International Organisation of Penal Law

XIXth International Congress of Penal Law

"Information Society and Penal Law"

Rio de Janeiro, Brazil, 31st August to 6th September 2014

Preparatory Colloquium Section 2:

General Rapporteur: Emilio C. Viano

Natonal rapporteurs – Denmark: *

Jørn Vestergaard[1] & Maria Raabye Füchsel[2]

(A) Scope of questionnaire

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

a. The provisions related to cyber-offences are to be found in various separate codes. The primary provisions are found in the Penal Code [Da.: straffeloven][3] and supplementary provisions in the Act on Processing of Personal Data [Da.: persondataloven], the Act on Intellectual Property/Copyright [Da.: lov om ophavsret], and other regulations. The provisions related to police investigating powers are codified in the Administration of Justice Act [Da.: retsplejeloven][4].

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

a. Denmark belongs to a civil-law tradition. The role of the judiciary is to interpret the law and implement it in concrete cases submitted to the courts. The judiciary only has limited powers to apply a radically dynamic style of interpretation and thus independently develop new law. However, court decisions can sometimes trigger legislative initiatives and thereby trigger changes in existing law. In the area of cyber crime, most of the criminal law regulations are results of thorough preparation by expert committees and Government legal officers.[5]

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

a. Laws are usually updated by issuing amendment laws that add new or supplement or modify existing provisions. Subsequently, amendments are regularly incerted in a consolidated text issued by the particular Minister.

b. Ex.: Law no. 319 of 28/04/2009 implemented the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

[1] Jørn Vestergaard is Professor of Criminal Law, Faculty of Law, University of Copenhagen: jv@jur.ku.dk, http://jura.ku.dk/jv.

[2] Maria Raabye Raabye Füchsel is Research Assistant, Center for International Law and Justice (CILJ), Faculty of Law, University of Copenhagen.

[3] An English translation of the Penal Code has been published by Frese Jensen et al, see list of litterature below.

[4] Parts of the Administration of Justice Act are published in the above mentioned book by Frese Jensen et al.

[5] The basic provisions on cyber crime in the Penal Code are derived from an expert committee report: Betænkning 1477/ 2002 om IT-kriminalitet.

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

a. As a matter of principle, offences criminalized in the Penal Code must be be conducted with some form of intent (dolus, mens rea, Da.: *forsæt*) to imply criminal responsibility, whereas offences criminalized in other laws can be punishable if the perpetrator acted negligently (culpa). However, a particular statute can widen or limit the scope of the culpability requirement. Danish courts accept not only direct intent [Da.: *direkte forsæt*] but also probability intent (the perpetrator acknowledges that certain consequences are highly probable [Da.: *sandsynlighedsforsæt*]) and in rare cases also dolus eventualis.

b. Only a few of the cyber crime related offences criminalized by the Penal Code requires a specific intent in the sense of 'dolus specialis', e.g. PC § 169 a (false electronic money); PC § 171 (forgery); PC § 168 (tampering with data suited for legal use). See subsections below.

(2) Are there also negligent offenses in this field?

a. Some cyber crime offences might be covered by broad traditional provisions in the Penal Code or other legislation. Since the questionnaire applies a rather broad definition of cybercrime, it is possible for most traditional offences to be committed as a sort of computer-related crime, which makes it somewhat difficult to draft an exhaustive list. Some examples are provided in the following subsection.

(3) If yes, please, provide a list of those offenses.

a. Penal Code: The provision on serious and extensive attacks on information systems vital to common public infrastructures or installations (PC § 193) covers both intentional (subsection 1) and gross negligent acts (subsection 2).[6] Similar regulations are stipulated regarding serious vandalism,[7] see PC § 291 (2 and 3).[8]

b. The Act on Intellectual Property/Copyright [Da.: lov om ophavsret]:[9]

§ 75 b (trading in or with a commercial intention possessing means which sole purpose is to facilitate the removing or circumvention of technical arrangements applied for the protection of a computer program, e.g. means such as another computer program or an instruction in writing).[10]

§ 75 c (circumvention of technical arrangements other than those designed for the protection of computer programs; manufacturing, import, disseminating, trading, renting, advertising, etc. devices, products or components intended for circumvention of technical arrangements, etc.); the actual wording of the statute is somewhat extensive.[11]

§ 75 e (unauthorized deletion or altering of electronic information regarding the administration of intellectual property rights; dissemination of or import with the intention of disseminating, ect., protected creations where information regarding the administration of IP rights has been deleted or altered).[12]

---

[6] Cf. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems art. 10; Council of Europe Convention on Cybercrime 185, 2001 art. 12. PC § 193 was latest amended in 2004. Intentional perpetration of PC § 193 is punishable by fine or imprisonment up to 6 years. Gross negligent acts are punishable by fine or punishent up to 6 months.

[7] Cf. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems art. 3, 4 and 6; Council of Europe Convention on Cybercrime 185, 2001 art. 5 and 6.

[8] Intentional perpetration of PC § 291 (2) is punishable by fine or imprisonment up to 6 years. Gross negligent acts are punishable by fine or punishent up to 6 months. One of the first judgements regarding cyber crime in a broad sense dealt with an employee in a labor union who established a trojan horse in a workplace computer and programmed it to delete the union's registrer of members after he was fired, see UfR 1987.216 Ø. The High Court stated that data processing media concaining data could be understod in the same sense as "things" covered by PC § 291. Deletion was equivalent to "destruction" under said provision.

[9] See the annexed translation of the Act in English or: http://www.wipo.int/wipolex/en/text.jsp?file_id=191420.

[10] Intentional or gross negligent violations of § 75 b are penalized by fine, see § 78 of the Act. Cf. Council Directive 91/250/ECC on the legal protection of computer programes Art. 7(1)(c).

[11] The statute in § 75 c was inserted in the Act in 2002 to implement the Infosoc-Directive Art. 6 (1-3), see Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society. Intentional or gross negligent violations of § 75 c are penalized by fine, see § 78 of the Act.

[12] The statute in § 75 e was inserted in the Act in 2002 to implement the Infosoc-Directive Art. 7. Intentional violations of § 75 e are penalized by fine, see § 78 of the Act.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

a. Deleting or in other ways damaging computer data or systems is considered vandalism and criminalized by the PC § 291, see subsection above.

b. Attacks like DoS (Denial-of-Service) and DdoS (Distributed Denial-of-Service) that overload computers, wreck computer systems and block users' access to electronic ressources, e.g. email-systems, is criminalized under PC § 293 (2).[13]

c. Serious and extensive attacks on information systems vital to common public infrastructures or installations are criminalized by PC § 193, see subsection above.[14] The attack has to be damaging to the general public which requires some kind of magnitude.

b. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

a. In a situation where a perpetrator has conducted a hack without actually interfering with data, the unauthorized act is punishable as an invasion of privacy, see PC § 263 (2).[15]

b. No specific condition relating to defeat of security measures has been stipulated in the Act, but the general wording of PC § 263 and the relevant standard commentary indicates a need for the system to be non-public, closed, or technically secured. The provision is applicable if the hacker has had to use some form of software or tools.

2. Data and system interference

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related para.s/articles of your code.

a. The Act on Processing of Personal Data [Da.: Persondataloven] provides various definitions, including:[16]
   - 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject');
   - 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means;
   - '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;
   - '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;
   - 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

---

[13] Cf. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems art. 3, 4 and 6; Council of Europe Convention on Cybercrime 185, 2001 art. 5, 6 and 12. Intentional perpetration of PC § 293 (2) is punishable by imprisonment up to 1 year, under aggravating circumstances by imprisonment up to 2 years. PC § 293 was amended in 2004 to accommodate for the penalization of illegal use of someone elses computer tools, e.g. to perform a DoS attack. This is not explicitly stated in the statute but can be deduced from the travaux préparatoires. The same provision can be applicable with regard to other instances of intrusion into an information system, e.g. in order to disseminate spam messages; to copy information from the system; or to apply unauthorized programs to compute something on the perpetrator's own equipment.

[14] In an unreported municipal court judgement, perpetration of PC § 193 was stipulated with regard to an attack on a U.S. military inslallation servicing some 5000 users and containing sensitive personal data, as well as am attack on a U.S. weather service provider, see Bryde Andersen, p. 124.

[15] Cf. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems art. 2 and 7; Council of Europe Convention on Cybercrime 185, 2001 art. 2, 3 and 6. Intentional perpetration of PC § 263 (2) is punishable by fine or imprisonment up to 1 year, under aggravating circumstances by imprisonment up to 6 years. PC § 263 was amended in 1985 to accommodate for activities within the area of electronic information processing comparable to classic instances of intrusion and trespassing into physical environments. If security measures prevent the hacker from gaining access, the perpetrator can be convicted of criminal attempt, see UfR 2000.1450 Ø and UfR 2002.1064 V.

[16] See the annexed translation of the Act in English or: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data.

a. There is no explicit definitions stipulated in the Penal Code. The standard commentary on the Penal Code offers an account by reference to the generel law on information technology which defines data as "any form of representation of facts or ideas, which can be communicated or handled through some kind of process".[17]

b. The standard commentary on the Penal Code also state that information systems are to be understod as "a computer or another system for processing data".[18]

b. Act – destruction/alteration/rendering inaccessible?
i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

a. If someone unauthorized interferes with a system and its files, data, or information, the act can be punishable by § 291 as vandalism, se subsection above.

ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

a. Unauthorized interception in penalized by PC § 263 (2) as an invasion of privacy, see subsection above.

b. In principle, an employer is entitled to intercept an employee's email correspondance practiced on the workplace's equipment, at least if it is communicated to the employee in advance that such a practice will be followed. However, the employer is not entitled to read private mail and must cease if the private character of the correspondence becomes apparent, or else such an intrusion into privacy can be punishbale under PC § 263 (1).[19]

3. Data Forgery
a. Object – authenticity
Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related para.s/articles of your code and/or special statutes.

a. The Penal Code penalizes manufactoring, procurement and distribution of false electronic money with a specific intent that it is utilized as genuine, see PC § 169 a (1). The legal definition of false electronic money is "means which are not genuine electronic money but are suited to be utilized as such", see PC § 169 a (2).[20]

b. The Penal Code common provision on vandalism might in a specific instance cover unauthorizd input, alteration, deletion or suppression of electronic data, see PC § 291 as mentioned in a subsection above.

c. The Penal Code contains no common provision to protect the authenticity of electronic data.

b. Act – alteration/deletion?
Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable para.s/articles of your code.

a. Such acts are penalized under the common provision regarding forgery, see PC § 171.[21] This statute covers written as well as electronic documents from being forged with the intention of deceiving in legal matters. In this relation, the standard commentary on the Penal Code define data as a document in an electronic version which can be used as legal evidence, e.g. emails and text messages. Pictures or false signatures without an intentional declaration fall outside of the scope of the statute. As a decisive element, the document has to have a signing or some kind of identification of the issuer or writer. The unauthorized alteration, deletion or suppression has to be conducted with the intention that the document will be acted upon or considered for legal purposes.

---

[17] Kommenteret straffelov, Speciel Del, 2012, § 263 p. 442.

[18] Kommenteret straffelov, Speciel Del, 2012, § 193 p. 276.

[19] Intentional perpetration of PC § 263 (1) is punishable by fine or imprisonment up to 1 year and 6 months, under aggravating circumstances by imprisonment up to 6 years.

[20] Cf. EU Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment. Intentional perpetration of PC § 169 a is punishable by fine or imprisonment up to 1 year and 6 months, under aggravating circumstances by imprisonment up to 6 years.

[21] PC § 171 was amended in 2004, cf. Council of Europe Convention on Cybercrime 185, 2001. Intentional perpetration of PC § 171 is punishable by fine or imprisonment up to 2 years, under aggravating circumstances by imprisonment up to 6 years.

b. Tampering with data suited for legal usage, e.g. data records, is penalized under the provision in PC § 178.[22] The offence has to be conducted with the intent to separate someone from their rights.

c. Data forgery committed for the sake of enrichment is penalized under PC § 279 a.[23] This provision is designed to protect property and not to protect the authenticity of data as such.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

a. No such provisions exist in Danish law. However, the Danish provisions on aiding and abetting are assessed as in compliance with the obligations set out in the CoE Cybercrime Convention Article 6, which criminalizes the development, sales, use, and possession of IT programs and devices specially developed with the intent to use them for committing a cybercrime[24].

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under *a*?

a. See the subsection above.

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

a. These situations are covered by various traditional provisions. The Penal Code contains no specific provision which targets the distribution or transfer of hacked information.

b. Hacking is penalized as an invasion of privacy, see § 263 (2), se subsection above.

c. Varius form of illegal trading in, distribution of, or procurement of passwords or other means of access to a non-public information system is penalized by PC § 263 a.[25]

d. To acquire or communicate confidential codes or other means of access to commercial information systems intended for paying subscribers is penalized by PC § 301 a.[26]

e. Unauthorized disemmination of private or in other ways sensitive information or pictures is penalized by PC § 264 d.

c. Possession?

a. See the subsection above.

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

---

[22] Intentional perpetration of PC § 178 is punishable by fine or imprisonment up to 2 years.

[23] Cf. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems; Council of Europe Convention on Cybercrime 185, 2001 art. 12. Intentional perpetration of PC § 279 a is punishable by imprisonment up to 1 year and 6 months, see PC § 285, under mitigating circumstances by fine, see PC § 287. PC § 279 a was inserted in the Penal Code in 1985.

[24] See Executive Order, Betænkning 1417 2002 point 7.3 regarding the CoE Cybercrime Convention.

[25] This statute was inserted in the Penal Code in 2004. Intentional perpetration of PC § 263 a is punishable by fine or imprisonment up to 1 year, under aggravating circumstances by imprisonment up to 6 years. No recorded jurisprudence is available.

[26] This statute was inserted in the Penal Code in 2004 Intentional perpetration of PC § 301 a is punishable by fine or imprisonment up to 1 year and 6 months, under aggravating circumstances by imprisonment up to 6 years.

a. Danish law distinguishes between two types of data collectors. The first type of collector accesses information already stored in the subscriber's or user's terminal equipment. The use of cookies is regulated in the Act on Electronic Communication Nets and Services [Da.: lov om elektroniske kommunikationsnet og – tjenester] and supplementary administrative rules.[27] The second type of collector collects and process personal data which identify or makes it possible to identify a person. The latter type of collection is in compliance with the rules laid down in the Act on Processing of Personal Data [Da.: persondataloven].[28]

b. Cookies: A data collector is not allowed to store information or gaining access to information already stored in the a subscriber's or user's terminal equipment or to let a third party store information or get access to information stored in a users terminal equipment unless the subscriber or user concerned has given an informed consent with regard to the purpose of the storing of or access to the information. Violation of this regulation is punishable by fine.[29] The Act on Electronic Communication Nets and Services require any data collector whether being an individual or a legal person to state the purpose of the storing of or access to data, to identify himself or itself, and to provide readily accessible option for declining or withdrawing consent at any time and clear information on how to enter such steps.[30]

c. If a person can be identified by an identification number, code, picture or anything else the situation will fall within the scope of the Act on Processing of Personal Data § 3 (1). When collecting private information the data collector or his representative has to give following information to the data subject: the identity of the collector, the purpose of the data processing, categories of recipients, whether the disclosure of information by the data subject is mandatory or voluntary, the consequences of non-disclosure, the regulations regarding access to and rectification of collected data. On information to be given to the data subject, see Act on Processing of Personal Data § 28.

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

a. Regarding stored information on terminal equipment, see the above mentioned.

b. The above mentioned rules in the Act on Processing of Personal Data regarding the duty of disclosure are applicable to private and public collectors both online and offline, see the Act on Processing of Personal Data § 1 and § 28. The Act does not require the collector to inform about the confidentiality, integrity, or the quality of data but the collector must inform about the right to access information and rectification. The collector is bound by a general safety obligation with regard to the data, see § 41 (3).

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?

a. No. The area concerning privacy policy is self-regulated with a possibility to join known certification agreements like a Danish version of Trust.e.[31]

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

a. Yes. Concerning the regulations derived from the Act on Electronic Communication Nets and Services, see answers above.

b. Violation of the Act on Processing of Personal Data § 28 conducted in line with data processing for a private individual or legal entity is penalized by fine or imprisonment up to 4 months, see § 70 (1).

---

[27] See Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment [Da.: bekendtgørelse 1148, 2011] § 5, cf. § 3 (1), as authorized by the Act on Electronic Communication Nets and Services [Da.: lov 169, 2011 om elektroniske kommunikationsnet og – services.] § 9 and § 81 (2). Extensive guidelines have been issued [Da.: vejledning 9018, 2011 om nye regler om lagring af cookies og lignende teknologier]. The regulations have been issued in order to implement Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Art. 5 (3). The Executive Order is annexed and can also be found here: http://www.erhvervsstyrelsen.dk/file/253401/cookie-exec-order-english-version.pdf. The Guidelines od the Executive Order are annexed, too, and can also be found here: http://www.erhvervsstyrelsen.dk/file/253400/cookie-exec-order-guidelines-english-version.pdf.

[28] See the annexed translation of the Act in English or: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data.

[29] See the above mentioned Executive Order, bekendtgørelse 1148, 2011 § 5, cf. § 5, as authorized by the Act on Electronic Communication Nets and Services § 9 and § 81 (2).

[30] See Executive Order, bekendtgørelse 1148, 2011 § 5, cf. § 3 (2), as authorized by the Act on Electronic Communication Nets and Services [Da.: lov 169, 2011 om elektroniske kommunikationsnet og – services.] § 9 and § 81 (2).

[31] Blume, Databeskyttelsesret p. 362.

b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data?

a. The Penal Code defines illegal transfer and distribution by the legal standard "unauthorized" [Da.: "uberettiget"] transfer and distribution, see for example PC § 263 a and PC § 264 d.

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

a. The Penal Code penalizes the more severe cases where someone violates the secrecy of correspondence, unauthorized monitors the internet (PC § 263 (1)(1 and 3); unauthorized and for commercial purposes sells codes and passwords to non-public information systems (PC § 263 a); disseminates private information (e.g. concerning sexual relations, suicide, income and tax matters) or personally sensitive pictures (PC § 264 d); acquires or communicates confidential codes or other means of access to information systems intended for paying subscribers (PC § 301 a)[32].

b. Violation of certain provisions under the Act on Processing of Personal Data is penalized by fine or imprisonment up to 4 months, see § 70.[33]

c. On violation of professional service confidentiality by an owner or provider of a teleservice or an employee or former employe, see subsection below.

c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

a. Under the conditions laid down in the Act on Electronic Communication Nets and Services, especially the provisions laid down in Government Order regarding access and conditions (§§ 1-6)[34], and the conditions laid down in the Act on Processing of Personal Data – especially Chapter 4 (§§ 5-14).[35]

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

a. The access and storage has to be legitimate, see the Government Order 1148 § 1 as authorized by the Act on Electronic Communication Nets and Services.

b. Data must be collected for specified, explicit and legitimate purposes, see the Act on Processing of Personal Data § 5.

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;

- Their disclosure practices;

a. The Act requires all data collectors to respect the duty of disclosure unless the data subject already is acquainted with the information cf. the Act on Processing of Personal Data § 28 (1)-2.

b. Violation of professional service confidentiality by an owner or provider of a teleservice or an employee or former employe is penalized under the Act on Telecommunication Nets and Services.[36]

- Their professional ethical obligations;

---

[32] Intentional perpetration of PC § 301 a is punishable by fine or imprisonment up to 1 year and 6 months, under aggravating circumstances by imprisonment up to 6 years.

[33] See answer under subsection 3.c.i above.

[34] See Executive Order, bekendtgørelse 1148, 2011, as authorized by the Act on Electronic Communication Nets and Services [Da.: lov 169, 2011 om elektroniske kommunikationsnet og – services.] § 9 and § 81 (2).

