body recognised by the competent authority.

(4) Collateral clauses may be attached to a licence where necessary to ensure compliance by the certification authority with the requirements in this Act and in the ordinance having the force of law pursuant to §16 upon starting operation and thereafter.

(5) The competent authority shall issue the certificates for the signature keys used for affixing signatures to certificates. The provisions applicable to the issue of certificates by certification authorities shall apply accordingly to the competent authority. The competent authority shall keep the certificates which it has issued available for verification and retrieval at all times and for everyone over publicly available telecommunication links. This shall also apply to information concerning addresses and call numbers of certification authorities, invalidation of certificates

issued by the competent authority, cessation and prohibition of the operation of a certification authority as well as withdrawal or revocation of licences.

(6) Any public services rendered in accordance with this Act and the ordinance having the force of law pursuant to §16 shall be subject to costs (fees and expenses).

## § 5: Issue of Certificates

(1) The certification authority shall reliably establish the identity of persons applying for a certificate. It shall confirm the assignment of a public signature key to an identified person by a signature key certificate which, together with any attribute certificates, shall be kept available for verification and, with the consent of the owner of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links.

(2) At an applicant's request the certification authority shall include in the signature key certificate or an attribute certificate information relating to his authority to represent a third party and to his professional admission to practice or other type of admission insofar as reliable proof is furnished of the consent by the third party to the inclusion of the authority of representation or of the admission.

(3) At an applicant's request the certification authority shall indicate a pseudonym instead of the applicant's name in the certificate.

(4) The certification authority shall take measures to prevent undetected forgery or manipulation of the data intended for certificates. It shall also take measures to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted.

(5) The certification authority shall engage reliable staff for the exercise of certification activities. For the provision of signature keys and the issue of certificates it shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above.

### § 6: Notification Requirement

The certification authority shall notify applicants according to § 5(1) of the measures necessary to support secure digital signatures and their reliable verification. It shall notify applicants of the technical components meeting the requirements of § 14(1) and (2) and of the assignment of digital signatures generated by a private signature key. It shall advise applicants that data bearing a digital signature may need to be signed again before the security of the existing signature decreases with time.

### § 7: Content of Certificates

(1) The signature key certificate shall contain the following information:

1. name of the owner of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the owner of the signature key, clearly marked as such,
2. public signature key assigned,
3. names of the algorithms with which the public key of the owner of the signature key and the public key of the certification authority can be used,
4. serial number of the certificate,
5. beginning and end of the validity period of the certificate,
6. name of the certification authority, and
7. an indication as to whether use of the signature key is restricted in type or scope to specific applications.

(2) Information relating to the authority to represent a third party and to the professional admission to practice or other type of admission may be included both in the signature key certificate and in an attribute certificate.

(3) Further information shall not be included in the signature key certificate unless the parties concerned give their consent.

### § 8: Invalidation of Certificates

(1) The certification authority shall invalidate a certificate when the owner of a signature key or his representative so requests, when the certificate was obtained through false statements in respect of §7, when the certification authority ceases operation and its activity is not continued by another certification authority or when invalidation is ordered by the competent authority pursuant to §13(5) sentence 2. The invalidation shall indicate the time at which it enters into effect. Retrospective invalidation shall not be permitted.

(2) Where a certificate contains third party information, this party may also request invalidation of the certificate.

(3) The competent authority shall invalidate certificates which it has issued according to §4(5) when a certification authority ceases operation or its licence is withdrawn or revoked.

### § 9: Time Stamp

Upon request the certification authority shall affix a time stamp to digital data. § 5 (5) sentences 1 and 2 shall apply mutatis mutandis.

### § 10: Documentation

The certification authority shall document the security measures for compliance with this Act and the ordinance having the force of law pursuant to §16 and the certificates issued in a manner such that the data and their integrity can be verified at all times.

### § 11: Cessation of Operation

(1) Upon cessation of operation the certification authority shall notify the competent authority accordingly at the earliest possible time and shall ensure that the certificates valid at the time of cessation of operation are taken over by another certification authority or invalidated.