[35] See the annexed translation of the Act in English or: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data .

[36] See the Act on Telecommunicationnets and -services [Da.: lov 169, 2011 om elektroniske kommunikationsnet- og tjenester] § 81, cf § 7 (1). Grave violations of professional secrecy can be punished under privisions in the Penal Code (PC §§ 152 ff.), see the Act on Telecommunicationnets and -services [Da.: lov 169, 2011 om elektroniske kommunikationsnet- og tjenester] § 81, see § 7 (2).

a. Reference is made to the relevant trade practices. Lawyers have to disclose their ethical obligations, see the Administration of Justice Act [Da.: retsplejeloven] § 126. The medical profession has a set of ethical guidelines.[37]

- And whether patients or clients have any control over the disclosure of their personal data?

a. The data subject has a general right to the access of information and rectification. These rights are a part of the duty of disclosure, see the Act on Processing of Personal Data § 28.

ii. Which data are specifically protected, if any?

a. Personal health declarations, see the Health Act [Da.: sundhedsloven].

b. Sensitive private information, see the Act on Processing of Personal Data § 7 (1) and § 8 (1). Sensitive private information is information about ethnicity, religion, political opinion, sexuality etc.

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

a. The Penal Code includes a general obligation for anybody to inform public authorities if there is a risk of a serious crime being committed, alternately to prevent the crime. See PC § 141. The crime must be one endangering the life or welfare of someone or substancial societal values. Said provision is almost never applied by the prosecution service.

b. The Penal Code also includes a general obligation for anybody to inform public authorities if there is a risk that an innocent person is being charged or convicted of a crime. See PC § 164 a.

c. Anyone who learns about children at risk of being abused is obliged to inform the social welfare service, see the Act on Social Welfare §§ 152-155.

d. In principle, public servants and others acting under public authorisation are excepted from testifying in court regarding professional matters covered by confidentiality. However, the court can overrule this privelege if the relevant interests are found to overweigh the interest in secrecy, see further the Procedural Act § 169.

e. The court can oblige physicians, legal mediators and lawyers, except defence attorneys, to give witness testemony when this is regarded as of decisive importance for the outcome of the case, and the character of the case and its importance for an involved party or for society jusfifies that testemony is required, see further the Procedural Act § 170 (2)-4. Priests can not be required to breach confidentiality, see § 169 (1). An attorney-client privilege cannot be overruled, see § 170 (1) and 2.

b. *Subject – Type of perpetrators?*
Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

a. See answers under subsection above.

c. *Act – illegal use and transfer/distribution?*
Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

a. The Penal Code penalizes disclosure and utilization of confidential information by public servants or others acting under a public authorisation, see PC § 152.[38] Said provision also emcompasses somebody who is or has been working with asignments under a conteact with public authorities, or who is or has been operating in relation to publicly authorized telephone facilities, see PC § 152 a. It also encompasses anybody working on the bases of a public authorization, see PC § 152 b. Further, it encompasses assistants for anybody covered by PC §§ 152-152 b, see PC § 152 c. In addition, the previously mentioned provisions encompas extranei who subsequently procures og utilizes information obtained by violation of professional confidentiality, see PC § 152 d (1). Likewise, disclosure of sensitive private information obtained by violation of professional confidentiality by an extraneus is penalized, see PC § 152 d (3). The same applies with regard to information which is secret for the sake of national security of defence, see PC § 152 d (3). Justifications with regard to the entioned activities are provided if the person has acted in legitimate safeguarding of manifest public interest or of own or others

---

[37] Cf. the ethical rules of the Danish Medical Association [Da.: Lægeforeningens etiske regler]: http://www.laeger.dk/portal/page/portal/LAEGERDK/Laegerdk/R%C3%A5dgivning%20og%20regler/ETIK/LAEGEFORENINGENS_ETISKE_REGLER .

[38] Intentional perpetration of PC § 152 or one of the following provisions is punishable by fine or imprisonment up to 6 months, under aggravating circumstances by imprisonment up to 2 years.

needs, see further PC § 152 e.

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

a. Analysis and processing of information (cookies) accessed and stored in terminal equipment are in compliance with the provisions in the Act on Processing of Personal Data.

b. Violation of the Act on Processing of Personal Data § 28 conducted in line with data processing for a private individual or legal entity is penalized by fine or imprisonment up to 4 months, see § 70 (1).

c. The Penal Code penalizes the more severe cases where someone violates the secrecy of correspondence, illegally monitors the internet (PC § 263 (1 and 3), illegally and for commercial purposes sells codes and passwords to non-public information systems (PC § 263 a), the distribution of data which are seen as confidential (like e.g. race, ethnicity, political background and sexuality) (PC § 264 d), or vandalism (PC § 291).

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

a. The Penal Code: Anybody.

b. The Act on Processing of Personal Data § 70 (1): Providers proessing data for private users, including individuals as well as legal entities.

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply *for each category listed below* citing the relevant law and its provisions, if available:

1. Illegal collection

a. The Act of Processing Data stipulates the correct way to collect data. If a data is collected in a incorrect way it can be penalized, see § 70 (1).

2. Illegal use

a. When collecting data the collector has to inform the data subject about the specified, explicit and legitimate purposes of the collection, see § 5 (2). If the collector uses the data for another purpose which is incompatible with the alleged such activity is penalized as illegal use, see § 70.

3. Illegal retention

a. Retained data is subject to the same safety provisions as collected data cf. § 41 (3). "The data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed" cf. § 5 (5). Any illegal retention can be penalized under the Act § 70

4. Illegal transfer

a. Transfer of data has to be conducted within the guidelines laid down in the Act on Processing of Personal Data, otherwise it can be penalized, see § 70.

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

a. There is no duty of disclosure if the if the data subject's interest in obtaining this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject himself cf. § 30 (1).

b. Other exceptions from the duty for disclosure is e.g. public interests, criminal proceedings, prevention of criminal acts, criminal investigating, or public safety are found in § 30 (2)

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of

personal and private data?

a. Under the conditions laid down in the Act on Processing of Personal Data – especially chapter 4. (§§ 5-14)[39].

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

a. Data must be collected for specified, explicit and legitimate purposes (§ 5).

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

a. The Penal Code has no specific provision which penalizes identity theft. In 2011, some politicians discussed the possibility of inserting a new provision on identity theft. This was turned down by the Government who assessed the traditional provisions as sufficient.

b. Forgery is penalized under PC § 171.

c. Intrusion of privacy, e.g. hacking personal mail accounts, is penalized under PC § 263. Identity theft on a social media can be viewed as an invasion of privacy or defamation and would in those cases be penalized under § 267 (with private cause of action).

d. Ordinary theft is penalized under the traditional statute in PC § 276.

e. Fraud is penalized under traditional statute in PC § 279. The articles also covers situations like phishing where a perpetrator takes advantage of a delusion and deceives someone to either do something or refrain from doing something, which will result in economic loss.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

a. See the above mentioned.

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

a. No.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

a. The Penal Code criminalizes the production (§230), dissemination (§ 235), and possession (§ 235 (2)) of online and offline child pornography.

ii. In particular, does your criminal law:

- Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:

---

[39] For an English translation of the Act on Processing og Personal Data, see http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/

1. to transmit,
2. make available,
3. export
4. and intentionally access child pornography on the Internet;

a. With respect to child pornography, there has not been inserted any new specific provisions in the Penal Code since 2000, but existing provisions have been amended on several occasions to cover new types of criminal conduct and to comply with EU and COE obligations.[40]

- Allow judges to order the deletion of child pornography posted on computer systems in your country;

a. The Administration of Justice Act authorizes seizure and the PC § 75 allows for confiscation of a domain if it contains illegal materials.

- Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;

a. The PC § 75 (2) no. 1 authorizes the forfeiture/confiscation of materials and equipment used to commit a criminal offense.

b. The PC § 77 a authorized the forfeiture/confiscation of materials and equipment if there is a risk of use to commit a criminal offense.

- Criminalize:

1. Knowingly accessing child pornography on the internet

a. Accessing child pornography though the internet is penalized by the PC § 235 (2).

2. Transmitting child pornography on the internet

a. The owner of a webpage can be liable as an accomplice or assessory to violation of PC § 235 if he becomes aware of illegal content and does not remove it.[41] A web provider is not presumed to be under an obligation to scan the facilitated web pages for illegal content.

3. Exporting child pornography on the internet

a. Dissemination of child pornography is penalized under PC § 235 (1).

4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it…?

b. Possession of child pornography is penalized under PC § 235 (2) (1). There is no requirement of dolus specialis to transmit, export, or otherwise disseminate the materials. Said provision penalizes accession to child pornography through the internet.

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

a. Yes, but such activities are not specifically penalized under a particular statute. They would be punishable under various provisions in force, e.g. as instigation of rape (PC § 216), child sexual abuse (PC § 222), child molesting (PC §§ 244-246), ect.

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

a. Yes.[42]

---

[40] Cf. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 201, 2007; Council of Europe Convention on Cybercrime 185, 2001; EU-FD L 13/44, 2004; EU-Dir L 335/1, 2011.

[41] Cf. Kommenteret straffelov, Speciel del, 2012, p. 356.

[42] The Penal Code provisions regarding child pornography is inspired by several international instruments: Second Optional Protocol to UN Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography; EU-Council framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography; EU-Directive 2004/68/JHA on combating the sexual abuse and sexual exploitation of children and child pornography; Council of Europe Convention on Cybercrime 185, 2001; Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 201, 2007.

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

a. Not relevant. Neither adult pornography nor prostitution is illegal under Danish law. Buying sexual services from a child or an adolescent under the age of 18 years is a criminal offence, see PC § 223 a.

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

a. Yes. Due to a 2004 amendment, the dissemination and possession of fictitious child pornography images is covered by the above mentioned provision PC § 235. The article targets situations where an image is portrayed in a way that makes it look like a real photography.

vii. *Mens rea*: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

a. Yes. A 2009 amendment of PC § 239 (2) made it possible to penalize a person who accesses child pornography through the internet. The amendment was critizised by some who held that such legislation could create uncertainties regarding the intent by which such websites were accessed. A perpetrator might claim he had entered a site containing child pornography by accident. Danish National Police Constable stated that it is difficult to enter a side containing child pornography unintentionally. Typically, the user need to have exact information about the particular web address. If a person inadvertently accesses a site containing child pornography and immediately leaves the site, such activity should not be judged as a criminal offence.

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)
Does your criminal law penalize the following conducts? Please cite the relevant law.
1. creation and use of true anonymity sending and/or receiving material on the ICT?

No.

2. cyber-bullying?

No. There are no specific provisions under Danish law regarding digital harassment. Such acts can be punishable under various broader provisions, such as those penalizing libel and slander (PC § 267)[43]; illegal dissemination of private information or personally sensitive pictures (PC § 264 d); grave threats (PC § 266); grave intimidation of public servants (PC § 119)[44]; stalking[45].

3. cyber-stalking?

No. See answer above.

4. cyber-grooming?

No. Such activities can be punishhable as attempted violation of broader provisions, e.g. as child sexual abuse (PC § 222). Danish law on criminal attemp is very wide reaching. In a recent municipal court judgement, a middle-aged man was convicted for agreeing to meet a minor and to having arrived at the meeting site intending to have sex with her; the initiative was actually on the part of another man who pretended to be a young girl, and the 'girl' was a fictitious character. The judgement is in line with previous jurisprudence.

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)
Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

---

[43] On jurisprudence regarding derogatory accusations on the internet, see e.g. UfR 2002.2767 Ø and U 2006.2803 Ø.

[44] A death threat against the Prime Minister by email has been punished under PC § 119, see UfR 2008.99 Ø.

[45] See law no. 112, 2012 on protective orders, admittance resusal and expulsion; Da.: lov om tilhold, opholdsforbud og bortvisning.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud

a. Data fraud is penalized by PC § 279 a, se subsection above.

2. Infringement of Intellectual Property IP rights

a. IP rights are basically protected by the Act on Intellectual Property/Copyright [Da.: lov om ophavsret].[46] Gross violations can be punishable under PC § 299 b.[47]

b. On manufacture, import, distribution, sale, rental, or possession or alteration of decoders or other decoding equipment for commercial purposes with the aim of providing unauthorised access to the content of a coded radio- or tv broadcast, see Act on radio and television operations § 91.[48] Gross violations can be punishable under PC § 299 b.[49]

c. On manufacture, import, distribution, sale, or possession or alteration of decoders or other decoding equipment for commercial purposes with the aim of providing unauthorised access to informations- and contentservices, see the Act on Telecommunication Nets and Services [Da.: lov 169, 2011 om elektroniske kommunikationsnet- og tjenester] § 81 (1) (3), see § 65.[50]

3. Industrial espionage

a. Industrial espionage is penalized by PC § 263 (3), see subsection above.

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

a. On virtual child pornography, see § 235 as mentioned above.

b. There is no specific provision particularly penalizing virtual violence.

c. There is no specific provision particularly penalizing virtual graffiti.

d. On cyber-defamation, see § 267, as mentioned above.

e. On sexual harasment, see § 264 d, as mentioned above.

f. There is no specific provision particularly penalizing harassment at work committed in the virtual world.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

a. The hindering of the work of the law enforcement agencies is penalized under a common provision that might also cover activities in the field of cyber crime, see PC §119 (3).

b. Mailing companies and the suppliers of telecommunication nets services are obliged to cooperate with the police for investigation and prosecution purposes, see the Administration of Justice Act § 786. A violation of this obligation is penalized by fine under § 786 (6 and 7). Providers of telecommunications nets and services are obliged to registrer and store teletraffic

---

[46] See the annexed translation of the Act in English or: http://www.wipo.int/wipolex/en/text.jsp?file_id=191420.

[47] The statute in PC § 299 b was inserted in the Penal Code in 2004 and amended in 2008. It carries a penalty of imprisonment up to 6 years.

[48] This Act was introduced in 1997. Regarding reported jurisprudence, see UfR 2000.714 Ø and UfR 2000.2307 V.

[49] See previous footnote on PC § 299 b.

[50] These provisions was introduced in 2000. It implements Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access.

information for one year.[51]

c. The Administration of Justice Act § 804 authorizes a production order [Da.: edition]. Violation to comply with such an obligation is sanctioned by fine, continuous fine [Da.: tvangsbøder], or custody, see § 807 (2), with a reference to § 178.

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

a. Most cybercrimes are covered by common provisions which make it difficult to provide adequate statistics.

b. Unauthorized accession of netbank accounts are reportet by the Danish Council of Finance [Da.: Finansrådet].[52] The prevalence of reported incidents peaked in 2008 (251 cases, including 132 involving loss for a total of approx. 6.5 mio. DKK). The lovest number of incidents so far occurred in 2011 (10 cases, including 4 involving loss for a total of 159.668 DKK). In 2012, there has been an increase in the number of cases (199 cases, including 56 involving loss for a total of approx. 6.2 mio. DKK).

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.

a. No.

(3) Do victimization surveys in your country include questions on cyber-crimes?

a. No.

(4) What types of computer crime / computer fraud are most often reported in your country?

a. Probably identity theft and bank account password fraud.

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

a. Yes. NITEC [Da.: Nationalt IT efterforskningscenter] is a unit under the National Police Constable, employing approx. 100 it-investigators.[53]

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

a. No, not specifically.

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)	X		
Hacking (illegal intrusion into computer systems; theft of information from computer systems)	X		
Malicious code (worms, viruses, malware and spyware)	X		
Illegal interception of computer data	X		
Online commission of intellectual property crimes	X		
Online trafficking in child pornography	X		
Intentional damage to computer systems or data	X		
Others			

(9) In addition, to the above, if there are there any other forms and means of cyber-crime that have occurred (either frequently or

[51] Cf. Executive Order 988, 2006 [Da.: bkg. 988, 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af opbevaring af teletrafik (logningsbekendtgørelsen)].

[52] See http://www.finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx.

[53] http://www.politiguiden.dk/content/29-it-efterforsker .

infrequently) in your country, please identify them as well as the frequency with which they occur in the following table:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently

Literature

Bagger Tranberg, Charlotte: ”Behandling af personoplysninger”, i Jan Trzaskowski (red.): *Internetretten*, Ex Tuto, 2012, 489-576.

Betænkning 1417/2002 om IT-kriminalitet.

Blume, Peter & Janne Rothmar Herrmann: *Ret, privatliv og teknologi*, 3. udgave, Jurist- og Økonomforbundets Forlag, 2013.

Blume, Peter: *Databeskyttelsesret*, 4. udgave, Jurist- og Økonomforbundets Forlag, 2013.

Blume, Peter: ”Persondataretten i skyen”, *Juristen*, 2011, 67-72.

Bryde Andersen, Mads: *IT-retten*, 2. udgave, 2005.

Frese Jensen, Malene et al: *The Principal Danish Criminal Acts*, 3rd Edition, DJØF Publishing, Copenhagen 2006.

Greve, Vagn et al.: *Kommenteret straffelov. Speciel del.* 10. udgave, Jurist - og Økonomforbundets Forlag, 2012.

Karnovs lovsamling.

Kommenteret straffelov, Speciel del, 10. udgave, Jurist- og Øoknomforbundets Forlag Forlag, 2012.

Langsted, Lars Bo & Charlotte Bagger Tranberg: ”Internet-kriminalitet”, i Jan Trzaskowski (red.): *Internetretten*, Ex Tuto, 2012, 675-722.

Langsted, Lars Bo, Peter Garde & Vagn Greve: *Criminal Law in Denmark*, Third Revised Edition, DJØF-Publishing & Wolters Kluver, 2011.

Trzaskowski, Jan: ”Unmodet kommunikation i sociale medier”, *Ugeskrift for Retsvæsen* 2012 B. 310-318.

UfR: *Ugeskrift for Retsvæsen*.

Vestergaard, Jørn: *Dansk straffemyndighed,* Det Juridiske Fakultet, Københavns Universitet 2009.

Vestergaard, Jørn (red.): *Forbrydelser og andre strafbare forhold*, Gjellerup, 2009.

Vestergaard, Jørn: *Straffeloven & straffuldbyrdelsesloven – med henvisninger og sagregister*, 17. udgave, 2012.

Waaben, Knud: *Strafferettens specielle del*, 5. udgave 1999.

Please notice that the English version of the Executive Order is translated for the Danish Telecommunication Authority (now the Danish Business Authority). The official version is published in "Lovtidende" (Official Journal) on 9 December 2011. Only the Danish version of the text has legal validity.

Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment [(1)]

Executive Order No. 1148 of 9 December 2011

Pursuant to section 9 and section 81(2) of the Act on Electronic Communications Networks and Services, cf. Act No. 169 of 3 March 2011, the following provisions shall apply:

Scope and application

1. The purpose of this Executive Order is to protect end-users against unauthorised storing of information, or gaining of access to information already stored, in the end-user's terminal equipment.

Definitions

2.-(1) In this Executive Order, the following definitions shall apply:

1) *Terminal equipment:*
   A device or a relevant component within a device enabling communication which is intended to be connected directly or indirectly to network termination points in public electronic communications networks.
2) *End-user:*
   User of electronic communications networks or services who does not make such electronic communications networks or services available to other parties on a commercial basis. This includes a recipient of the service.
3) *Information and content service:*
   Any form of electronic provision of information or content to which other end-users get access via electronic communications networks or services on the basis of an individual request.
4) *Services in the information society (information society services):*
   Any service that has a commercial purpose and that is delivered online (electronically over a certain distance) at the individual request of a recipient of the service.
5) *Service provider:*
   Any natural or legal person providing an information society service.
6) *Legal person:*
   Public limited companies, private limited companies, cooperative societies, partnerships, associations, foundations, local authorities, regional authorities and government authorities etc.
7) *Third party:*
   A natural or legal person arranging for storing of information, or gaining of access to

information already stored, in an end-user's terminal equipment via an information and content service not provided by the natural or legal person in question.

8) *Consent:*
Any freely given, specific and informed indication of the end-user's wishes by which the end-user signifies its agreement to information being stored, or access to stored information being gained, in the end-user's terminal equipment.

(2) The definitions in subsection (1), nos. 2 and 3, shall be interpreted in accordance with the applicable definitions of the Act on Electronic Communications Networks and Services, and rules laid down in pursuance thereof.

Storing or accessing information in terminal equipment

3.-(1) Natural or legal persons may not store information, or gain access to information already stored, in an end-user's terminal equipment, or let a third party store information or gain access to information, if the end-user has not consented thereto having been provided with comprehensive information about the storing of, or access to, the information.

(2) Information, cf. subsection (1), shall be comprehensive if it meets the following minimum requirements:

1) it appears in a clear, precise and easily understood language or similar picture writing,
2) it contains details of the purpose of the storing of, or access to information, in the end-user's terminal equipment,
3) it contains details that identify any natural or legal person arranging the storing of, or access to, the information,
4) it contains a readily accessible means by which the end-user to refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end-user should make use thereof, and
5) it is immediately available to the end-user by being communicated fully and clearly to the end-user. In addition, when storing of information or access to information takes place through an information and content service, information to end-users must be directly and clearly marked and accessible at all times for the end-user on the information and content service in question.

4.-(1) Notwithstanding section 3, natural or legal persons may store information, or gain access to information already stored, in an end-user's terminal equipment if:

1) storing of or access to information is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
2) storing of or access to information is necessary in order for the service provider of an information society service explicitly requested by the end-user to provide this service.

(2) Storing of or access to information in an end-user's terminal equipment is necessary, cf. subsection (1), no. 2, if such storing of or access to information is a technical precondition for being able to provide a service operating in accordance with the purpose of the service.

Penalty provisions

5.-(1) Any person who violates section 3 shall be liable to a fine.

(2) Criminal liability may be imposed on companies etc. (legal persons) under the rules of Part 5 of the Penal Code.

Coming into force

6. This Executive Order shall come into force on 14 December 2011.

Ministry of Business and Growth, 9 December 2011

Ole Sohn

/ Kresten Bay

---

[1] This Executive Order implements parts of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal 2002, no. L108, p.51, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directiv2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal 2009, no. L337, p.11.

New rules on storing of cookies and similar technologies

- Guidelines on Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment

Version of 8 December 2011

The Danish Telecommunication Authority
(now the Danish Business Authority)

Preface

In connection with the revision of the European telecommunications directives in 2008/2009, the European Parliament adopted an amendment to Article 5(3) of the ePrivacy Directive on the storing of or access to information in users' terminal equipment, e.g. computers, smartphones or tablets. The amendment included new requirements for obtaining consent from the users in connection with the storing of or access to information in their terminal equipment.

The amendment to the Article was caused by a wish from the European Parliament to increase protection of the users' private sphere when they navigate in a digital world, and concern that the former wording of the Article did not meet this purpose to a sufficient extent - especially in connection with the use of cookies and similar technologies.

It is therefore the significance of the rules to the use of cookies that has attracted particular attention. Cookies are often compared to programs or software such as virus, spyware or malware which is capable of interacting with and manipulating the users' terminal equipment and the information stored in the equipment. However, cookies are usually passive files that can be stored or accessed in the users' terminal equipment, but cannot interact with or manipulate equipment or information.

Cookies however enable service providers or other parties that store or access cookies to identify the users across individual visits to a given service. This means that service providers will be able to obtain detailed knowledge of the users' behaviour and preferences such as this is expressed on the service. In some cases the users can also be identified across visits to different services, e.g. by using third-party cookies.

This knowledge can be used for a wide variety of purposes, e.g. personalisation and development of more user-friendly services, generating analyses about the use of a website or targeting behaviour-based marketing at the users. Depending

on the individual user's personal attitudes, these purposes may either be desirable or non-desirable to the user. The ability of users to make their own decisions as to whether they want to be identified by cookies and similar technologies in their terminal equipment is therefore an important element in protecting the private sphere of citizens in an increasingly digital world.

The present Guidelines are primarily intended for providers of services that use cookies and similar technologies. As a result, services and service providers are concepts often used in the Guidelines, but the rules apply to all parties that store or gain access to information in users' terminal equipment. Similarly, the examples in the Guidelines focus on the use of cookies, but, as mentioned before, the rules are not limited hereto.

The purpose of the Guidelines is to support service providers etc. in their practical implementation of and compliance with the rules of the Executive Order. Users of services can also benefit from reading the Guidelines, thus gaining a better knowledge of their rights.

The Guidelines are not intended as a definitive description of how we will be handling the rules in a given case. This must depend on the specific circumstances of the case at hand. The Guidelines are rather intended as an indication of the basic conditions underlying the administration of the Executive Order, and might therefore be of assistance in observing the rules.

The complexity and diversity of digital services today imply that it is not possible to describe in detail how the rules are to be complied with, but together with these Guidelines the Executive Order defines a framework or range of options within which service providers may find solutions that match their specific context. New innovative and user-friendly solutions that increase transparency and user control can best be created by the service providers themselves, and the rules provide scope for that.

Development of solutions within the framework of the rules is proceeding rapidly, and the Guidelines are therefore expected to be updated regularly as new knowledge that may serve as inspiration for others becomes available.

The Danish Telecommunication Authority
December 2011

Please notice that the English version of the Guidelines is translated for the Danish Telecommunication Authority (now the Danish Business Authority).

The Guidelines itself is not legally binding.

1. Introduction

The Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment has been issued pursuant to section 9 and section 81(2) of Act No. 169 of 3 March 2011 on Electronic Communications Networks and Services. The Executive Order implements Article 5(3) of the ePrivacy Directive, Directive 2002/58/EC, as amended by Directive 2009/136/EC.

Links to the legislation and directives referred to above can be found at the end of the Guidelines.

In these Guidelines, the Danish Telecommunication Authority (now the Danish Business Authority) explains the rules of the Executive Order in the following areas:

- Purpose and scope
- Requirements for information and consent
- Exemptions
- Self-regulation
- Inspiration for process steps
- Supervision of rules
- Links to legislation and directives

2. Purpose and scope

What do the rules protect?
The purpose of the rules is to protect the private sphere of the users. The rules are based on the view that the users' terminal equipment is part of their private sphere, and that this should be protected against unwarranted intrusion. Terminal equipment means computers, smartphones, tablets etc., in which information can be stored or already stored information be accessed, cf. section 2(1), no. 1, of the Executive Order.

What actions are covered?
The Executive Order is only concerned with the actions consisting in storing of or access to already stored information in a user's terminal equipment.

Actions taking place before or after storing of or access to information in a user's terminal equipment do not fall within the rules of the Executive Order.

What information is covered?
The Executive Order applies to any type of information stored or accessed in a user's terminal equipment.

Thus no distinction is made between information and personal information. Nor is it significant whether the information is semantically meaningful, unintelligible text strings, code or whether the information is encrypted.

Depending on the specific case and the processing of information otherwise taking place, especially the type of information being processed, the rules of the Act on Processing of Personal Data may be applicable.

Example 1: Storing or accessing cookies for the use of web statistics
A provider of a website wants to conduct an analysis of how website visitors use the site with a view to improving user experience. For this purpose the provider of the website wants to place cookies in the users' terminal equipment.

The service provider is governed by the requirements of the Executive Order for information and consent as regards the storing of cookies and any later access to these cookies in the users' terminal equipment.

If the service provider subsequently wants to analyse the information collected by means of the cookies, such processing falls outside the scope of the Executive Order. This applies for instance to further processing of the information by the service provider for the purpose of preparing statistics.

What technologies are covered?
The Executive Order is technology-neutral. Thus the Executive Order extends beyond storing of or access to information in the users' terminal equipment in connection with internet access; it also includes storing of or access to information from external media such as USB keys, CDs, CD-ROMs, external hard disks etc.

As for the form, type or standard used for storing the information, the Executive Order covers not only "classic" http cookies, but similar technologies of any type, including Flash cookies (Local Shared Objects), Web Storage (HTML5) or cookies set when using Microsoft Silverlight.

The Executive Order also covers any form of virus, spyware and malware as well as web bugs, beacons or other hidden identification mechanisms stored or accessed in users' terminal equipment.

Who are governed by the rules?
All parties that store or gain access to information in users' terminal equipment is governed by the rules (see also the section below on where specific rules are applicable).

The provider of a service is also obliged under the rules in connection with storing of or access to information in users' terminal equipment by third-parties if this is done via the provider's service, for instance by means of embedded code or similar techniques.

The service provider need not itself be in charge of practical and technical observance of the rules (information and obtaining the consent of a user), but may agree that a third-party should handle this on behalf of the service provider.

However, the responsibility for compliance with the rules will always lie with the provider of a service (first party) no matter what that party might have agreed with a third-party.

Example 2: Embedding a comment module on a website
A major news medium wants to embed a module that enables users of its website to comment on the content of the site. For this purpose, the news medium contacts the provider of a comment module that can be imbedded on websites. The news medium and the provider agree that the module should be embedded on all the news medium's webpages.

The provider of the comment module wants to set cookies in the users' terminal equipment when the users access a website in order to see how much the module is being used. The news medium therefore agrees with the provider of the comment module that the provider should ensure that the rules on storing of or access to information in users' terminal equipment are observed by informing the users and obtaining their consent.

However, the news medium is responsible for the rules being observed and hence for ensuring that no unwarranted storing is made in the users' terminal equipment when these access the website of the news medium, irrespective of what the news medium might have agreed with the provider of the comment module.

Where are specific rules applicable?
The European Commission has indicated that *within the EU* the legislation of the country in which the provider of a service is established will be applicable.

If the provider of a service established in Denmark stores or gains access to information in a user's terminal equipment, the service provider is liable under Danish rules. The Danish rules will also be applicable if the provider of a service established in Denmark lets a third-party established in another country store or gain access to information in a user's terminal equipment via the provider's service.

If, however, the provider of a service is established *outside the EU*, legislation in the country where storing of or access to information in a user's terminal equipment takes place will be applicable.

Example 3: Use of "plug-in" provided by a social medium located in another country
The provider of a webshop established in Denmark wants to imbed a plug-in provided by a social medium established in another country. The desired plug-in enables the user to indicate its opinion about the webshop in question.

When the user goes to a page in the webshop where the plug-in is embedded, the plug-in will also store cookies in the user's terminal equipment.

Even if the social medium is established in another country, storing of or access to cookies in users' terminal equipment must comply with the Danish rules since the use of cookies takes place through the webshop service established in Denmark.

3. Requirements for information and consent

In section 3 of the Executive Order, requirements are made for information and consent in case of storing of or access to information in users' terminal equipment:

3.-(1) Natural or legal persons may not store information, or gain access to information already stored, in an end-user's terminal equipment, or let a third party store information or gain access to information, if the end-user has not consented thereto having been provided with comprehensive information about the storing of, or access to, the information.

(2) Information, cf. subsection (1), shall be comprehensive if it meets the following minimum requirements:

1) it appears in a clear, precise and easily understood language or similar picture writing,
2) it contains details of the purpose of the storing of, or access to information, in the end-user's terminal equipment,
3) it contains details that identify any natural or legal person arranging the storing of, or access to, the information,
4) it contains a readily accessible means by which the end-user to refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end-user should make use thereof, and
5) it is immediately available to the end-user by being communicated fully and clearly to the end-user. In addition, when storing of information or access to information takes place through an information and content service, information to end-users must be directly and clearly marked and accessible at all times for the end-user on the information and content service in question.

The requirements for comprehensive information and consent respectively should be seen as two complementary elements supporting one another in a combined protection of the users' terminal equipment, to be understood as part of their private sphere.

The rules do not prohibit storing of or access to information in users' terminal equipment, but the rules set requirements for this. If the requirements are met, it is permitted to store or gain access to information in the user's terminal equipment.

In the following, the individual requirements are elaborated, but it will still be for the individual service provider to assess how the requirements can best be observed for precisely their services.

What requirements are made for comprehensive information?
Section 3(2) of the Executive Order lists the requirements that must be met as a *minimum* before the information can be described as comprehensive. Requirements are made for the character, content and availability of the information.

The information must constitute a knowledge basis that enables the users to make actual informed choices. In some cases it should therefore be considered to include information in addition to what is required under the Executive Order if this is necessary to enable the users to understand the consequences of their choice.

Section 3(2), no. 1, requires the information to appear *in a clear, precise and easily understood language or similar picture writing.*

This implies that the information should not be given in unnecessary technical or legal terms, and that the user can easily assess the information.

The use of tables or pictorial language, e.g. pictograms, can supplement or replace more traditional text and make the information easier to understand.

It is not specified in what language the information should be given. But the language should be chosen with due regard for the users addressed by a service, including in particular the geographic location of these users.

Section 3(2), no. 2, requires the information to contain *details of the purpose of the storing of, or access to information, in the end-user's terminal equipment*.

Users are entitled to be informed why information is stored or being accessed, and it is not sufficient merely to advise that this is done.

Information about the purpose of storing or accessing information is essential and should serve to ensure that users are aware of the consequences of their choice. As a result, the purpose should always be described in precise and adequate terms.

If the storing of or access to information has more than one purpose, all purposes should be explained. If several pieces of information are stored or accessed for the same purpose or on several occasions, it will usually be sufficient to describe the purpose once and not for each piece of information stored or accessed.

Example 4: Information about the purpose of using cookies

The use of cookies is very widespread and may have a variety of purposes, e.g.

- optimising the user experience or design of a service,
- generating web statistics,
- targeting marketing activities at the users.

The information given should describe the purpose of using cookies on the service and not the specific cookies as such.

If for instance a service is using four cookies for optimising the design of the service [1], while another two cookies are used for handling advertisements [2] and a seventh cookie is used for generating web statistics [3], it will normally be sufficient to give information about the three different purposes of using cookies and not necessarily about all of the seven cookies employed by the site.

Section 3(2), no. 3, requires the information to contain *details that identify any natural or legal person arranging the storing of, or access to, the information.*

Users must be able to identify the party arranging the storing. In many cases this will be the provider of the service, but where the provider of a service lets a third party store or gain access to information in a user's terminal equipment via the provider's service, it must also be possible to identify that third party.

As for information stored or being accessed in users' terminal equipment by an organisation, e.g. a company or another legal person, the information to be indicated must identify the organisation and not its employees.

What specific information must be available for users to identify the person(s) undertaking the storing will vary from service to service and depend on the parties involved.

Section 3(2), no. 4, requires the information to contain *a readily accessible means by which the end-user to refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end-user should make use thereof.*

Users must be able to refuse consent or withdraw a consent already given. This is intended to support real user control and the voluntary basis of the user's consent. For this purpose there must be a readily accessible means by which the user to refuse consent or withdraw consent and clear, precise and easily understood guidance on how the user should make use thereof.

In some cases it may be relevant to refer to guidance and tools prepared by others. It is not required in the Executive Order that guidance or tools for giving, refusing or withdrawing consent should be available on the service that stores or

gains access to information. What the service has to make readily accessible to the user is the access to guidance and tools.

Section 3(2), no. 5, requires the information to be *immediately available to the end-user by being communicated fully and clearly to the end-user. In addition, when storing of information or access to information takes place through an information and content service, information to end-users must be directly and clearly marked and accessible at all times for the end-user on the information and content service in question.*

To ensure real user control, it is necessary for the information to be immediately available to the users and easy to access. It is also a condition that users can withdraw a consent already given. How the information is best made available will depend on factors such as the design and structure of the service, for which reason it will vary from service to service.

It may be expedient to make use of layered or step-by-step information so that the users get brief and precise information on essentials such as the purpose of the storing, at the same time being offered the option of getting more detailed information. The use of pictograms or other clearly marked entries to the information may support this.

In addition, a service may distinguish between how the information is presented to the users *before* the users give or refuse consent, and how the information is presented *after* the users have given or refused consent.

On information and content services, including websites and other online services that store or access information in a user's terminal equipment the information must remain available to users via direct and clearly marked access on the information and content service in question.

This implies that users employing such services must have access at any time to the information, and that such access should be easy to find and use. It may be considered to meet the requirement by placing such access within the context of other permanent elements on a service. The use of pictograms or similar features may also be considered in this context.

Obtaining consent
Under the Executive Order, it is required that the user should consent to information being stored or accessed in the user's terminal equipment. Consent is defined in section 2(1), no. 8, of the Executive Order as:

> Any freely given, specific and informed indication of the end-user's wishes by which the end-user signifies its agreement to information being stored, or access to stored information being gained, in the end-user's terminal equipment.

As services and their users differ widely, the ways in which such consent is best obtained will also be widely different.

The requirement for consent is intended to support that users get real control of whether information is stored or accessed in their terminal equipment. When consent is to be obtained, it is therefore essential to be mindful of the users' control options.

The rules give services a wide range of options for choosing how consent can best be obtained in a way that works well within their specific context.

That the consent must be **freely given** implies that users must have a real choice. Such voluntariness also implies that users should have the opportunity to withdraw a consent already given, see also section 3(2), no. 4, of the Executive Order on the requirement for information.

That the consent must be **specific** implies that the consent must be precise and well-defined. However, the consent need not be related to each individual storing of or access to information in the users' terminal equipment. Instead the consent should be linked with the purpose underlying the storing of or access to information, see also section 3(2), no. 2, of the Executive Order on the requirement for information.

If storing of or access to information is used at a later date for purposes extending beyond what has been the subject of an earlier consent, a new consent covering the new purpose must be obtained.

That the consent must be **informed** is supported by the requirements for information in section 3(2) of the Executive Order, where, not least, the purpose of the storing is essential. As part of an informed consent, the users should also be informed of the consequences of their choice or refusal. Such consequences might be for instance that users cannot get access to the service or certain parts of it if refusing consent, or that the consent will result in third parties being allowed to store or access already stored information in users' terminal equipment.

The **indication of the user's wishes** is a key element in obtaining the consent. A service provider must identify an action on the part of its users that can reasonably be interpreted as an indication of their wishes on an informed basis. However, it should be emphasised that a wish can be indicated in a variety of ways, and that the rules of the Executive Order do not take a position on how it should be expressed.

An indication of the user's wishes can be many things, *for example*:

- ticking a box, clicking on a button or filling in a form in connection with relevant information on a service,
- active use of a service where it must be expected that the user is informed that there will be stored or accessed information (in case this has not been refused).

The ways in which consent can best be obtained will differ widely. The individual service itself is best suited for choosing a solution that meets the requirement

for consent and offers the users of the service a real ability to express their wishes on an informed basis.

The complexity and diversity of digital services do not make it possible to define more precisely how users should express their wishes in specific cases. The requirement for consent as stated in the Executive Order therefore allows services a wide range of options for developing new and innovative solutions that increase user control and transparency. Such solutions can improve the user's experience of a service and need not interrupt the flow characterising the interaction between a digital service and its users.

If users choose not to give their consent to information being stored or choose to withdraw consent, there is no requirement in the Executive Order that users should still be allowed access to content on a service.

Example 5: Obtaining consent to use cookies for targeted advertisements

A service on the internet offering a number of tools to its users intends to make use of cookies for registering which advertisements are clicked on by the users, so as to make its advertising more targeted.

The service must give users comprehensive information about the use of cookies and obtain their consent.

The service chooses that users of the service can best express their wishes by responding to a small box inserted in connection with the advertisements on the service. It appears from the box that users, by accepting cookies, will be able to get more targeted advertisements. In addition, the box contains separate access to getting more detailed information about the use of cookies.