(2) It shall forward the documentation according to §10 to the certification authority taking over the certificates or otherwise to the competent authority.

(3) It shall notify the competent authority without undue delay of a bankruptcy petition or petition for institution of composition proceedings.

## § 12: Data Protection

(1) The certification authority may only collect personal data directly from the party concerned and only insofar as they are required for the purposes of a certificate. Collection of data from third parties shall be permitted only with the consent of the party concerned. The data may only be used for purposes other than those given in sentence 1 if this is permitted within the framework of this Act or another legal provision or if the party concerned has given its consent.

(2) Where the owner of a signature key uses a pseudonym, the certification authority shall be obliged to communicate, upon request, to the competent bodies any data pertaining to his identity which is required for the prosecution of criminal or administrative offences, for averting danger to public safety or order or for the discharge of statutory duties by the Federal and State authorities for the protection of the Constitution, the Federal Intelligence Service [*Bundesnachrichtendienst*], the Military Counter-Intelligence Service [*Militärischer Abschirmdienst*] or the Customs Criminological Office [*Zollkriminalamt*]. Such disclosures shall be documented. The requesting authority shall inform the owner of the signature key about disclosure of the pseudonym as soon as this no longer interferes with the discharge of its statutory duties or if there is an overriding interest of the owner of the signature key in being given such information.

(3) § 38 of the Federal Data Protection Act shall apply subject to the proviso that verification may also be carried out when there is no indication of a violation of data protection provisions.

## § 13: Control and Enforcement of Obligations

(1) The competent authority may take measures vis-à-vis certification authorities to ensure compliance with this Act and the ordinance having the force of law. In particular, it may prohibit use of unsuitable technical components and may temporarily prohibit the operation of the certification authority wholly or in part. Parties who appear to have a licence according to §4 without this being the case may be prohibited from carrying out their certification activity.

(2) For purposes of monitoring according to (1) sentence 1 above certification authorities shall allow the competent authority to enter the production sites and business premises during normal business hours, shall upon request make available for inspection any relevant books, records, supporting documents, papers and any other documentation, shall disclose information and provide all necessary support. Whosoever is obliged to provide information may refuse to answer questions which would render himself or a person related by blood affinity as specified in §383

(1) Nr. 1 to 3 of the Code of Civil Procedure liable to prosecution or proceedings under the Administrative Offences Act. Any person obliged to answer inquiries shall be advised of this right.

(3) In the event of non-fulfillment of obligations arising under this Act or the ordinance having the force of law or in the event of a reason for denial of a licence the competent authority shall revoke the licence granted when measures according to § 13 (1) sentence 2 above are unlikely to be successful.

(4) In the event of withdrawal or revocation of a licence or cessation of operation of a certification authority the competent authority shall ensure transfer of the activity to another certification authority or winding up of the contracts with the owners of signature keys. This shall also apply when a bankruptcy petition or a petition for institution of composition proceedings is filed and the licensed activity is discontinued.

(5) The validity of the certificates issued by a certification authority shall remain unaffected by the withdrawal or revocation of a licence. The competent authority may order the invalidation of certificates when facts warrant the assumption that certificates have been forged or are not adequately protected against forgery or when technical components used for the signature keys reveal security flaws enabling digital signatures to be forged or signed data to be manipulated without detection.

**§ 14: Technical Components**

(1) Technical components with safeguards are required for the generation and storage of signature keys and for the generation and verification of digital signatures which reliably reveal forged digital signatures and manipulated signed data and provide protection against unauthorised use of private signature keys.

(2) Technical components with safeguards are required for the presentation of data to be signed which clearly indicate in advance the generation of a digital signature and enable identification of the data to which the digital signature applies. Technical components with safeguards are required for the verification of signed data which allow the integrity of the signed data, the data to which the digital signature applies and the owner of the signature key to whom the digital signature belongs to be established.

(3) Technical components enabling signature key certificates to be kept available for verification or retrieval in accordance with §5(1) sentence 2 require safeguards to protect the lists of certificates against unauthorised alteration and retrieval.