If users choose to accept cookies for instance by clicking "Yes please" in the box, the box will change to merely containing the access to getting detailed information about the use of cookies, cf.3(2) of the Executive Order.

4. Exemptions

Section 4 of the Executive Order contains two exemptions from the requirements in section 3 for information and consent:

> 4.-(1) Notwithstanding section 3, natural or legal persons may store information, or gain access to information already stored, in an end-user's terminal equipment if:
>
> 1) storing of or access to information is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
> 2) storing of or access to information is necessary in order for the service provider of an information society service explicitly requested by the end-user to provide this service.
>
> (2) Storing of or access to information in an end-user's terminal equipment is necessary, cf. subsection (1), no. 2, if such storing of or access to information is a technical precondition for being able to provide a service operating in accordance with the purpose of the service.

Section 4(1), no. 1, is solely addressing Internet Service Providers and the storing of or access to information in users' terminal equipment that might be undertaken as part of connecting to the internet and maintaining the connection.

Section 4(1), no. 2, has a wider scope and is concerned with the situations in which *storing of or access to information is necessary in order for the service provider of an information society service explicitly requested by the end-user to provide this service*.

Who is exempted under section 4(1), no. 2, of the Executive Order?
To fall within the exemption rule in section 4(1), no. 2, two requirements must be fulfilled. In the first place, users must have *explicitly* requested the service. Secondly, the storing of or access to information in the user's terminal equipment must be *necessary*.

Section 4(2), clarifies when storing of or access to information in users' terminal equipment is *necessary*. In case storing of or access to information is not a technical precondition for being able to provide a service (or parts thereof) operating in accordance with the purpose of the service, the exemption cannot be applied.

As for the purpose of the service, emphasis should be on the purpose for which *users* access the service.

The exemption provision in section 4(1), no. 2, may be applied for instance in connection with the use of electronic shopping baskets in webshops where it is necessary to be able to recognise the user across page breaks (reloading of the webshop) as the basket would otherwise be empty when a new page is shown. Storing of a cookie or a similar technology is thus a technical precondition for being able to provide the service (e-business) that the user has explicitly re-

quested (accessing the webshop and placing goods in its shopping basket). The shopping basket also works in accordance with the purpose (to buy goods) for which the user accesses the webshop.

Similar services (or parts thereof), e.g. payment gateways, booking systems or web forms, may also fall within the exemption provision.

An example of where the exemption *does not* apply is the use of cookies or similar technologies for web statistics or other analysis of user behaviour on a service (or parts thereof). Web statistics will rarely be a technical precondition for delivering a service and rarely be the purpose for which users access a service.

5. Self-regulation

The complexity and diversity of digital services do not make it possible or efficient to define more precisely how the rules should be observed. Together with the present Guidelines, the Danish rules provide a framework or range of options within which service providers can work to find solutions that match their specific context.

New innovative and user-friendly solutions that increase transparency and user control can best be created by the service providers themselves. In the light of this, the European Commission has indicated that it would like to see development of self-regulation as an element in observing the rules.

Self-regulation initiated by industry associations or other stakeholders, if established in a sensible way, has a number of advantages, e.g.

- greater flexibility and adaptability in relation to development and adjustment of solutions,
- greater practical and technical insight in the field regulated by the rules,
- broader protection of service users in relation to the minimum statutory regulations,
- increased transparency, recognisability and consistency for users of the services provided, and
- increased confidence in the services provided.

What elements should be included in self-regulation?
The European Commission has indicated that the following minimum elements should preferably be included in self-regulation of the area:

- Information and effective transparency about what happens in the users' terminal equipment.
- Obtaining consent in an appropriate form of affirmation.
- User-friendly solutions.
- Effective enforcement, including
  - easily understandable and simple complaint procedure for the users,
  - convincing supervision of third parties, and
  - effective sanctions.

The Executive Order takes account of and provides scope for the European Commission's wish to develop self-regulation as an element in observing the rules.

6. Inspiration for process steps

Many services will have to be adjusted to a greater or lesser extent in order to conform to the rules. This section outlines some general process steps that may be used as a basis for the individual provider.

For those services that need to be adjusted, there may be special organisational, business-related or technical factors of significance in the process to be performed. It is therefore important to organise a process that will also take account of these aspects.

1. *Examine if your service is storing or accessing information, e.g. cookies, in users' terminal equipment.*
   Not all services are storing or accessing information in users' terminal equipment. If your service does not store or access information, the rules and subsequent process steps are not relevant for you. So examine as a first step if your service is storing or accessing information in users' terminal equipment. The party hosting your website or the provider of the CMS system you use might be able to help you. Otherwise there are several services on the internet that screen for cookies, and it is also possible to install plug-ins in certain browsers that may show what cookies are being set.

2. *Examine if the information possibly being stored or accessed in users' terminal equipment is necessary at all.*
   Many websites set cookies that have no direct significance for whether the site or parts of it are working. You may try to block all cookies in a browser and look if your website is still working. If it still works, you may consider removing the cookies that are not necessary.

3. *Examine if your service's storing of or access to information in users' terminal equipment is exempted from the requirements for information and consent.*
   Not all storing of or access to information in users' terminal equipment falls within the requirements for information and consent. See in particular section 4 of the Guidelines on exemptions from the requirements for information and consent.

4. *Decide how you will give users comprehensive information and obtain consent.*
   If your service is subject to the requirements for information and consent, you need to decide how you intend to observe these requirements on your service.

   The rules allow you to choose solutions for conforming to the require-

ments that will suit precisely your service. You may also consider to examine if there are existing solutions aimed at observing the requirements which you may possibly make use of on your service.

You are under an obligation to give users of your service comprehensive information and obtain consent from the users of your service if you wish to continue storing or accessing information in users' terminal equipment.

The requirements for information and consent should be seen as two complimentary elements supporting one another, and a general advice world be to put yourself in the users' place when solutions are to be developed and implemented.

7. Supervision of rules

The Danish Telecommunication Authority (now the Danish Business Authority) will supervise compliance with the rules of the Executive Order, cf. section 20 of Act no. 169 of 3 March 2011 on Electronic Communications Networks and Services. The Danish Telecommunication Authority (now the Danish Business Authority) is not subject to instructions from the Minister for Business and Growth in handling the supervisory activities of the Authority.

Failure to observe the rules of the Executive Order may be punishable by a fine, cf. section 5 of the Executive Order.

8. Links to legislation and directives

Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment:
https://www.retsinformation.dk/Forms/R0710.aspx?id=139279 (in Danish)

Directive on privacy and electronic communications (ePrivacy Directive, 2002/58/EC):
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DA:NOT (in Danish)

Directive 2009/136/EC, amending the ePrivacy Directive:
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:DA:NOT (in Danish)

Act No. 169 of 3 March 2011 on Electronic Communications Networks and Services:
https://www.retsinformation.dk/forms/r0710.aspx?id=136073 (in Danish)

Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, directive 1995/46/EC:
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=31995L0046 (in English)

Act on Processing of Personal Data:
https://www.retsinformation.dk/Forms/R0710.aspx?id=828 (in Danish)

Consolidated Act on Copyright 2010 [1]

(Consolidated Act No. 202 of February 27th, 2010)

The Act on Copyright is hereby promulgated.

Chapter 1

Subject Matter and Scope of Copyright

Protected Works

1.–(1) The person creating a literary or artistic work shall have copyright therein, be it expressed in writing or in speech as a fictional or a descriptive representation, or whether it be a musical or dramatic work, cinematographic or photographic work, or a work of fine art, architecture, applied art, or expressed in some other manner.

(2) Maps and drawings and other works of a descriptive nature executed in graphic or plastic form shall be considered as literary works.

(3) Works in the form of computer programs shall be considered as literary works.

Scope of Protection

2.–(1) Within the limitations specified in this Act copyright implies the exclusive right to control the work by reproducing it and by making it available to the public, whether in the original or in an amended form, in translation, adaptation into another literary or artistic form or into another technique.

(2) Any direct or indirect, temporary or permanent reproduction, in whole or in part, by any means and in any form, shall be considered as reproduction. The

[1] Act No. 395 of June 14, 1995 contains provisions implementing Council Directive 92/100/EEC, OJ 1992 L 346/61, Directive 93/83/EEC, OJ 1993 L 248/15, and Directive 93/98/EEC, OJ 1993 L 290/9. This Act re-enacts provisions from Act No. 1010 of December 19, 1992 whereby Council Directive 91/250/EEC, OJ 1991 L 122/42, was implemented. Act No. 1207 of December 27, 1996 contains provisions which in addition implement Council Directive 92/100/EEC, OJ 1992 L 346/61, and 93/83/EEC, OJ 1993 L 248/15. Act No. 407 of June 26, 1998 contains provisions implementing Directive 96/9/EEC of the European Parliament and of the Council, OJ 1996 L 77/20. Act No. 1051 of December 17, 2002 contains provisions implementing Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 2001 L 167/10. Act No. 997 of December 9, 2003 contains a provision that additionally implements Council Directive 93/83/EEC of September 27, 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ 1993 L 248, p. 15. Act. No. 1402 of December 21, 2005 contains provisions that implement the European Parliament's and the Council's Directive 2001/84/EC of September 27, 2001 on the resale right for the benefit of the author of an original work of art, OH 2001 no. L 272. p. 32. Act. No. 1430 of December 21, 2005 implements the European Parliament's and the Council's Directive 2004/48/EC on enforcement of intellectual property rights, OJ 2004, L 195, p. 15. Act. No. 510 of June 12, 2009 implements part of the Parliament and Council Directive 2006/123/EC on services in the internal market OJ 2006 nr. L 376, p. 39. Act. No. 1269 of December 16, 2009 contains provisions, that implement parts of the Parliament and Council Directive 2007/65/EC of December 11, 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities OJ 2007 L 332, p. 27.

recording of the work on devices which can reproduce it, shall also be considered as a reproduction.

(3) The work is made available to the public if

(i) copies of the work are offered for sale, rental or lending or distribution to the public in some other manner;

(ii) copies are exhibited in public; or

(iii) the work is performed in public.

(4) Public performance within the meaning of subsection (3)(iii) shall include

i) communication to the public of works, by wire or wireless means, including broadcasting by radio or television and the making available to the public of works in such a way that members of the public may access them from a place and at a time individually chosen by them; and

ii) performance at a place of business before a large group, which would otherwise have been considered not public.

3.–(1) The author of a work shall have the right to be identified by name as the author in accordance with the requirements of proper usage, on copies of the work as well as if the work is made available to the public.

(2) The work must not be altered nor made available to the public in a manner or in a context which is prejudicial to the author's literary or artistic reputation or individuality.

(3) The right of the author under this section cannot be waived except in respect of a use of the work which is limited in nature and extent.

Adaptations

4.–(1) The person translating, revising or otherwise adapting a work, including converting it into some other literary or artistic form, shall have copyright in the work in the new form, but his right to control it shall be subject to the copyright in the original work.

(2) Copyright in a new and independent work created through the free use of another work, shall not be subject to the copyright in the original work.

Composite Works

5. A person who, by combining works or parts of works, creates a composite literary or artistic work, shall have copyright therein, but the right shall be without prejudice to the rights in the individual works.

Joint Authorship

6. If a work has two or more authors, without the individual contributions being separable as independent works, the copyright in the work shall be held jointly. Each of the authors, however, may bring an action for infringement.

Copyright Holder Presumption, etc.

7.–(1) If not otherwise stated the person whose name or generally known pseudonym or signature is indicated in the usual manner on copies of the work, or where the work is made available to the public, shall be deemed to be the author.

(2) If a work is published without the author being indicated in accordance with subsection (1), the editor, if named, and otherwise the publisher, shall act on behalf of the author until the latter is named in a new edition of the work.

Publication and Publishing

8.–(1) A work shall be considered to have been made public if it has lawfully been made available to the public.

(2) A work shall be considered published if, with the consent of the author, copies of the work have been put on the market or otherwise distributed to the public.

Public Documents

9.–(1) Acts, administrative orders, legal decisions and similar official documents are not subject to copyright.

(2) The provision of subsection (1) shall not apply to works appearing as independent contributions in the documents mentioned in subsection (1). Such works may, however, be reproduced in connection with the document. The right to further use shall be subject to the provisions otherwise in force.

Relation to Protection under other Legislation

10.–(1) Protection under the Act on Designs does not preclude copyright.

(2) Layout designs (topography) of semiconductor products are not protected under this Act, but are protected under the provisions in the Act on Protection of the Design (Topography) of Semiconductor Products.

Chapter 2

Limitations on Copyright and Management of Rights in the event of Extended Collective License

General Provisions

11.–(1) The provisions of this chapter do not limit the author's rights under section 3, except as provided in section 29.

(2) Where a work is used in accordance with the provisions of this chapter, the work may not be altered more extensively than is required for the permitted use. If

the work is used publicly, the source shall be indicated in accordance with the requirements of proper usage.

(3) Where a work is used in accordance with the provisions of this chapter, copies may not be made on the basis of a reproduction of the work which is contrary to section 2 or on the basis of circumvention of a technical device which is contrary to section 75 c(1). The provision in the first sentence does not apply to the production of copies pursuant to section 16 (5).

Temporary reproduction

11 a.–(1) It is permitted to make temporary copies

i) which are transient or incidental;
ii) which are an integral and essential part of a technical process;
iii) the sole purpose of which is to enable a transmission of a work in a network between third parties by an intermediary, or a lawful use of a work; and
iv) which have no independent economic significance.

(2) The provision of subsection (1) shall not apply to computer programs and databases.

Reproduction for Private Use

12.–(1) Anyone is entitled to make or have made, for private purposes, single copies of works which have been made public if this is not done for commercial purposes. Such copies must not be used for any other purpose.

(2) The provision of subsection (1) does not provide the right to

(i) construct a work of architecture;
(ii) make a copy of a work of art by casting, by printing from an original negative or base, or in any other manner implying that the copy can be considered as an original;
(iii) make copies of computer programs in digitized form;
(iv) make copies in digital form of databases if the copy is made on the basis of a reproduction of the database in digital form; or
(v) make single copies in digital form of other works than computer programs and databases unless this is done exclusively for the personal use of the copying person himself or his household.

(3) Notwithstanding the provision in subsection (2) (v), it is not permitted without the consent of the author to produce copies in digital form on the basis of a copy that has been lent or hired.

(4) The provision of subsection (1) does not confer a right to engage another person to make copies of

(i) musical works;
(ii) cinematographic works;
(iii) literary works if the other person assists for commercial purposes;
(iv) works of applied art; or
(v) works of art if the copying is in the form of an artistic reproduction.

(5) The provision of subsection (1) does not entitle the user to make copies of musical works and cinematographic works by using technical equipment made

available to the public in libraries, on business premises, or in other places accessible to the public. The same applies for literary works if the technical equipment has been provided for commercial purposes.

Reproduction within Educational Activities

13.–(1) For the purpose of educational activities copies may be made of published works and copies may be made by recording of works broadcast in radio and television provided the requirements regarding extended collective license according to section 50 have been met. The copies thus made may be used only in educational activities comprised by the agreement presumed in section 50.

(2) The provision of subsection (1) concerning recording shall not apply to cinematographic works which are part of the general cinema repertoire of feature films except where only brief excerpts of the work are shown in the telecast.

(3) The provision of subsection (1) concerning reproduction of published works shall not apply to computer programs in digital form.

(4) Teachers and students may as part of educational activities make recordings of their own performances of works if this is not done for commercial purposes. Such recordings may not be used for any other purposes.

(5) If disputes arise on whether, an organisation approved according to section 50(4) to make license agreements according to subsection (1), proposes unreasonable terms to such a license agreement, each party to the license agreement is entitled to bring the dispute before the Copyright License Tribunal cf. § 47. The Tribunal may lay down all the terms of the said license agreement, including terms relating to remuneration.

Reproduction by Business Enterprises, etc.

14.-(1) Public or private institutions, organisations and business enterprises may for internal use for the purpose of their activities by photocopying, etc., make or have copies made of descriptive articles in newspapers, magazines and collections, of brief excerpts of other published works of descriptive nature, of musical works and of illustrations reproduced in association with the text, provided the requirements regarding extended collective license according to section 50 have been met. Such copies may be used only for activities which are covered by the agreement presumed in section 50.

(2) If disputes arise on whether, an organisation approved according to section 50(4) to make license agreements according to subsection (1), proposes unreasonable terms to such a license agreement, each party to the license agreement is entitled to bring the dispute before the Copyright License Tribunal cf. § 47. The Tribunal may lay down all the terms of the said license agreement, including terms relating to remuneration.

Reproduction by Hospitals, etc.

15. Hospitals, nursing homes, prisons and other 24-hour institutions within the social and welfare sector, the prison service, and similar institutions may for the brief use of the inmates and others of the institution make recordings of works broadcast on radio and television if this is not done for commercial purposes. Such recordings may be used only within the institution in question.

Archives, Libraries and Museums

16.-(1) Public archives, public libraries and other libraries that are financed in whole or in part by the public authorities, as well as State-run museums and museums that have been approved in accordance with the Museums Act, may use and distribute copies of works in their activities in accordance with the provisions of subsections (2)-(6) if this is not done for commercial purposes. However, this does not apply for computer programs in digital form, with the exception of computer games.

(2) The institutions may make copies for the purpose of back-up and preservation.

(3) If a copy in an institution's collection is incomplete, the institution may make copies of the missing parts, unless the work can be acquired through general trade or from the publisher.

(4) Libraries may make copies f published works that should be available in the library's collections, but which cannot be acquired through general trade or from the publisher.

(5) The copyright does not prevent the making of copies in accordance with the provisions of the Act on Legal Deposit of Published Material.

(6) Copies that have been made in accordance with subsections (3)-(5) or delivered pursuant to the Act on Legal Deposit of Published Material may be loaned to users. The same applies in special case to copies made in accordance with subsection (2). The provisions in the first and second sentences do not apply to recordings of moving pictures and copies made in digital form or in the form of sound recordings.

(7) The right to exploitation of copies made pursuant to subsections (2)-(5) shall be subject to the provisions otherwise in force.

16 a.-(1) Published works may be made available to individuals at the institutions specified in section 16 (1) for personal viewing or study on the spot by means of technical equipment.

(2) Notwithstanding the provisions of subsection (1), copies that are made or deposited pursuant to the Act on Legal Deposit may only be made available at the Royal Library, the State and University Library and the Danish Film Institute for separate individual persons.

(3) The institutions named in subsection (2) may communicate and hand over legal deposited copies of works that have been broadcast on radio and television, films and works published on electronic communication networks, for research purposes, if the work cannot be acquired through general trade. Such copies may not be used in any other way.

16 b.-(1) Public libraries and other libraries financed in whole or in part by the public authorities may upon request in digital form reproduce articles from newspapers, magazines and composite works, brief excerpts of books and other published literary works, as well as illustrations and music reproduced in connection with the text, provided the requirements regarding the extended collective license according to section 50 have been met. The provision of the first sentence shall not comprise broadcast by radio or television or the making available to the public of works in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2 (4)(i).

(2) If disputes arise on whether, an organisation approved according to section 50(4) to make license agreements according to subsection (1), proposes unreasonable terms to such a license agreement, each party to the license agreement is entitled to bring the dispute before the Copyright License Tribunal cf. § 47. The Tribunal may lay down all the terms of the said license agreement, including terms relating to remuneration.

Visually- and Hearing-handicapped Persons

17.–(1) is permitted to use and distribute copies of published works if the use and the distributed copies are specifically intended for the blind, visually impaired, the deaf and sufferers from speech impediments, as well as persons who on account of handicap are unable to read printed text. The provision of the first sentence does not apply to the use or distribution of copies for commercial purposes.

(2) The provision of subsection (1) does not apply to sound recordings of literary works or use that consists solely of sound recordings of musical works.

(3) Sound recordings of published literary works may be used and distributed for use by visually impaired persons and backward readers if this is not done for commercial purposes. The author is entitled to remuneration. If agreement can not be made on the size of remuneration, each party is entitled to bring the dispute before the Copyright License Tribunal, cf. § 47.

(4) Government or municipal institutions and other social or non-profit institutions may, for the use of visually handicapped and hearing-impaired persons, by means of sound or visual recording produce copies of works broadcast on the radio or television, provided the requirements regarding the extended collective license according to section 50 have been met. Such recording may only be used for the purpose of activities covered by the agreement presumed in section 50.

Production of Anthologies for Educational Use, etc.

18.–(1) Minor portions of literary works and musical works or such works of small proportions may be used in composite works compiling contributions by a large number of authors for use in educational activities, provided that five years have elapsed since the year when the work was published. In connection with the text also works of art and works of a descriptive nature, cf. section 1(2), may be used, provided that five years have elapsed since the year when the work was made

public. The author shall be entitled to remuneration. If agreement can not be made on the size of remuneration, each party is entitled to bring the dispute before the Copyright License Tribunal, cf. § 47.

(2) The provision of subsection (1) does not apply to works prepared for use in educational activities or if the use is for commercial purposes.

(3) A few published songs may be freely used in song booklets produced solely for the use of participants in a particular meeting. However, no more than 300 copies of each booklet may be produced.

Distribution of Copies

19.–(1) Where a copy of a work has been sold or otherwise transferred to others within the European Economic Area with the consent of the author the copy may be further distributed. In respect of further distribution in the form of lending or rental, the provision of subsection (1) shall also apply to sale or assignment in any other form to other persons outside the European Economic Area.

(2) Notwithstanding the provision of subsection (1), copies may not be distributed to the general public through rental without the consent of the author. However, this does not apply to works of architecture and applied art.

(3) Notwithstanding the provision of subsection (1), copies of cinematographic works and copies of computer programs in digitized form may not be distributed to the public through lending without the consent of the author. However, this does not apply if a copy of a computer program in digitized form constitutes a part of a literary work and is lent together with it.

(4) The provision of subsection (1) shall not carry any limitation in the right to receive remuneration etc., under the Act on Public Lending Right Remuneration.

Exhibition of Copies

20. Where a work has been published or if a copy of a work of art has been transferred to other parties by the author, the published or transferred copies may be exhibited in public.

Public Performances

21.–(1) A published work, which is not a dramatic work or a cinematographic work, may be performed in public

(i) on occasions when the audience is admitted free of charge where the performance is not the main feature of the event and where the event does not occur for commercial purposes; and

(ii) where the performance occurs in the case of divine services or educational activities.

(2) The provision of subsection (1)(ii) does not apply to performances on radio or television and to performances in educational activities which occur for commercial purposes.

(3) In public libraries works which have been made public can be made available to individuals for personal viewing or study on the spot by means of technical equipment.

Quotations

22. A person may quote from a work which has been made public in accordance with proper usage and to the extent required for the purpose.

Use of Works of Fine Art, etc.

23.–(1) Works of art and works of a descriptive nature, cf. section 1(2), which have been made public may be used in critical or scientific presentations in connection with the text in accordance with proper usage and to the extent required for the purpose. Reproduction is not allowed for commercial purposes.

(2) Works of art made available to the public may be used in newspapers and periodicals in connection with the reporting of current events in accordance with proper usage and to the extent required for the purpose. The provision of the first sentence does not apply to works produced with a view to use in newspapers or periodicals.

(3) Published works of art or copies of works of art that have been transferred to others by the author may be used in newspapers, periodicals, films and television if the use is of subordinate importance in the context in question.

24.–(1) Works of art included in a collection, or exhibited, or offered for sale may be reproduced in catalogues of the collection. Such works of art may also be used in notices of exhibitions or sale, including in the form of communication to the public.

(2) Works of art may be reproduced in pictorial form and then made available to the public if they are permanently situated in a public place or road. The provision of the first sentence shall not apply if the work of art is the chief motif and its reproduction is used for commercial purposes.

(3) Buildings may be freely reproduced in pictorial form and then made available to the public.

24 a.-(1) A work of art that has been made public may be reproduced, if the terms regarding extend collective license according to section 50 have been met. This shall, however, not apply is the author has issued a prohibition against use of the work in relation to any of the parties to the license agreement.

(2) If disputes arise on whether, an organisation approved according to section 50(4) to make license agreements according to subsection (1), proposes unreasonable terms to such a license agreement, each party to the license agreement is entitled to bring the dispute before the Copyright License Tribunal cf. § 47. The Tribunal may lay down all the terms of the said license agreement, including terms relating to remuneration.

Reporting of Current Events etc.

25. If performance or exhibition of a work is part of a current event and it is used in film, radio or television, the work may be included to the extent the work forms a natural part of the reporting of the current event.

25 a. Works which are part of short reports given access to under section 90(3) of the Radio and Television Broadcasting Act and under provisions issued according to section 90(5) of the same Act, may be reproduced in accordance with section 90(4) of the Radio and Television Broadcasting Act and in accordance with provisions issued according to section 90(5) of the same Act.

Public Proceedings, Public Access, etc.

26. Proceedings in Parliament, municipal councils and other elected public authorities, in judicial proceedings and in public meetings held to discuss general matters may be used without the author's consent. However, the author shall have the exclusive right to publish compilations of his own statements.

27.–(1) Where copies of works protected under this Act have come in to an administrative authority or court in connection with its activities, the copyright shall not prevent other parties from demanding access to copies of works, including demanding a transcript or a copy, in accordance with the provisions of the legislation on access to public documents. The same shall apply to works produced within the administrative authority or court.

(2) The copyright shall not prevent that documents delivered to a public record office or an institution which the Minister for Culture has decided shall be considered equivalent hereto are made available to the public in accordance with the provisions of the legislation on archives. However, it shall be prohibited to issue transcripts or to make copies of private documents.

(3) The right to further exploitation of works to which access has been given in pursuance of subsection (1) or (2) or of which transcripts or copies have been issued shall be subject to the provisions otherwise in force.

28.–(1) Works may to the extent justified by the purpose be used in connection with

(i) judicial proceedings and proceedings before administrative tribunals, etc., and

(ii) proceedings within public authorities and institutions under Parliament.

(2) The right to further exploitation depends on the rules otherwise in force.

Alteration of Buildings and Articles for Everyday Use

29.–(1) Buildings may be altered by the owner without the consent of the author if this is done for technical reasons or for the purpose of their practical use.

(2) Articles for everyday use may be altered by the owner without the consent of the author.

Special Provisions on Radio and Television

30.–(1) DR, TV 2/Danmark A/S and the regional TV 2 companies may on radio or television broadcast published works provided the requirements regarding extended collective license according to section 50 have been met. The provision of the first sentence does not apply to dramatic or cinematographic works.

(2) The author may issue a prohibition to the broadcaster against the broadcast of the work pursuant to subsection (1).

(3) The Minister for Culture may stipulate that the provisions of subsections (1) and (2) shall apply correspondingly to agreements made by other broadcasters.

(4) The provision of subsection (1) shall apply correspondingly if the author of a work of art has transferred one or more copies to others.

(5) The provision of the first sentence of subsection (1) shall not apply to broadcasts on radio and television via satellite unless the broadcaster makes a simultaneous broadcast via a terrestrial network.

(6) If disputes arise on whether, an organisation approved according to section 50(4) to make license agreements according to subsection (1), proposes unreasonable terms to such a license agreement, each party to the license agreement is entitled to bring the dispute before the Copyright License Tribunal, cf. § 47. The Tribunal may lay down all the terms of the said license agreement, including terms relating to remuneration.

30 a.–(1) Works which have been made public and are a part of DR, TV 2/DANMARK A/S and the regional TV 2 companies' own productions can, by the mentioned broadcasters, be repeated and made available in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2 (4)(i), provided that the requirements regarding extended collective license according to section 50 have been met. The provision the first sentence shall apply correspondingly to the making of copies, which are necessary for the reproduction. The provisions of the first and second sentences shall apply exclusively to works which are a part of productions broadcast before January 1, 2007.

(2) The author may issue a prohibition to the broadcaster against the reproduction of the work pursuant to subsection (1).

31.–(1) Broadcasters may for the purpose of their broadcasts record works on tape, film, or any other device that can reproduce them provided they have the right to broadcast the works in question. The right to make such works available to the public shall be subject to the provisions otherwise in force.

(2) The Minister for Culture may lay down rules on the conditions to make such recordings and on their use and storage.

32. Broadcasts of debate programs in which general questions are discussed may be used without the consent of the author. However, the author shall have the exclusive right to publish compilations of his own statements.

33.–(1) Broadcasts of works may be recorded on tape, film or any other device by means of which they can be reproduced and may be stored with the National Media Collection if the broadcast is of documentary value. The Media Collection may produce single copies of the broadcasts for security and protection purposes and for research purposes. The right to further exploitation shall be subject to the provisions otherwise in force.

(2) The Minister for Culture may provide that the provision in subsection (1) shall apply correspondingly to other public archives.

34. Broadcasters may on request deliver recordings of broadcasts to persons who have taken part in the broadcasts in question or who feel offended by comment in a specific broadcast or through public mention of the broadcast in question. Recordings delivered according to the first sentence may be used for internal use only.

35.–(1) Works which are broadcast wireless on radio or television may be retransmitted simultaneously and without alteration via cable systems and may in the same manner be retransmitted to the public by means of radio systems, provided the requirements regarding extended collective license according to section 50 have been met. The provision of the first sentence shall not apply to rights held by broadcasters.

(2) Notwithstanding the provision of subsection (1), works forming part of a wireless radio or television broadcast received by means of the receivers' own antennae, may be retransmitted via cable systems consisting of no more than two connections.

(3) The owner of a system as mentioned in subsection (1) is responsible for an agreement being made regarding retransmission of radio and television broadcasts via the systems. If remuneration to be paid by the owner according to an agreement made in accordance with subsection (1) or an order from the Copyright License Tribunal under section 48(1), is fixed as an amount per connection, the user of the individual connection is under an obligation to pay the owner a corresponding amount.

Special Provisions on Computer Programs, etc.

36.–(1) The person who has the right to use a computer program shall be entitled to

(i) produce such copies of the program and to make such alterations of the program which are necessary for the person to use the computer program in accordance with its intended purpose, including for error correction;

(ii) make a back-up copy insofar as it is necessary for the use of the program; and

(iii) observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing, etc. the program which he is entitled to.

(2) The person who has the right to use a database may perform such actions which are necessary for the person to obtain access to the contents of the database and make normal use of it.

(3) The provisions of subsection (1)(ii) and (iii) and of subsection (2) may not be deviated from by agreement.

37.–(1) Reproduction of the code of a computer program and translation of its form shall be permitted where this is indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(i) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;

(ii) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in (i); and

(iii) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

(2) The provisions of subsection (1) shall not permit the information obtained through its application:

(i) to be used for goals other than to achieve the interoperability of the independently created computer program;

(ii) to be given to others, except where necessary to achieve the interoperability of the independently created computer program; or

(iii) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

(3) The provisions of subsections (1) and (2) may not be deviated from by agreement.

Artists' Resale Right

38.–(1) The author is entitled to remuneration for the resale of copies of works of art, including paintings, collages, drawings, engravings, prints, lithographs, sculptures, tapestries, ceramic art, glass art and photographic works (resale right remuneration). The provision in the first sentence relates to copies of works of art that have been produced in one copy or in a limited quantity by the author himself or with his permission. The provision in the first sentence does not comprise architectural works.

(2) Resale right remuneration shall be paid for all instances of resale in which sellers, buyers or agents are involved on a professional basis in the art market, including auction houses, art galleries and art dealers. The obligation to pay the remuneration rests with the seller or the intermediary. Remuneration shall only be paid if the sales price exceeds 300 euros (excl. VAT). The total remuneration cannot exceed 12,500 euros (excl. VAT) per copy.

(3) The remuneration is calculated as

(i) 5 per cent for the portion of the sale price up to 50,000 euros (excl. VAT),

(ii) 3 per cent for the portion of the sale price from 50,000.01 to 200,000 euros (excl. VAT),

(iii) 1 per cent for the portion of the sale price from 200,000.01 to 350,000 euros (excl. VAT),
(iv) 0.5 per cent for the portion of the sale price from 350,000.01 to 500,000 euros (excl. VAT),
(v) 0.25 per cent for the portion of the sale price exceeding 500,000 euros (excl. VAT).

(4) The right to remuneration shall last until the expiration of the term of copyright, cf. section 63. This right is personal and unassignable. After the death of the author the right shall, however, succeed to the author's spouse and issue. Where the author does not leave behind any spouse or issue, the right of remuneration shall pass to the organisation mentioned in subsection (5).

(5) The right of remuneration of resale right may be exercised only by an organisation approved by the Minister for Culture. The organisation shall be in charge of the collection and make distribution to the beneficiaries. The beneficiary's claim against the organisation shall last until three years have elapsed from the end of the year in which the resale took place. The period of limitation shall be suspended by written demand from the beneficiary.

(6) The Minister for Culture stipulates detailed provisions on the procedure for approval of the joint organisation, mentioned in subsection (5).

(7) The seller or agent, cf. the second sentence in subsection (2), shall
(i) submit an annual statement to the organisation as at 1 June specifying the previous year's sales of works of art that are covered by the resale right scheme, cf. subsections (1) and (2), attested by an authorised public accountant or a registered auditor and
(ii) at the organisation's request and within four weeks of receipt of the request to submit all of the information necessary to secure payment of remuneration when the organisation requests this within three years of the resale.

Remuneration for Reproduction for Private Use

39.–(1) Anyone who for commercial purposes produces or imports sound tapes or videotapes or other devices on to which sound or images can be recorded shall pay remuneration to the authors of the works mentioned in subsection (2).

(2) The remuneration shall be paid for tapes, etc., which are suitable for production of copies for private use, and only for works which have been broadcast on radio or television, or which have been published on phonogram, film, videogram, etc.

(3) Administration and control, including collection, shall be carried out by a joint organisation representing a substantial number of authors, performers and other rightholders, including record producers, etc., and photographers, whose works, performances, etc., are used in Denmark. The organisation shall be approved by the Minister for Culture. The Minister may demand to be supplied with all information about collection, administration and distribution of the remuneration.

(4) The organisation lays down guidelines for payment of the remuneration to the beneficiaries so that to the greatest possible extent distribution will take place in accordance with the copying actually made. One third of the annual amount for

payment shall, however, be used to support purposes common to the authors and others within the groups represented by the organisation, cf. subsection (3).

(5) The Minister for Culture stipulates detailed provisions on the procedure for approval of the joint organisation, mentioned in subsection (3).

40. For 2006, the remuneration per minute playing time for analogue sound tapes is DKK 0.0603 and for analogue videotapes DKK 0.0839.

(2) For 2006, the remuneration for digital sound media is DKK 1.88 per unit, for digital image media DKK 3 per unit and for digital memory cards DKK 4.28 per unit.

(3) The remuneration specified in subsections (1) and (2) shall be adjusted annually from 2007 by the rate adjustment percentage, cf. Act on Rate Adjustment Percentage.

41.–(1) Companies which for commercial purposes produce or import sound tapes or videotapes, etc., shall be registered with the joint organisation.

(2) The organisation shall issue a certificate for the registration.

(3) Registered companies shall without the remuneration having been settled be entitled to import or from another registered company to receive sound tapes or videotapes liable to remuneration in accordance with section 39.

42.–(1) The remuneration period shall be the month.

(2) Registered companies shall prepare a statement of the number of sound tapes and videotapes liable to remuneration which during the period have been distributed by the company, and their playing time.

(3) Registered companies using sound tapes or videotapes within the company shall include the terms for distribution according to subsection (2).

(4) The statement shall be specified in accordance with guidelines to be laid down by the Minister for Culture according to negotiation with the joint organisation. The Minister for Culture may, moreover, subject to negotiation with the joint organisation lay down guidelines for control measures in connection with the statement mentioned in the first sentence of this subsection.

(5) The Minister for Culture can define rules, the purpose of which is to simplify the scheme with deductions or repayments of remuneration for sound tapes and videotapes, etc., used for professional purposes, cf. section 43 (1) (iii), and section 44 (1) (ii).

(6) Anyone selling sound tapes and videotapes, etc. is obliged when ordered to do so by the organisation to explain within four weeks from whom the tapes, etc. were bought.

43.–(1) A deduction shall be made from the number liable to remuneration made up in accordance with section 42(2):

(i) the number of sound tapes and videotapes distributed to another registered company in accordance with section 41(3);

(ii) the number of exported sound tapes and videotapes;

(iii) the number of sound tapes and videotapes to be used for professional purposes, including educational purposes;
(iv) the number of sound tapes and videotapes to be used for production of recordings to be used for the visually handicapped and hearing-impaired persons;
(v) the number of sound tapes and videotapes to be used for special purposes which by the Minister for Culture have been exempted from the remuneration.

(2) The Minister for Culture may according to negotiation with the joint organisation lay down guidelines for controlling deductions in accordance with subsection (1).

44.–(1) The remuneration shall be repaid in case of:
(i) commercial export of sound tapes or videotapes on which remuneration has been paid;
(ii) utilization of sound tapes or videotapes for professional purposes, including educational purposes, on which remuneration has been paid;
(iii) utilization of sound tapes or videotapes for production of recordings to be used by visually handicapped or hearing-impaired persons, on which remuneration has been paid; or
(iv) utilization of sound tapes or video tapes for special purposes which by the Minister for Culture have been exempted from payment of remuneration, on which remuneration has been paid.

(2) In accordance with negotiation with the joint organisation, the Minister for Culture lays down the guidelines to apply to refunding of remuneration according to subsection (1).

45.–(1) Registered companies shall keep accounts of production, import and distribution etc., of sound tapes and videotapes liable to remuneration.

(2) In accordance with negotiation with the joint organisation, the Minister for Culture lays down guidelines to apply to the accounting of the registered companies, including issue of invoices etc.

(3) Registered companies shall keep accounting material for five years after the end of the financial year.

46. After the end of each remuneration period and not later than at the end of the next month registered companies shall to the joint organisation deliver a statement specifying the number of distributed sound cassette tapes and video cassette tapes, and their playing time, cf. sections 42 and 43. The company shall at the latest together with delivery of the statement pay the remuneration to the organisation. The statement shall be signed by the management of the company.

46 a. The Minister for Culture can compensate rightholders for the difference between the proceeds of the sale of blank dvd’s in a specific year and the proceeds of the sale of blank dvd’s in 2005, to the extend that the proceeds of a specific year is less than in 2005.

The Copyright License Tribunal

47.–(1) The Minister for Culture sets up the Copyright License Tribunal. The Tribunal consists of a chairperson and two members appointed by the Minister for Culture. The chairperson shall be a judge of the Supreme Court.

(2) The Copyright License Tribunal can make decisions according to sections 13, 14 and 16 b, 17(3), 18(1), 24 a, 30, 48(1) and 48(2), 51(2), 68, 75 a(3) and 75 d. The decisions of the Tribunal may not be brought before any other administrative authority.

(3) The Minister for Culture will lay down the rules governing the activities of the Tribunal and may in this connection lay down rules on the covering of the expenses incurred in connection with such activities.

48.–(1) If an organisation approved in accordance with section 50(4) or a broadcaster unreasonably refuses to consent to retransmission via cable systems or wireless of works and broadcasts that are broadcast wireless simultaneously and without alteration or if such retransmission is offered on unreasonable terms, the Copyright License Tribunal may at request grant the necessary permission and lay down the conditions in this respect. The provision of section 50(3), first sentence, shall apply correspondingly. The Copyright License Tribunal's decisions as described in the first sentence are not binding on radio and television companies..