(4) Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority.

(5) Technical components lawfully manufactured or placed on the market in accordance with regulations or requirements in force in another Member State of the European Union or in another State party to the Agreement on the European Economic Area which ensure the same level of security shall be assumed to fulfil the technical security requirements according to § 14 (1) to (3) above. In a given justified instance and at the request of the competent authority proof shall be furnished of compliance with the requirements according to sentence 1 above. Insofar as presentation of a confirmation by a body recognised by the competent authority is required as evidence of compliance with the technical security requirements within the meaning of § 14 (1) to (3) above, confirmations by bodies licensed in other Member States of the European Union or other States parties to the Agreement on the European Economic Area shall also be accepted if the technical requirements, tests and test procedures on which the test reports of these bodies are based are deemed equivalent to those of the bodies recognised by the competent authority.

### § 15: Certificates Issued by Other Countries

(1) Digital signatures capable of being verified by a public signature key certified in another Member State of the European Union or in another State party to the Agreement on the European Economic Area shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security.

(2) Paragraph (1) above shall also apply to other states insofar as relevant supranational or intergovernmental agreements have been concluded.

### § 16: Ordinance Having the Force of Law

The Federal Government shall be empowered to issue, by ordinance having the force of law, the legal provisions required for implementation of §§ 3 to 15 with respect to

1. further details of the procedure pertaining to the granting, withdrawal and revocation of a licence and the procedure upon cessation of the operation of a certification authority,

2. chargeable services according to §4(6) and the level of the fee,

3. further details of the obligations of certification authorities,

4. validity periods of signature key certificates,

5. further details of the control over certification authorities,

6. detailed requirements applicable to technical components, their testing, and confirmation of compliance with the requirements,

7. the period after which a new digital signature should be affixed and the associated procedure.

**Article 4**

**Amendment of the Penal Code**
**(*Strafgesetzbuch*)**

The Penal Code as promulgated on 10 March 1987 (Federal Law Gazette *BGBl*. I, page 945, 1160) last amended by ...(*BGBl*.....) is amended as follows:

1. § 11 (3) of the Penal Code is amended to read as follows:

   "(3) Sound and visual recordings, data storage devices, illustrations and other representations shall be equivalent to writings in those provisions which refer to this subsection."

2. § 74 d is amended as follows:

   a) § 74 d (3) is amended by inserting the reference "(§ 11 subsec.3)“ following the word "writings".

   b) § 74 d (4) is amended by replacing the words "when at least part" by the words "when a writing (§ 11subsec. 3) or at least part of such writing".

3. § 86 (1) is amended by inserting the words "or provides public access to such material through data storage devices" following the word "exports".

4. § 184 is amended as follows:

   a) § 184 (4) is amended by inserting the words "or realistic" following the word "real".

   b) § 184 (5) sentence 1 is amended by inserting the words "or realistic" following the word "real".

**Article 5**

**Amendment of the Administrative Offences Act (*Ordnungswidrigkeitengesetz*)**

The Administrative Offences Act as promulgated on 19 February 1987 (Federal Law Gazette BGBl. I p. 602), last amended by .....(BGBl .....) is amended as follows:

1. § 116 (1); § 120 (1) Nr. 2 and § 123 (2) sentence 1 are amended by inserting in each case a comma and the words „data storage devices“ following the words „visual recordings“.

2. § 119 is amended as follows:

   a) § 119 (1) Nr.2 is amended by inserting the words „or by providing public access to data storage devices“ following the word „representations“.

   b) § 119 (3) is amended by inserting a comma and the words „data storage devices“ following the words „visual recordings“.