(2) Where in accordance with section 69, a broadcaster refuses to give its consent to a broadcast be recorded in a manner as mentioned in the second division of the first sentence of section 13(1) or section 17(4) or in the absence of any agreement on the conditions of such a recording, the Copyright License Tribunal may at the request of each party grant the necessary permission and lay down the conditions in this respect.

(3) The provision of subsection (2) shall apply only if an organisation of authors has made an agreement comprised by section 50, cf. the second division of the first sentence of section 13(1) or section 17(4). The provision of section 49 shall apply correspondingly.

Statute-barring of Claims for Remuneration

49.–(1) Claims for remuneration according to section 17(3), section 18(1), and section 68 shall become statute-barred after three years from the end of the year in which the utilization of the work took place.

(2) If the claim for remuneration is made by an organisation the provision of subsection (1) shall apply also to the author's claim against the organisation.

(3) The limitation shall be suspended by written demand.

Common Provisions on Extended Collective License

50.–(1) Extended collective license according to sections 13, 14 and section 16 b, section 17(4), and section 24 a, 30, 30 a and 35 may be invoked by users who have made an agreement on the exploitation of works in question with an

organisation comprising a substantial number of authors of a certain type of works which are used in Denmark.

(2) Extended collective license may also be invoked by users who, within a specified field, have made an agreement on the exploitation of works with an organisation comprising a substantial number of authors of a certain type of works which are used in Denmark within the specified field. However, this does not apply, if the author has issued a prohibition against use of his work in relation to any of the contracting parties

(3) The extended collective license gives the user right to exploit other works of the same nature even though the authors of those works are not represented by the organisation. The extended collective license gives the user right only to exploit the works of the unrepresented authors in the manner and on the terms that follow from the license agreement made with the organisation.

(4) Rightholder organisations which make agreements of the nature mentioned in subsection (1) and (2), shall be approved by the Minister for Culture to make agreements within specified fields. The Minister may decide that an approved organisation in certain fields shall be a joint organisation comprising several organisations which meet the conditions of subsection (1) or (2).

(5) The Minister for Culture stipulates detailed provisions on the procedure for approval of the rightholder organisations, mentioned in subsection (4).

51.–(1) For exploitation of works according to section 50 the rules laid down by the organisation with regard to the distribution of remuneration between the authors represented by the organisation shall apply correspondingly to unrepresented authors.

(2) Unrepresented authors may claim an individual remuneration although such a right appears neither from the agreement with the user nor from the organisation's rules on remuneration. The claim for individual remuneration shall be directed to the organisation only. If agreement can not be made on the size of remuneration, each party is entitled to bring the dispute before the Copyright License Tribunal, cf. § 47.

52.–(1) In the absence of any result of negotiations on the making of agreements as mentioned in section 13(1), section 14, section 16 b, section 17(4), section 24 a and section 30 a, each party may demand mediation.

(2) Demands for mediation shall be addressed to the Minister for Culture. The request may be made if one of the parties has broken off the negotiations or rejected a request for negotiations, or if the negotiations do not appear to lead to any result.

(3) The mediation shall be made by a mediator to be appointed by the Minister for Culture. The mediation negotiations shall be based on the parties' proposal for a solution, if any. The mediator may propose to the parties to have the dispute settled by arbitration and may participate in the appointment of arbitrators.

(4) The mediator may make proposals for the solution of the dispute and may demand that such a proposal be submitted to the competent bodies of the parties for adoption or rejection within a time-limit fixed by the mediator. The mediator shall notify the Minister for Culture of the outcome of the mediation.

(5) The mediator may decide that agreements shall remain in force although the agreement term has expired or will expire in the course of the negotiations. However, the agreement cannot be prolonged for more than two weeks after the parties have decided on a final mediation proposal or proposal for arbitration, or after the mediator has notified that there is no basis to make such proposals.

(6) The person who is or who has been mediator must not without authorisation disclose or utilize any knowledge obtained in his capacity of being a mediator.

(7) The Minister for Culture may lay down rules regarding the covering of expenses incurred in connection with the work of the mediator.

Chapter 3
Assignment of Copyright

General Provisions

53.–(1) Subject to the limitations following from sections 3 and 38 the copyright holder may wholly or partially assign his rights under this Act.

(2) The transfer of copies shall not include an assignment of the copyright.

(3) Where a right to exploit the work in a specific manner or through specific means has been assigned, the assignment does not give the assignee the right to exploit the work in any other manners or through any other means.

(4) The provisions of sections 54-59 on assignment of copyright may be deviated from by agreement between the parties except where otherwise provided in the individual provisions.

54.-(1) The assignee shall be under an obligation to exploit the assigned rights. The author may cancel the agreement with 6 months notice, if the assignee has not exploited the rights within 3 years after the time where the agreement has been fulfilled on the part of the author. This does not apply when the exploitation is initiated before the expiration of the notice.

(2) The provisions of subsection (1) cannot be derogated from, unless it is a mere change of the outlined time limits.

55. (Repealed)

Alterations and Reassignment

56.–(1) Assignment of copyright does not give the assignee any right to alter the work unless the alteration is usual or obviously presumed.

(2) Assignment of copyright does not give the assignee any right to reassign copyright unless the reassignment is usual or obviously presumed. The assignor remains liable for the performance of the agreement with the author.

Settlement and Control

57.–(1) If the author's remuneration depends on the assignee's turnover, sales figures, etc., the author may demand that settlement is made at least once a year. The author may likewise demand that the settlement be accompanied by satisfactory information on the circumstances forming the basis of the calculation of the remuneration.

(2) The author may demand that the accounts, bookkeeping and inventory together with certifications by the party who has exploited the work in connection with the annual settlement according to subsection (1) be made available to a state-authorised public accountant or registered accountant appointed by the author. The accountant shall inform the author of the correctness of the settlement and of irregularities, if any. The accountant shall otherwise observe secrecy about all other matters that become known to him in connection with his review.

(3) The provisions of subsections (1) and (2) shall not be deviated from to the detriment of the author.

Special Provisions concerning Agreements on Recording of Films

58.–(1) An agreement to take part in the recording of a film shall imply that the author shall have no right to oppose that

(i) copies of the film are made;
(ii) copies of the film are distributed to the public;
(iii) the film is performed in public; or
(iv) the film is subtitled or dubbed in another language.

(2) The provision of subsection (1) shall not apply to

(i) works already existing;
(ii) scripts, dialogues and musical works created for the purpose of making the film; or
(iii) the principal director of the film.

Provisions on Unassignable Claims for Remuneration in Connection with Rental of Moving Pictures and Sound Recordings.

58 a. If an author has assigned his right to make a work available to the public through rental to a producer of moving pictures or sound recordings, the author shall be entitled to an equitable remuneration from the producer for the rental. The right to remuneration may be exercised only through organisations which represent the individual groups of rightholders. The provisions of the first and second sentence may not be deviated from by agreement.

Special Provisions on Computer Programs Produced in the Course of Employment

59. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer the copyright in such a computer program shall pass to the employer.

Commissioned Portraits

60. The author cannot exercise his rights in a commissioned portrait without the consent of the commissioner.

Inheritance and Creditor Proceedings

61.–(1) The usual provisions of the inheritance laws shall apply to the copyright upon the author's death.

(2) The author may give directions in his will with binding effect also for the spouse and issue concerning the exercise of the copyright, or may authorise somebody else to give such directions.

62.–(1) The author's right to control his work shall not be subject to creditor proceedings, either when remaining with the author or when with any person who has acquired the copyright by virtue of marriage or inheritance.

(2) Copies of the work shall not be subject to creditor proceedings either when remaining with the author or when with any person to whom copies have been assigned by virtue of marriage or inheritance if the proceedings are in respect of

(i) manuscripts;
(ii) bases, plates, forms, etc., by which a work of art can be performed; or
(iii) copies of works of art which have not yet been exhibited, offered for sale or in any other way approved for publication.

Chapter 4
Duration of Copyright

63.–(1) The copyright in a work shall last for 70 years after the year of the author's death or with regard to the works mentioned in section 6 after the year of death of the last surviving author. With regard to cinematographic works the copyright, however, shall last for 70 years after the year of death of the last of the following persons to survive:

(i) the principal director;
(ii) the author of the script;
(iii) the author of the dialogue; and
(iv) the composer of music specifically created for use in the cinematographic work.

(2) Where a work is made public without indication of the author's name, generally known pseudonym or signature, the copyright shall last for 70 years after the year in which the work was made public. Where a work consists of parts, volumes, instalments, issues or episodes a separate term of protection shall run for each item.

(3) If within the period mentioned the author is indicated in accordance with section 7 or if it is established that he had died before the work was made public, the duration of copyright shall be calculated in accordance with subsection (1).

(4) Copyright in a work of unknown authorship that has not been made public shall last 70 years after the end of the year in which the work was created.

64. Where a work has not been published previously, the person who lawfully makes the work public or publishes it for the first time after the expiry of copyright protection, shall have rights in the work equivalent to the economic rights attributed by the Act to the person creating a literary or artistic work. This protection shall last for 25 years after the end of the year in which the work was made public or published.

Chapter 5
Other Rights

Performing Artists

65.–(1) The performance of a literary or artistic work by a performing artist may not without his consent

(i) be recorded on tape, film or any other device by means of which it can be reproduced; or

(ii) be made available to the public.

(2) Where a performance has been recorded as stated in subsection (1)(i), it must not without the consent of the performing artist be copied or be made available to the public until 50 years after the end of the year in which the performance took place. However, if a recording of the performance is lawfully published or lawfully communicated to the public during this period, the rights shall expire 50 years from the date of the first such publication, or the first such communication, whichever is the earlier.

(3) An agreement between a performing artist and a film producer to take part in the recording of a film implies that in the absence of any opposite agreement the performing artist is assumed to have assigned his right to the rental of the film to the producer.

(4) The provisions of section 2(2)-(4), sections 3, 7, 11 and 11 a, section 12(1), (2)(v), (3), (4)(i), and (5) first sentence, sections 13, 15, 16 and 16 a, section 17(1), (2) and (4), section 18(1) and (2), section 19(1) and (2), sections 21, 22, 25, 25 a, 27, 28, 30 a, 31, 34, 35, 39-47, 49-57, 58 a, 61 and 62 shall apply correspondingly to performing artists' performances and recordings of such performances.

Producers of Sound Recordings

66.–(1) Sound recordings may not without the consent of the producer be copied or made available to the public until 50 years have elapsed after the end of the year in which the recording was made. If a sound recording is published during this period the protection shall, however, last until 50 years have elapsed after the end of the year of the first publication. If a sound recording is not published but is made public in any other manner within the period mentioned in the first sentence,

the protection shall, however, last until 50 years have elapsed after the end of the year in which it was made public.

(2) The provisions of section 2(2)-(4), section 7 (1), section 11(2) and (3), section 11 a, section 12(1), (2)(v), (3), (4) (i), and (5), first sentence, sections 13, 15, 16 and 16 a, section 17, (1), (2) and (4), section 18(1) and (2), section 19(1) and (2), sections 21, 22, 25, 25 a, 27, 28, 30 a, 31, 34, 39-47 and 49-52 shall apply correspondingly to sound recordings.

(3) Notwithstanding the provision of subsection (1), sound recordings broadcast wireless may be retransmitted via cable systems and be retransmitted to the public by means of radio systems if this is done without alterations and simultaneously with the broadcast.

Producers of Recordings of Moving Pictures

67.–(1) Recordings of moving pictures may not without the consent of the producer be copied or made available to the public until 50 years have elapsed after the end of the year in which the recording was made. If a recording of a moving picture is published or made public during this period the protection shall, however, last until 50 years have elapsed after the end of the year in which it was first published or made public, whichever is the earlier.

(2) The provisions of section 2(2)-(4), section 7(1), section 11(2) and (3), section 11 a, section 12(1), (2)(v), (3), (4) (ii), and (5), first sentence, sections 13, 15, 16 and 16 a, section 17 (1) and (4), section 18(1) and (2), section 19(1) and (2), sections 22, 25, 25 a, 27, 28, 30 a, 31, 32, 34, 39-47 and 49-52 shall apply correspondingly to recordings of moving pictures.

(3) Notwithstanding the provision of subsection (1), recordings of moving pictures broadcast wireless on television may be retransmitted via cable systems and be retransmitted to the public by means of radio systems if this is done without alterations and simultaneously with the broadcast.

Remuneration for Use of Sound Recordings in Broadcasts on Radio and Television, etc.

68.–(1) Notwithstanding the provisions of section 65(2) and section 66(1), published sound recordings may be used in broadcasts on radio and television and for other public performances. The provision of the first sentence shall not apply to public performance in the form of the making available to the public of published sound recordings in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2(4)(i).

(2) Performing artists and producers of sound recordings shall be entitled to remuneration. The claim for remuneration may be made only through a joint organisation approved by the Minister for Culture, which comprises performers as well as producers of sound recordings. If agreement can not be made on the size of remuneration, each party is entitled to bring the dispute before the Copyright License Tribunal, cf. § 47.

(3) The Minister for Culture stipulates detailed provisions on the procedure for approval of the joint organisation, mentioned in subsection (2).

(4) The provisions of subsections (1) and (2) shall not apply to broadcasts on television and other public performances of cinematographic works if sound and images are broadcast or performed simultaneously.

(5) When the user of a sound recording in relation to this provision does not pay the remuneration set out in the parties license agreement or by the decision of the Copyright License Tribunal, judgement can be obtained, stating that the said exploitation only can be done with the consent of the author, until remuneration have been paid.

Broadcasters

69.–(1) A radio or television broadcast may not without the consent of the broadcaster be rebroadcast by others or in any other manner be performed in public. Neither may the broadcast without consent be photographed or recorded on tape, film or any other device by means of which it can be reproduced.

(2) Where a broadcast is photographed or recorded as mentioned in subsection (1), it must not without the consent of the broadcaster be copied or made available to the public until 50 years have elapsed after the end of the year in which the broadcast took place.

(3) The provisions of section 2(2)-(4), section 7(1), 11(2) and (3), section 11 a, section 12(1), (2)(v), (3), (4)(ii) and (5) first sentence, sections 15-16 a, section 17(1) and (2), section 19(1) and (2), sections 21, 22 and 25 and 25 a, section 27(1) and (3) and sections 28, 31, 32 and 39-46 shall apply correspondingly to radio and television broadcasts.

Producers of Photographic Pictures

70.–(1) The person who produces a photographic picture (the photographer) shall enjoy the exclusive right to make copies of it and make it available to the public.

(2) The rights in a photographic picture shall last until 50 years have elapsed from the end of the year in which the picture was taken.

(3) The provisions of section 2(2)-(4), sections 3, 7, 9, 11 and 11 a, section 12(1), (2)(v) and (3), sections 13-16 b, section 17(1) and (4), section 18(1) and (2), section 19(1) and (2), sections 20, 21 and 23, section 24(1) and (2), sections 24 a, 25, 25 a, 27, 28, 30-31, 34, 35, 39-47, 49-58 and sections 60-62 shall apply correspondingly to photographic pictures. If a photographic picture is subject to copyright according to section 1, this right may also be exercised.

Producers of Catalogues, etc.

71.–(1) The person who produces a catalogue, a table, a database or the like, in which a great number of items of information has been compiled, or which is the result of a substantial investment, shall have the exclusive right to control the prod-

uct in question as a whole or an essential part thereof by making copies of it and by making it available to the public.
(2) The provision of subsection (1) shall apply correspondingly to a reproduction or making available to the public of insubstantial parts of the contents of a catalogue, a table, a database or the like, which is made repeatedly and systematically, if the said acts may be equalled to acts which conflict with normal exploitation of the products in question or which unreasonably prejudice the legitimate interests of the producer.

(3) If products of the nature mentioned in subsection (1) or parts thereof are subject to copyright or other protection, such rights may also be exercised.

(4) The protection according to subsection (1) shall last until 15 years have elapsed after the end of the year in which the product was produced. If a product of the said nature is made available to the public within this period of time, the protection shall, however, subsist until 15 years have elapsed after the end of the year in which the product was made available to the public for the first time.

(5) The provisions of section 2(2)-(4), sections 6-9, section 11(2) and (3), section 12(1) and (2)(iv), (4)(iii) and (5) second sentence, sections 13-17, section 18(1) and (2), section 19(1) and (2),section 20-22, 25, 27, 28, 30-32, 34 and 35, section 36(2) and (3), section 47 and sections 49-52 shall apply correspondingly to the catalogues, tables, databases, etc., mentioned in subsection (1).

(6) Terms of agreement which extend the right of the producer according to subsection (1) in a product made public shall be null and void..

Press Releases

72. Press releases supplied under contract from foreign news agencies or from correspondents abroad, may not without the consent of the recipient be made available to the public through the press, the radio or in any other similar manner until after 12 hours after they have been made public in Denmark.

Chapter 6
Various Provisions

Protection of Titles, etc.

73.–(1) A literary or artistic work may not be made available to the public under a title, pseudonym or signature likely to be confused with a work previously made public or with its author.

(2) Where the publication of the work made public previously has taken place less than three months prior to the publishing of the other work, the provision of subsection (1) shall not apply unless it may be presumed that confusion was intended.

Signing of Works of Art

74.–(1) The name or signature of the artist may not be placed on a work of art by others than himself without his consent.

(2) The name or signature of the artist may not in any case be put on a reproduction in such a manner that the reproduction may be confused with the original.

Moral Rights after the Expiration of Copyright

75. Although the copyright has expired a literary or artistic work may not be altered or made available to the public contrary to section 3(1) and (2) if cultural interests are thereby violated.

Public Performance of Musical Works

75 a.–(1) Commercial activity whereby a representative of the owner of the copyright or a contractual owner of this right makes agreements on public performance of a musical work protected under this Act, shall be approved by the Minister for Culture. The Minister may lay down specific requirements for the approval. Agreements made in contravention of the first and second sentence shall be null and void.

(2) The Minister for Culture stipulates detailed provisions on the procedure for approval, mentioned in subsection (1).

(3) If an organisation, etc., approved in accordance with subsection (1) stipulates unreasonable terms for consenting to the public performance of musical works, the Copyright License Tribunal may at request lay down the conditions for the performance. The provisions of section 47(2), second sentence and section 47 (3), shall apply correspondingly.

Chapter 6 a

Technical Measures, etc.

75 b. It is not permitted to market or for commercial purposes possess means the only purpose of which is to facilitate unlawful removal or circumvention of technical devices which are used to protect a computer program.

75 c.–(1) It is not permitted to enable circumvention of effective technical measures without the consent of the rightholder.

(2) It is not permitted to produce, import, distribute, sell, rent, advertise for sale or rental of or to possess for commercial purposes devices, products or components that

(i) are promoted, advertised or marketed for the purpose of circumvention of effective technical measures;

(ii) have only a limited commercially significant purpose or use other than to circumvent effective technical measures; or

(iii) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of effective technical measures.

(3) The provision of subsection (2) shall apply correspondingly to services.

(4) The expression effective technological measures in subsections (1) and (2) shall mean any effective technological measures that, in the normal course of their operation, are designed to protect works and performances and productions, etc. protected under this Act.

(5) The provisions of subsections (1)-(4) shall not apply to the protection of computer programs.

(6) The provisions of subsections (1)-(4) shall not prevent research into cryptography.

75 d.–(1) The Copyright License Tribunal, cf. section 47(1), may, upon request, order a rightholder who has used the effective technological measures mentioned in section 75 c(1) to make such means available to a user which are necessary for the latter to benefit from the provisions of section 15 and 16, section 17(1)-(3), section 18(1) and (2), section 21(1)(ii), section 23(1) and sections 26-28, 31 and 68. If the rightholder does not comply with the order within 4 weeks from the decision of the Tribunal, the user may circumvent the effective technological measure, notwithstanding the provision of section 75 c(1). The provisions of the first and second sentences shall apply only to users with legal access to the work or the performance or the production, etc.

(2) The provision of subsection (1) shall apply only to the extent that the rightholder has not, by voluntary measures, including agreements with other parties concerned, ensured that the user may benefit from the provisions mentioned in subsection (1) notwithstanding the use of effective technological measures.

(3) The provision of subsection (1) shall not apply to works and performances or productions, etc. made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2(4)(i).

75 e.–(1) It is not permitted without the consent of the rightholder to

(i) remove or alter any electronic rights-management information; or

(ii) distribute, import for distribution or communicate to the public works and performances or productions, etc. from which electronic rights-management information has been removed or altered without consent.

(2) The provision of subsection (1) shall apply only if the actions concerned are carried out by a person who knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of the right to a work or another performance or production, etc. protected under this Act.

Chapter 7
Enforcement of the Law

Penal Sanctions

76.–(1) Anyone who with intent or by gross negligence
(i) violates section 2 or section 3;
(ii) violates sections 65, 66, 67, 69, 70 or 71;
(iii) violates section 11(2), section 60 or sections 72-75;
(iv) fails to file a statement or information according to section 38(7);
(v) fails to register or fails to disclose information to the joint organisation according to section 41(1), section 42(6) and the first sentence of section 46, or fails to keep and hold accounts according to section 45; or
(vi) violates regulations laid down pursuant to section 61(2)
is liable to a fine.

(2) Where an intentional violation of the provisions mentioned in subsection (1)(i) and (ii) has been committed by using works, performances or productions protected under sections 65-71 or by distributing copies hereof among the general public, the punishment may under particularly aggravating circumstances be increased to imprisonment in one year and 6 months, unless a more severe punishment is provided by section 299 b in the penal code. Particularly aggravating circumstances are deemed to exist especially where the offence is commercial, concerns production or distribution of a considerable number of copies, or where works, performances or productions are made available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them, cf. the second division of section 2 (4)(i).

77.(1) Where copies of works or of performances or productions that are protected under sections 65-71 have been produced outside Denmark under such circumstances that a similar production in Denmark would have been in conflict with the law, anyone who with intent or by gross negligence imports such copies with a view to making them available to the public shall be liable to a fine.
(2) The provision of section 76(2) shall apply correspondingly to intentional violations of the provision of subsection (1).

78.(1) Anyone who with intent or by gross negligence violates section 75 b or 75 c is liable to a fine. Anyone who with intent violates section 75 e is liable to a fine.

79. In regulations issued pursuant to section 16, section 31(2), section 42(4), section 43(2), section 44(2) and section 45(2) may be laid down a fine for violation of provisions of the regulations.

80. Companies, etc. (legal persons) may be liable to punishment under the provisions of Chapter 5 of the Criminal Code.

Legal Proceedings

81.(1) Legal proceedings in respect of violations comprised by section 76(1), section 77(1) or section 79 shall be instituted at the instance of the aggrieved party.

(2) After the death of the author, legal proceedings in respect of violations of section 3 and of the regulations laid down pursuant to section 61(2) shall, moreover, be instituted by the author's spouse, relative in direct line of ascent or descent, or any sisters or brothers.

(3) After the death of the author, legal proceedings in respect of violation of sections 3 and 73-74 shall, moreover, be instituted by the public authorities. However, legal proceedings in respect of violations of section 3 may be instituted by the public authorities only where cultural interests must be deemed to be infringed by the violation.

(4) Notwithstanding the provision of subsection (1), legal proceedings shall be instituted by the public authorities in the event of violations of section 75.

(5) Legal proceedings shall be instituted by the public authorities in the event of violations of section 78, cf. section 75 b and section 75 c(2).

(6) Legal proceedings shall be instituted by the aggrieved party in the event of violations of section 78, cf. section 75 c(1) and section75 e.

82. Legal proceedings in respect of violations comprised by section 76(2) or section 77(2) shall only be instituted by request if the aggrieved party, unless public interests require legal proceedings.

Damages and Compensation

83.–(1) Anyone who with intent or by negligence violates any of the provisions of sections 76 and 77 shall pay

(i) reasonable remuneration to the infringed party for the exploitation

(ii) damages to the infringed party for any additional damage caused by the violation.

(2) When setting the damages according to subsection (1)(ii), consideration shall be given to such matters as the infringed party's loss of profits and the offender's unfair profits.

(3) In cases covered by subsection (1), compensation can also be set to the infringed party for non-financial damage.

Destruction, etc.

84.–(1) The court can by sentence decide that copies infringing the right to works or productions protected according to sections 65-71 shall

(i) be recalled from the channels of commerce,

(ii) be definitively removed from the channels of commerce,

(iii) be destroyed or

(iv) be handed over to the infringed party.

(2) Subsection (1) applies correspondingly to materials, tools, etc. that have primarily been used for illegal production or application of copies of the work or the production.

(3) Measures according to subsection (1) shall be undertaken without any form of compensation to the offender and does not have any effect on any possible com-

pensation to the infringed party. Measures shall be undertaken at the offender's expense, unless special reasons dictate otherwise.

(4) In considering a request for corrective measures according to subsection (1) the need for proportionality between the seriousness of the infringement and the remedies ordered as well as the interests of third parties shall be taken into account by the court.

Publication of Judgements

84 a.-(1) In a judgement in which someone is sentenced according to sections 83 or 84, the court may upon request decide that the judgement shall be published in full or in part.

(2) The obligation to publish rests with the offender. Publication shall be arranged at the offender's expense and in as prominent a way as can reasonably be expected.

Disclosure of Information

84 b. If customs and/or tax authorities presume a violation covered by section 76 or 77, information relating to the presumption can be disclosed to the rightholder.

Chapter 8
Scope of Application of this Act

Copyright

85.–(1) The provisions of this Act concerning copyright shall apply to

(i) works of persons who are nationals of or who have their habitual residence in a country within the European Economic Area;

(ii) works first published in a country within the European Economic Area, or first published simultaneously in a country within the European Economic Area and in another country;

(iii) cinematographic works, the maker of which has his headquarters or his habitual residence in a country within the European Economic Area;

(iv) buildings situated in a country within the European Economic Area; and

(v) works of art incorporated in a building or other structure in a country within the European Economic Area.

(2) Where subsection (1)(ii) is applied, publication shall be considered as simultaneous if the work is published in a country within the European Economic Area within 30 days of its publishing in another country.

(3) Where subsection (1)(iii) is applied, the person or corporate body whose name appears on the cinematographic work in the usual manner shall, in the absence of information to the contrary, be presumed to be the maker of the said work.

(4) The provision of section 38 shall apply to works of persons who are nationals of or who have their habitual residence in a country within the European Economic Area.

(5) The provisions of section 64 shall apply to publications etc. made by

(i) persons who are nationals of or who have their habitual residence in a country within the European Economic Area; or

(ii) companies having their headquarters in a country within the European Economic Area.

(6) The provisions of sections 73-75 shall apply to any work.

Other Rights

86.–(1) The provisions of section 65 shall apply to

(i) performances which have taken place in a country within the European Economic Area; and

(ii) performances which are reproduced on sound recordings which are protected in accordance with the provision of subsection (2).

(2) The provisions of section 66 shall apply to

(i) sound recordings that have taken place in a country within the European Economic Area;

(ii) sound recordings that are made by persons who are nationals of or who have their habitual residence in a country within the European Economic Area; and

(iii) sound recordings that are made by companies having their headquarters in a country within the European Economic Area.

(3) The provision of section 67 shall apply to

(i) recordings of moving pictures that have taken place in a country within the European Economic Area;

(ii) recordings of moving pictures that have been made by persons who are nationals of or who have their habitual residence in a country within the European Economic Area; and

(iii) recordings of moving pictures that have been made by companies having their headquarters in a country within the European Economic Area.

(4) The provision of section 69 shall apply to

(i) broadcasts which have taken place in a country within the European Economic Area; and

(ii) broadcasters which have their headquarters in a country within the European Economic Area.

(5) The provision of section 70 shall apply to

(i) photographs made by persons who are nationals of or who have their habitual residence in a country within the European Economic Area; and

(ii) photographs incorporated in buildings or structures in a country within the European Economic Area.

(6) The provision of section 71 shall apply to

(i) catalogues, etc. made by persons who are nationals of or who have their habitual residence in a country within the European Economic Area; and

(ii) catalogues, etc. made by companies which have their headquarters in a country within the European Economic Area.

(7) The provisions of subsection (6) shall apply correspondingly to press releases as mentioned in section 72.

(8) Notwithstanding the provision of subsection (1), the provision of section 65(1) on recording shall apply to all sound recordings of performances. Notwithstanding the provision in subsection (2), section 66(1) on copying shall apply to all sound recordings. Notwithstanding the provisions in subsections (1)-(4), the provisions of section 65(2), section 66(1), section 67(1) and section 69(2) on the distribution of copies to the public shall apply to all performances, sound recordings, moving pictures recordings and radio and television broadcasts.

Special Provisions on Satellite Broadcasting

87.–(1) Satellite broadcasting shall be deemed to occur in Denmark if the programme-carrying signals intended for reception by the public under the control and responsibility of a broadcaster in this country are introduced into an uninterrupted chain of communication leading to the satellite and down towards the earth.

(2) Satellite broadcasting shall also be deemed to occur in Denmark if the introduction in the chain of communication occurs in a State that is not a member of the European Economic Area and which does not provide the level of protection provided for under Chapter II of Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission in the following cases

(i) if the programme-carrying signals are transmitted to the satellite from an uplink station situated in Denmark. The rights provided for under sections 2, 64, and 65-73 shall then be exercisable against the person operating the station;

(ii) if there is no use of an uplink station situated in an EEA Member State and a broadcaster with its headquarters in Denmark has commissioned the introduction into the chain of communication. The rights provided for under sections 2, 64, and 65-73 shall then be exercisable against the broadcaster.

Application of this Act with Respect to other Countries, etc.

88.–(1) The Minister for Culture may define more detailed rules under which the application of the provisions of this Act may be extended to other countries conditional upon reciprocity.

(2) The Minister for Culture may also define more detailed rules under which the Act may be made applicable to works first published by international organisations and to unpublished works that such organisations are entitled to publish.

Chapter 9
Coming into Force and Transitional Provisions

89.–(1) This Act shall come into force on July 1, 1995.

(2) Simultaneously the following Acts shall be repealed:

(i) Act on the Copyright in Literary and Artistic Works, cf. Consolidated Act No. 1170 of December 21, 1994; and

(ii) Act on the Right in Photographic Pictures, cf. Consolidated Act No. 715 of September 8, 1993.

(3) A proposal for revision of sections 75 c and 75 d shall be submitted to the Folketing (Parliament) in the year 2005-2006 at the latest.

90.–(1) This Act shall apply also to works and performances and productions, etc., made before the coming into force of this Act.

(2) This Act shall not apply to acts of exploitation concluded or rights acquired before the coming into force of this Act. Copies of works or of performances or productions etc. can still be distributed to the public and be exhibited in public if they have been lawfully made at a time when such distribution or exhibition was permitted. The provisions of section 19(2) and (3) shall, however, always apply to rental and lending carried out after the coming into force of this Act.

(3) If by application of the new provisions the term of protection for a work or a performance or a production etc. shall become shorter than according to the previous provisions those provisions shall apply. The provision of section 63(4) shall, however, always apply.

91.–(1) The provisions of sections 54, 55, 56, and 58 shall not apply to agreements made before July 1, 1995.

(2) The provision of section 65(3) shall also apply to agreements made before July 1, 1995.

(3) The provisions of section 30(5) and section 87(2) shall not apply until January 1, 2000 to agreements made before January 1, 1995.

(4) The provision of section 59 shall not apply to computer programs produced before January 1, 1993.

(5) The provision of section 70 shall not apply to photographic pictures made before January 1, 1970.

92. The special privileges and prohibitions provided under older laws shall remain in force.

93. This Act shall not extend to the Faeroe Islands and Greenland but may by Royal Ordinance be brought into full or partial operation in the Faeroe Islands and Greenland, subject to such modifications as required by the special conditions obtaining in the Faeroe Islands and Greenland.

Act no. 1404 of 27 December 2008 to amend the Trademark Act, The Penal Code, the Radio and Television Broadcasting Act and various other Acts[2], contains the following coming into force provisions, etc.:

Section 9

(1)This Act enters into force 1 January 2009
(2) (omitted)
(3) (omitted)
(4) (omitted)

Section 10

(1) This Act shall not extend to the Faeroe Islands and Greenland.
(2) Section 1-5 of the Act may by Royal Ordinance be brought into operation in full or in part in the Faeroe Islands and Greenland subject to such modifications as required by the special conditions obtaining in the Faeroe Islands and Greenland.
(3) (omitted)

Act no. 510 of 12. June 2009 to amend the Copyright Act (Implementation of the Service Directive etc.) contains the following coming into force provisions etc.:

Section 2

This Act enters into force 28 December 2009

Section 3

This Act shall not extend to the Faeroe Islands and Greenland, but may by Royal Ordinance be brought into operation for these regions subject to such modifications as required by the special conditions obtaining in the Faeroe Islands and Greenland.

Act no. 1269 of 16 December 2009 to amend the Radio and Television Broadcast Act and the Copyright Act (Implementation of the AVMS-directive) contains the following coming into force provisions etc.:

Section 3

(1) This Act enters into force 18 December 2009
(2) Section 90(3) of the Radio and Television Broadcast Act[3], as drawn up by section 1() is only applicable to exclusive rights transmissions, which have been agreed upon or which have been prolonged after this Act has entered into force

---

[2] Section 5 of the act contains an amendment of the Copyright Act.

(3) (Omitted)

(4) This Act shall not extend to the Faeroe Islands and Greenland. Section 2 of the Act may by Royal Ordinance be brought into operation in full or in part for Greenland subject to such modifications as required by the special conditions obtaining Greenland.

---

[3] Section 90(3) of the Radio and Television Broadcasting Act forms the basis for section 25 a of the Copyright Act. Section 25 a concerns the use of short reports from events of great interest to the public.

The Act on Processing of Personal Data [Persondataloven][1]

Act No. 429 of 31 May 2000 as amended by section 7 of Act No. 280 of 25 April 2001, section 6 of Act No. 552 of 24 June 2005, section 2 of Act No. 519 of 6 June 2007, section 1 of Act No. 188 of 18 March 2009, section 2 of Act No. 503 of 12 June 2009, section 2 of Act No. 422 of 10 May 2011 and section 1 of Act No. 1245 of 18 December 2012.

This version is translated for the Danish Data Protection Agency. The official version is published in "Lovtidende" (Official Journal) on 2 June 2000. Only the Danish version of the text has legal validity. This version is updated with amendments until December 2012.

Title I

General Provisions

Chapter 1

Scope of the Act

1. - (1) This Act 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 Act shall further apply to other non-automatic systematic processing of data which is performed for private persons or bodies and which includes data on individual persons' private or financial matters or other data on personal matters which can reasonably be claimed to be withheld from the public. However, this shall not apply to Chapters 8 and 9 of this Act.

(3) Section 5 (1) to (3), sections 6 to 8, section 10, section 11 (1), section 38 and section 40 of the Act also apply to manual transmission of personal data to another administrative authority. The Danish Data Protection Agency is responsible for the supervision of such transmission, in accordance with chapter 16 of the Act, as mentioned in the first sentence.

(4) This Act shall further apply to the processing of data concerning companies, etc., see subsections (1) and (2), if the processing is carried out for credit information agencies. The same shall apply in the case of processing of data covered by section 50 (1) 2.

(5) Chapter 5 of the Act shall also apply to the processing of data concerning companies, etc., see subsection (1).

(6) In other cases than those mentioned in subsection (4), the Minister of Justice may decide that the provisions of this Act shall apply, in full or in part, to the processing of data concerning companies, etc. which is performed for private persons or bodies.

(7) In other cases than those mentioned in subsection (5), the competent Minister may decide that the provisions of this Act shall apply, in full or in part, to the processing of data concerning companies, etc., which is performed on behalf of public administrations.

(8) This Act shall apply to any processing of personal data in connection with video surveillance.

2. - (1) Any rules on the processing of personal data in other legislation which give the data subject a better legal protection shall take precedence over the rules laid down in this Act.

---

[1] Cf. http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data.

(2) This Act shall not apply where this will be in violation of the freedom of information and expression, see Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(3) This Act shall not apply to the processing of data undertaken by a natural person with a view to the exercise of purely personal activities.

(4) The provisions laid down in Chapters 8 and 9 and sections 35 to 37 and section 39 shall not apply to processing of data which is performed on behalf of the courts in the area of criminal law. Nor shall the provisions laid down in Chapter 8 of the Act and sections 35 to 37 and section 39 apply to processing of data which is performed on behalf of the police and the prosecution in the area of criminal law.

(5) This Act shall not apply to the processing of data which is performed on behalf of Folketinget (the Danish Parliament) and its related institutions.

(6) This Act shall not apply to the processing of data covered by the Act on information databases operated by the mass media.

(7) This Act shall not apply to information databases which exclusively include already published periodicals or sound and image programmes covered by paragraphs 1 or 2 of section 1 of the Act on media responsibility, or part hereof, provided that the data are stored in the database in the original version published. However, sections 41, 42 and 69 of the Act shall apply.

(8) Furthermore, this Act shall not apply to information databases which exclusively include already published texts, images and sound programmes which are covered by paragraph 3 of section 1 of the Act on media responsibility, or parts hereof, provided that the data are stored in the database in the original version published. However, sections 41, 42 and 69 of the Act shall apply.

(9) This Act shall not apply to manual files of cuttings from published, printed articles which are exclusively processed for journalistic purposes. However, sections 41, 42 and 69 of the Act shall apply.

(10) Processing of data which otherwise takes place exclusively for journalistic purposes shall be governed solely by sections 41, 42 and 69 of this Act. The same shall apply to the processing of data for the sole purpose of artistic or literary expression.

(11) This Act shall not apply to the processing of data which is performed on behalf of the intelligence services of the police and the national defence.

Chapter 2

Definitions

3. - (1) For the purpose of the Act:

1. ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’);

2. ‘processing’ shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means;

3. ‘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;

4. ‘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;

5. ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

6. ‘third party’ shall mean any natural or legal person;

7. '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;‘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;

8. ‘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;

9. ‘third country’ shall mean any state which is not a member of the European Community and which has not implemented agreements entered into with the European Community which contain rules corresponding to those laid down in Directive 95/46/EC 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.

Chapter 3

Geographical territory of the Act

4. – (1) This Act shall apply to processing of data carried out on behalf of a controller who is established in Denmark, if the activities are carried out within the territory of the European Community.

(2) This Act shall further apply to processing carried out on behalf of Danish diplomatic representations.

(3) This Act shall also apply to a controller who is established in a third country, if

1. the processing of data is carried out with the use of equipment situated in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the European Community; or

2. 2. the collection of data in Denmark takes place for the purpose of processing in a third country.

(4) A controller who is governed by this Act by rule of paragraph 1 of subsection (3) must appoint a representative established in the territory of Denmark. This shall be without prejudice to legal actions which could be initiated by the data subject against the controller concerned.

(5) The controller shall inform the Data Protection Agency in writing of the name of the appointed representative, see subsection (4)

(6) This Act shall apply where data are processed in Denmark on behalf of a controller established in another Member State and the processing is not governed by Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of data and on the free movement of such data. This act shall also apply if data are processed in Denmark on behalf of a controller established in a state which has entered into an agreement with the European Community which contains rules corresponding to those laid down in the above-mentioned Directive and the processing is not governed by these rules.

Title II
Rules on processing of data

Chapter 4
Processing of data

5. - (1) Data must be processed in accordance with good practices for the processing of data.