**Article 6**

**Amendment of the Law on the Dissemination of Publications Morally Harmful to Youth (*Gesetz über die Verbreitung jugendgefährdender Schriften*)**

The Law on the Dissemination of Publications Morally Harmful to Youth as promulgated on 12 July 1985 (Federal Law Gazette BGBl. I, page 1502) last amended by .....(BGBl.....) is amended as follows:

1. The title of the Law is amended to read as follows:

   "Law on the Dissemination of Publications and Other Media Morally Harmful to Youth"

2. § 1 (3) is amended to read as follows:

   "(3) Sound and visual recordings, data storage devices, illustrations and other representations shall be equivalent to writings. Writings as defined by this Act do not include radio programmes pursuant to § 2 of the Interstate Agreement on Broadcasting or content provided by distribution and on-demand services if the emphasis is on editorial arrangement to form public opinion pursuant to § 2 of the Interstate Agreement on Media Services signed between 20 January and 7 February 1997".

3. § 3 is amended to read as follows:

   a) At the end of § 3 (1) Nr. 3 the full stop is replaced by a comma, and the following number 4 is added:

      "4. are disseminated, made available or otherwise made accessible by means of electronic information and communication services."

   b) At the end of § 3 (2), the following sentence is added:

      "§ 3 (1) Nr. 4 shall not apply if technical measures have been taken to ensure that the offer or dissemination within Germany is restricted to users of legal age."

4. § 5 (3) is amended to read as follows:

   "(3) § 5 (2) shall not apply

1. if the act is performed in the course of commercial transactions with the relevant trade or

2. if dissemination to or exposure of children or minors is excluded by technical or other means."

5. After § 7, the following § 7a is added:

"§ 7a: Youth Protection Commissioners

Whoever makes available, on a commercial basis, electronic information and communication services which are based on transmission by means of telecommunication, shall appoint a commissioner responsible for the protection of minors, if such services are generally available and might include content morally harmful to youth. The commissioner shall be the contact for users and shall advise providers concerning questions relating to the protection of minors. The commissioner shall be consulted by providers in planning their services and in formulating their general terms and conditions of use. The commissioner may suggest to the provider that services offered be restricted. The provider may also meet his obligation under the first sentence by obligating a self-regulation organization to take over the duties under sentences 2 through 4 above."

6. The following number 3a is added following § 21 (1) Nr. 3 of § 21 (1):

1. "3a. disseminates, makes available or otherwise makes accessible such material in violation of § 3 (1) Nr. 4,"

7. § 18 is amended to read as follows:

"(1) A writing is subject to the restrictions contained in § 3 to § 5 even if it has not been included in the list and published provided that its content is wholly or significantly identical with that of a writing in the list. The same applies where there is a final judgment by a court that a writing is pornographic or that its content falls within § 130 (2) or § 131 of the Penal Code.

(2) In cases where there is doubt as to whether the preconditions of subsection (1) have been fulfilled, the president shall bring about a decision by the Federal Examining Board. No application (§ 11 (2) sent. 1) is necessary. § 12 applies mutatis mutandis.

(3) Where a writing is included in the list, § 19 applies mutatis mutandis."

8. § 18 is deleted.

9. § 2 is amended as follows:
   a) The former text shall be designated as subsection 1.
   b) A new subsection 2 is inserted:
   "(2) Where inclusion in the list is obviously out of the question, the president may discontinue proceedings".

10. § 21 a (1) is amended to read as follows:
"(1) An administrative offence shall be deemed to be committed by any person who

1. contrary to § 4 (2) sentence 2 fails to draw a user's attention to restrictions on distribution, or
2. contrary to § 7 a (1) sentence 1 fails to appoint a youth protection commissioner or fails to obligate a self-regulation organization to take over such duties."

**Article 7**

**Amendment of the Copyright Act**
***(Urheberrechtsgesetz)***

The Copyright Act dated 9 September 1965 (Federal Law Gazette [BGBl.] Part I, p. 1273), last amended by Art. 5 of the Act of 19 July 1996 (BGBl. Part I, p. 1014) shall be amended as follows:

1. § 4 shall be worded as follows:

"§ 4

Collections and Database Works

(1) Collections of works, data or other independent elements which, by reason of the selection or arrangement of the elements, constitute a personal intellectual creation (collections) shall enjoy protection as independent works without prejudice to a copyright or neighbouring right existing in the elements included in the collection.

(2) Within the meaning of this Act a database work is a collection arranged in a systematic or methodical way, the elements of which are individually accessible either by electronic or by other means. A computer program (§ 69 a) used to create the database work or to render its elements accessible does not constitute a component of the database work."

2. § 23 second sentence shall be amended as follows:

a) The word "or" appearing after the word "arts" shall be replaced by a comma.

b) The words "or of the adaption or other transformation of a database work" shall be inserted after the word "architecture".

3. § 53 shall be amended as follows:

a) The following subsection 5 shall be inserted after subsection 4:

"Subsection 1 as well as subsection 2 (2) to (4) shall not apply to database works the elements of which are individually accessible by electronic means. Subsection 2 (1) shall apply to such database works on condition that the scientific use does not serve commercial purposes."

b) The former subsections 5 and 6 shall become subsections 6 and 7.

4. The following § 55a shall be inserted after § 55:

"§ 55a

Use of a Database Work

Adaption or other transformation and the reproduction of a database work by the owner of a copy of the data base work, having been put into circulation with the consent of the creator by way of sale, by a person in other ways entitled to use the copy of the database work or by anyone to whom a database work has been made accessible on the basis of a contract with the creator or with a third party who has the former's consent, shall be permissible if and to the extent that the adaptation or other transformation or reproduction is necessary for access to the elements of the database work and for its usual use. If, on the basis of a contract described in sentence 1, only a part of the database work is made accessible, it shall only be permissible to adapt or otherwise transform and to reproduce this part. Any contractual provisions to the contrary shall be null and void."

5. § 63 subsection 1 (1) shall be amended as follows:

a) The following sentence 2 shall be inserted after sentence 1 in § 63 subsection 1:

"The same shall apply to the reproduction of a database work in the cases outlined in § 53 subsection 2 (1) and subsection 3 (1)."

b) The former sentences 2 and 3 shall become sentences 3 and 4.

6. The following chapter shall be inserted after § 87:

"Chapter Six

Protection of the Maker of a Database

§ 87a

Definitions

(1) A database within the meaning of this Act is a collection of works, data or other independent elements arranged in a systematic or methodical way the elements of which are individually accessible either by electronic or by other means, and the obtaining, verification or presentation of which requires a qualitatively or quantitatively substantial investment. A database the contents of which has been changed in a way that is

qualitatively or quantitatively substantial is deemed a new database provided that the change entails a qualitatively or quantitatively substantial investment.

(2) The maker of a database within the meaning of this Act is the one who has made the investment defined in subsection 1.

§ 87b

Rights of the Maker of the Database

(1) The maker of the database has the exclusive right to reproduce, to distribute and to communicate to the public the whole data base or a qualitatively or quantitatively substantial part thereof. The repeated or systematical reproduction, distribution or communication to the public of qualitatively and quantitatively insubstantial parts of the database shall be deemed as equivalent to the reproduction, distribution or communication of a qualitatively or quantitatively substantial part of the database provided that these acts conflict with a normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database.

(2) § 17 subsection 2 and § 27 subsections 2 and 3 shall apply mutatis mutandis.

§ 87c

Limitations on the Rights of the Maker of a Database

(1) The reproduction of a qualitatively or quantitatively substantial part of a database shall be permissible:

1. for private use; this shall not apply to a database the elements of which are individually accessible by electronic means;

2. for the purposes of personal scientific use, if and to the extent that the copying for this purpose is necessary and the scientific use does not serve commercial purposes;

3. for personal use in teaching, in non-commercial institutions of education and further education and in vocational training in a quantity required for one school class.

In the cases outlined in numbers 2 and 3, the source must be clearly acknowledged.

(2) The reproduction, distribution and communication to the public of a qualitatively or quantitatively substantial part of a database shall be permissible for use in proceedings

before a court, an arbitration tribunal or a public authority as well as for purposes of public security.

§ 87d

Term of Protection

The rights of the maker of a database shall expire fifteen years after the publication of the database, and fifteen years after the making of the database if it has not been published within that period of time. The period of time shall be calculated in accordance with § 69.

§ 87e

Contracts Dealing with the Use of a Database

A contractual agreement according to which the owner of a copy of the database, having been put into circulation with the consent of the maker of the database by way of sale, or the person in other ways entitled to use the copy of the database or anyone to whom a database has been made accessible on the basis of a contract with the maker of the database or with a third party who has the former's consent, obligates himself vis-à-vis the maker of the database to refrain from reproducing, distributing or communicating to the public qualitatively and quantitatively insubstantial parts of the database, shall be invalid to the extent that these acts do not conflict with the normal exploitation of the database nor unreasonably prejudice the legitimate interests of the maker of the database."

7. The following number shall be inserted after § 108 subsection 1 (7):

   "8. uses a database in breach of § 87b subsection 1."

8. In § 119 subsection 3 after the word "photographs", the word "and" shall be replaced by a comma and the words "and the databases protected according to § 87b subsection 1" shall be inserted after the word "phonogram".

9. The following § 127 a shall be inserted after § 127:

"§ 127a

Protection of the Maker of a Database

(1) The protection granted by § 87 b shall be available to German citizens and to legal entities with a registered office located in the territory in which this Act applies. § 120 subsection 2 shall apply.

(2) Legal entities without a registered office in the territory in which this Act applies but which have been established according to German law or according to the law of one of the states listed in § 120 subsection 2 (2) shall enjoy the protection granted by § 87b if:

1. their central administration or principal place of business is geographically located in one of the states listed in § 120 subsection 2 (2); or

2. their registered office, as defined by the articles of association, is located in one of these states and their activities have a de facto connection with the German economy or to the economy of one of these states.

(3) In the remaining cases, foreign citizens and legal entities shall enjoy the protection granted by the provisions of international agreements and the protection of agreements entered into between the European Community and third party states; these agreements are published by the Federal Ministry of Justice in the *Bundesgesetzblatt* [Federal Law Gazette]."

10. The following § 137g shall be inserted after § 137f:

"§ 137g

Transitional Regulation
in implementing Directive 96/9/EC

(1) § 23 second sentence, § 53 subsection 5, § 55a and § 63 subsection 1 second sentence shall also apply to database works created prior to 1 January 1998.

(2) The provisions contained in Chapter Six of Part II shall also apply to databases created between 1 January 1983 and 31 December 1997. The term of protection in such cases shall commence on 1 January 1998.

(3) § 55a and § 87e shall not apply to contracts concluded before 1 January 1998."

**Article 8**

**Amendment of the Price Indication Act**
**(*Preisangabengesetz*)**

The following sentence is added to § 1 of the Price Indication Act dated 3 December 1984 (Federal Law Gazette (BGBI.) Part I, p. 1429):

"In the case of services to be provided in the field of electronic information and communications services, also regulations regarding information on the price level of on-going services may be issued."

**Article 9**

**Amendment of the Price Indication Ordinance**
**(*Preisangabenverordnung*)**

The Price Indication Ordinance dated 14 March 1985 (Federal Law Gazette (BGBI.) Part I, p. 580), last amended by .... (BGBI.) ....) is amended as follows:

1. The following sentences are added to subsection 1 of § 3:

"The screen of a monitor shall also be deemed to be a place of the offer to provide a service. If a service is provided by display on a monitor and charged per unit, separate display of the price to be paid for the on-going use of such service shall be offered free of charge."

2. Number 2 of subsection 2 of § 8 is amended to read as follows:

"2. of the first, second or fourth sentence of subsection 1 of § 3, or subsection 2, in each case also in conjunction with subsection 5 of § 2 regarding the erection, affixing or provision of price lists or regarding the offer to display the price."

**Article 10**

**Return to Uniform Order of Ordinance**

**(*Rückkehr zum einheitlichen Verordnungsrang*)**

Those parts of the Price Indication Ordinance which are based on Article 8 of this Act can be amended through a legal ordinance on the basis of the empowerment contained in § 1 of the Price Indication Act.

**Article 11**

**Entry into Force**

This Act shall enter into force on 1 August 1997 with the exception of Article 7, which shall enter into force on 1 January 1998.