(2) Data must be collected for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes. Further processing of data which takes place exclusively for historical, statistical or scientific purposes shall not be considered incompatible with the purposes for which the data were collected.

(3) Data which are to be processed must be adequate, relevant and not excessive in relation to the purposes for which the data are collected and the purposes for which they are subsequently processed.

(4) The processing of data must be organised in a way which ensures the required up-dating of the data. Furthermore, necessary checks must be made to ensure that no inaccurate or misleading data are processed. Data which turn out to be inaccurate or misleading must be erased or rectified without delay.

(5) The data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

6. - (1) Personal data may be processed only if:

1. the data subject has given his explicit consent; or
2. 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
3. processing is necessary for compliance with a legal obligation to which the controller is subject; or
4. processing is necessary in order to protect the vital interests of the data subject; or
5. processing is necessary for the performance of a task carried out in the public interest; or
6. processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
7. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

(2) A company may not disclose data concerning a consumer to a third company for the purpose of marketing or use such data on behalf of a third company for this purpose, unless the consumer has given his explicit consent. The consent shall be obtained in accordance with the rules laid down in section 6 of the Danish Marketing Act.

(3) However, the disclosure and use of data as mentioned in subsection (2) may take place without consent in the case of general data on customers which form the basis for classification into customer categories, and if the conditions laid down in subsection (1) 7 are satisfied.

(4) Data of the type mentioned in sections 7 and 8 may not be disclosed or used by virtue of subsection (3). The Minister of Justice may lay down further restrictions in the access to disclose or use certain types of data by virtue of subsection (3).

7. - (1) No processing may take place of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life.

(2) The provision laid down in subsection (1) shall not apply where:

1. the data subject has given his explicit consent to the processing of such data; or
2. processing is necessary to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of giving his consent; or
3. the processing relates to data which have been made public by the data subject; or
4. the processing is necessary for the establishment, exercise or defence of legal claims.

(3) Processing of data concerning trade union membership may further take place where the processing is necessary for the controller's compliance with labour law obligations or specific rights.

(4) Processing may be carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or tradeunion aim of the data mentioned in subsection (1) relating to the members of the body or to persons who have regular contact with it in connection with its purposes. Disclosure of such data may only take place if the data subject has given his explicit consent or if the processing is covered by subsection (2) 2 to 4 or subsection (3).

(5) The provision laid down in subsection (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 law to the obligation of professional secrecy.

(6) Processing of the data mentioned in subsection (1) may take place where the processing is required for the performance by a public authority of its tasks in the area of criminal law.

(7) Exemptions may further be laid down from the provision in subsection (1) where the processing of data takes place for reasons of substantial public interests. The supervisory authority shall give its authorization in such cases. The processing may be made subject to specific conditions. The supervisory authority shall notify the Commission of any derogation.

(8) No automatic registers may be kept on behalf of a public administration containing data on political opinions which are not open to the public.

8. - (1) No data about criminal offences, serious social problems and other purely private matters than those mentioned in section 7 (1) may be processed on behalf of a public administration, unless such processing is necessary for the performance of the tasks of the administration.

(2) The data mentioned in subsection (1) may not be disclosed to any third party. Disclosure may, however, take place where:

1. the data subject has given his explicit consent to such disclosure; or
2. disclosure takes place for the purpose of pursuing private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relate; or
3. disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority; or
   4. disclosure is necessary for the performance of tasks for an official authority by a person or a company.

(3) Administrative authorities performing tasks in the social field may only disclose the data mentioned in subsection (1) and the data mentioned in section 7 (1) if the conditions laid down in subsection (2) 1 or 2 are satisfied, or if the disclosure is a necessary step in the procedure of the case or necessary for the performance by an authority of its supervisory or control function.

(4) Private persons and bodies may process data about criminal offences, serious social problems and other purely private matters than those mentioned in section 7 (1) if the data subject has given his explicit consent. Processing may also take place if necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject.

(5) The data mentioned in subsection (4) may not be disclosed without the explicit consent of the data subject. However, disclosure may take place without consent for the purpose of pursuing public or private interests, including the interests of the person concerned, which clearly override the interests of secrecy.

(6) Processing of data in the cases which are regulated by subsections (1), (2), (4) and (5) may otherwise take place if the conditions laid down in section 7 are satisfied.

(7) A complete register of criminal convictions may be kept only under the control of a public authority.

9. - (1) Data as mentioned in section 7 (1) or section 8 may be processed where the processing is carried out for the sole purpose of operating legal information systems of significant public importance and the processing is necessary for operating such systems.

(2) The data covered by subsection (1) may not subsequently be processed for any other purpose. The same shall apply to the processing of other data which is carried out solely for the purpose of operating legal information systems, see section 6.

(3) The supervisory authority may lay down specific conditions concerning the processing operations mentioned in subsection (1). The same shall apply to the data mentioned in section 6 which are processed solely in connection with the operation of legal information systems.

10. - (1) Data as mentioned in section 7 (1) or section 8 may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant public importance and where such processing is necessary in order to carry out these studies.

(2) The data covered by subsection (1) may not subsequently be processed for other than statistical or scientific purposes. The same shall apply to processing of other data carried out solely for statistical or scientific purposes, see section 6.

(3) The data covered by subsections (1) and (2) may only be disclosed to a third party with prior authorization from the supervisory authority. The supervisory authority may lay down specific conditions concerning the disclosure.

11. - (1) Official authorities may process data concerning identification numbers with a view to unambiguous identification or as file numbers.

(2) Private individuals and bodies may process data concerning identification numbers where:

1. this follows from law or regulations; or
2. the data subject has given his explicit consent; or
3. the processing is carried out solely for scientific or statistical purposes or if it is a matter of disclosing an identification number where such disclosure is a natural element of the ordinary operation of companies, etc. of the type mentioned and the disclosure is of decisive importance

for an unambiguous identification of the data subject or the disclosure is demanded by an official authority.

(3) Irrespective of the provision laid down in subsection (2) 3, an identification number may not be made public without explicit consent.

12. - (1) Controllers who sell lists of groups of persons for marketing purposes or who perform mailing or posting of messages to such groups on behalf of a third party may only process:

1. data concerning name, address, position, occupation, e-mail address, telephone and fax number;

2. data contained in trade registers which according to law or regulations are intended for public information; and

3. other data if the data subject has given his explicit consent. The consent shall be obtained in accordance with section 6 of the Danish Marketing Act.

(2) Processing of data as mentioned in section 7 (1), or section 8, may, however, not take place. The Minister of Justice may lay down further restrictions in the access to process certain types of data.

13. - (1) Public authorities and private companies, etc. may not carry out any automatic registration of the telephone numbers to which calls are made from their telephones. However, such registration may take place with the prior authorization of the supervisory authority in cases where important private or public interests speak in favour hereof. The supervisory authority may lay down specific conditions for such registration.

(2) The provision laid down in subsection (1) shall not apply where otherwise provided by law or as regards the registration of numbers called by suppliers of telecommunications networks and by teleservices, either for own use or for use in connection with technical control.

14. Data covered by this Act may be archived under the rules laid down in the legislation on archives.

Chapter 5
Disclosure to credit information agencies of data on debts to public authorities

15. – (1) Data on debts to public authorities may be disclosed to credit information agencies in accordance with the provisions laid down in this Chapter of the Act.

(2) No disclosure may take place of data mentioned in section 7 (1) or section 8 (1).

(3) Confidential data disclosed in accordance with the rules laid down in this Chapter shall not for this reason be deemed to be otherwise accessible to the general public.

16. – (1) Data on debts to public authorities may be disclosed to a credit information agency where

1. permitted by law or regulations; or

2. the total amount of debts is due and payable and is in excess of DKK 7,500; however, this amount must not include debts covered by an agreement for an extension of the time for payment or for payment by instalments which has been observed by the data subject.

(2) It is a condition that the same collection authority administers the total amount of debts, see subsection (1) 2.

(3) It is further a condition for the disclosure of data under the provisions of subsection (1) 2, that:

1. the debt may be recovered by means of a distraint, and that two letters requesting payment have been sent to the debtor;

2. execution has been levied, or attempts have been made to levy execution in respect of the claim;

3. the claim has been established by a final and conclusive court order; or

4. the public authorities have obtained the debtor's written acknowledgement of the debt being due and payable.

17. – (1) The public authority concerned shall notify the debtor hereof in writing prior to the disclosure of such data. Disclosure may at the earliest take place 4 weeks after such notification.

(2) The notification referred to in subsection (1) shall include information stating:

1. which data will be disclosed;

2. the credit information agency to which disclosure of the data will take place;

3. when disclosure of the data will take place; and

4. that no disclosure of the data will take place if payment of the debt is effected prior to the disclosure, or if an extension of the time for payment is granted or an agreement is entered into and observed on payment by instalments.

18. The competent minister may lay down more detailed rules on the procedure in relation to disclosure to credit information agencies of data on debts to public authorities. In this connection it may be decided that data on certain types of debts to public authorities may not be disclosed, or may be disclosed only where further conditions than those referred to in section 16 have been complied with.

Chapter 6
Credit information agencies

19. Any person who wishes to carry on business involving processing of data for assessment of financial standing and creditworthiness for the purpose of disclosure of such data (credit information agency) must obtain authorization to do so from the Data Protection Agency prior to commencing such processing, see section 50 (1) 3.

20. – (1) Credit information agencies may only process data which by their nature are relevant for the assessment of financial standing and creditworthiness.

(2) Data as mentioned in section 7 (1) and section 8 (4) may not be processed.

(3) Data on facts speaking against creditworthiness and dating back more than 5 years may not be processed, except where it is obvious in the specific case that the facts in question are of decisive importance for the assessment of the financial standing and creditworthiness of the person concerned.

21. According to the provisions of section 28 (1) or section 29 (1), credit information agencies must notify the person to whom the data relate of the data mentioned in these provisions.

22. – (1) Credit information agencies must, at any time, at the request of the data subject, notify him within 4 weeks, in an intelligible manner, of the contents of any data or assessments relating to him that the credit information agency has disclosed within the last 6 months, and of any other data relating to the data subject that the agency records or stores at the time of the receipt of the request, whether in a processed form or by way of digital media, including any credit ratings.

(2) Where the agency is in possession of further material relating to the data subject, the existence and type of such further material must at the same time be communicated to him, and he shall be informed of his right to inspect such material by personally contacting the agency.

(3) The agency shall further provide information on the categories of recipients of the data and any available information as to the source of the data referred to in subsections (1) and (2).

(4) The data subject may demand that the agency's communication as referred to in subsections (1) to (3) is given in writing. The Minister of Justice shall lay down rules on payment for communications given in writing.

23. – (1) Data on financial standing and creditworthiness may be given only in writing, cf., however, section 22 (1) to (3). The agency may, however, either orally or in a similar manner, disclose summary data to subscribers, provided that the name and address of the inquirer are recorded and stored for at least 6 months.

(2) Publications from credit information agencies may contain data in a summary form only and may be distributed only to persons or companies subscribing to notices from the agency. The publications may not indicate the identification numbers of data subjects.

(3) Disclosure of summary data on indebtedness may only take place where the data originate from the Danish Official Gazette, have been notified by a public authority under the rules laid down in Chapter 5 of this Act, or if the data relate to indebtedness in excess of DKK 1,000 to a single creditor and the creditor has obtained the written acknowledgement by the data subject of the debt being due and payable, or where legal proceedings have been instituted against the debtor concerned. Data on approved debt re-scheduling schemes may, however, not be disclosed. The rules referred to in the first and second clauses of this subsection shall also apply to the disclosure of summary data on indebtedness in connection with the preparation of broader credit ratings.

(4) Summary data on the indebtedness of individuals may be disclosed only in such a manner that the data cannot form the basis for assessment of the financial standing and creditworthiness of other persons than the individuals concerned.

24. Any personal data or credit ratings which turn out to be inaccurate or misleading must be rectified or erased without delay.

25. Where any data or credit ratings which turn out to be inaccurate or misleading have already been disclosed, the agency must immediately give written notification of the rectification to the data subject and to any third party who has received the data or the credit rating during the six months immediately preceding the date when the agency became aware of the matter. The data subject must also be notified of any third party that has been notified under clause 1 of this section, and of the source of the personal data or credit rating.

26. – (1) Where a data subject requests the erasure, rectification or blocking of data or credit assessments which are alleged to be inaccurate or misleading, or requests the erasure of personal data which may not be processed, see section 37 (1), the agency must reply in writing without delay and within 4 weeks from receipt of such a request.

(2) Where the agency refuses to carry out the requested erasure, rectification or blocking, the data subject may within 4 weeks from receipt of the reply of the agency or from expiration of the time-limit for replying laid down in subsection (1) bring the matter before the Data Protection Agency, which will decide whether erasure, rectification or blocking shall take place. The provisions laid down in section 25 shall be correspondingly applicable.

(3) The reply of the agency in the cases mentioned in subsection (2) must contain information about the right to bring the matter before the Data Protection Agency and about the time-limit for such submission.

Chapter 6a
Video surveillance

26 a. – (1) Disclosure of image and sound recordings containing personal data, which are recorded in connection with video surveillance for criminal prevention purposes may only take place if

1. the data subject has given his explicit consent, or
2. the disclosure follows from law, or
3. the data are disclosed to the police for crime-solving purposes.

(2) Recordings as mentioned in subsection (1) must be erased no later than 30 days after the recording has taken place, see however subsection (3).

(3) Recordings may be retained for a longer period than mentioned in subsection (2) if necessary for the controller's handling of a specific dispute. In this case the controller must within the time limit set forth in subsection (2) notify the object of the dispute hereof, and upon request disclose a copy of the recording to the person concerned.

26 b. The provisions of sections 29 and 30 shall apply regardless of any signs posted according to sections 3 and 3 a in the Act on Video Surveillance.

26 c. – (1) Sections 43, 48 and 52 of this Act concerning notification to the Data Protection Agency or the Danish Courts Administration shall not apply to processing of personal data in connection with video surveillance.

(2) Regardless of the exception of personal data processed in connection with video surveillance from section 48, the authorization of the Data Protection Agency must always be obtained when such data are transferred to third countries in accordance with subsections (1) and (3) 2-4 of section 27, if the data are covered by section 50 (1).

26 d. - A municipality may only process image recordings containing personal data which are recorded in connection with video surveillance covered by section 2 a in the Act on Video Surveillance if

1. the data subject has given his explicit consent, or
2. the processing is carried out for the purpose of promoting security for the people present in the monitored area.

(2) Disclosure of recordings as mentioned in subsection (1) may only take place in the cases mentioned in section 26 a (1).

(3) Recordings as mentioned in subsection (1) must be erased no later than 30 days after the recording has taken place.

Chapter 7

Transfer of personal data to third countries

27. – (1) Transfer of data to a third country may take place only if the third country in question ensures an adequate level of protection, see however subsection (3).

(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, in particular the nature of the data, the purpose and duration of the processing operation, the country of origin and country of final destination, the rules of law in force in the third country in question and the professional rules and security measures which are complied with in that country.

(3) In addition to the cases mentioned in subsection (1), transfer of data to a third country may take place if:

1. the data subject has given his explicit consent; or

2. 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

3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

4. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

5. the transfer is necessary in order to protect the vital interests of the data subject; or

6. the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case; or

7. the transfer is necessary for the prevention, investigation and prosecution of criminal offences and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings; or

8. the transfer is necessary to safeguard public security, the defence of the Realm, or national security.

(4) Outside the scope of the transfers referred to in subsection (3), the Data Protection Agency may authorize a transfer of personal data to a third country which does not fulfil the provisions laid down in subsection (1), where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject. Specific conditions may be laid down for the transfer. The Data Protection Agency shall inform the European Commission and the other Member States of the authorizations granted pursuant to this provision.

(5) The transfer of personal data to third countries may be carried out without authorization under the first clause of subsection (4), on the basis of contracts in accordance with the standard contractual clauses approved by the European Commission.

(6) The rules laid down in this Act shall otherwise apply to transfers of personal data to third countries in accordance with subsections (1) and (3) to (5).

Title III

The data subject's rights

Chapter 8

Information to be given to the data subject

28. – (1) Where the personal data have been collected from the data subject, the controller or his representative shall provide the data subject with the following information:

1. the identity of the controller and of his representative;

2. the purposes of the processing for which the data are intended;

3. any further information which is necessary, having regard to the specific circumstances in which the personal data are collected, to enable the data subject to safeguard his interests, such as:

(a) the categories of recipients;
(b) whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply;
(c) the rules on the right of access to and the right to rectify the data relating to the data subject.

(2) The provisions of subsection (1) shall not apply where the data subject already has the information mentioned in paragraphs 1 to 3.

29. - (1) Where the data have not been obtained from the data subject, the controller or his representative shall at the time of undertaking the registration of the data, or where disclosure to a third party is envisaged, no later than the time when the data are disclosed, provide the data subject with the following information:

1. the identity of the controller and of his representative;

2. the purposes of the processing for which the data are intended;

3. any further information which is necessary, having regard to the specific circumstances in which the data are obtained, to enable the data subject to safeguard his interests, such as:
(a) the categories of data concerned;
(b) the categories of recipients;
(c) the rules on the right of access to and the right to rectify the data relating to the data subject.

(2) The rules laid down in subsection (1) shall not apply where the data subject already has the information referred to in paragraphs 1 to 3 or if recording or disclosure is expressly laid down by law or regulations.

(3) The rules laid down in subsection (1) shall not apply where the provision of such information to the data subject proves impossible or would involve a disproportionate effort.

30. – (1) Section 28 (1) and section 29 (1) shall not apply if the data subject's interest in obtaining this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject himself.

(2) Derogations from section 28 (1) and section 29 (1) may also take place if the data subject's interest in obtaining this information is found to be overridden by essential considerations of public interests, including in particular:

1. national security;

2. defence;

3. public security;

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

5. important economic or financial interests of a Member State or of the European Union, including monetary, budgetary and taxation matters; and

6. monitoring, inspection or regulatory functions, including temporary tasks, connected with the exercise of official authority in cases referred to in paragraphs 3 to 5.

Chapter 9

The data subject's right of access to data

31. – (1) Where a person submits a request to that effect, the controller shall inform him whether or not data relating to him are being processed. Where such data are being processed, communication to him shall take place in an intelligible form about:

1. the data that are being processed;
2. the purposes of the processing;
3. the categories of recipients of the data; and
4. any available information as to the source of such data.

(2) The controller shall reply to requests as referred to in subsection (1) without delay. If the request has not been replied to within 4 weeks from receipt of the request, the controller shall inform the person in question of the grounds for this and of the time at which the decision can be expected to be available.

32. – (1) Section 30 shall be correspondingly applicable.

(2) Data which are processed on behalf of the public administration in the course of its administrative procedures may be exempted from the right of access to the same extent as under the rules of section 2, sections 7 to 11 and section 14 of the Act on Public Access to Documents in Administrative Files.

(3) The right of access shall not apply to data processed on behalf of the courts where the data form part of a text which is not available in its final form. This shall, however, not apply where the data have been disclosed to a third party. There is no right of access to the records of considerations of verdicts or to any other court records of the deliberations of the court or material prepared by the courts for the purpose of such deliberations.

(4) Section 31 (1) shall not apply where data are processed solely for scientific purposes or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

(5) As regards processing of data in the area of criminal law carried out on behalf of the public administration, the Minister of Justice may lay down exemptions from the right of access under section 31 (1) in so far as the provision of section 32 (1), see section 30, is assumed to result in requests for rights of access in general being turned down.

33. A data subject who has received a communication in accordance with section 31 (1) shall not be entitled to a new communication until 6 months after the last communication, unless he can establish that he has a specific interest to that effect.

34. – (1) Communication in accordance with section 31 (1) shall be in writing, if requested. In cases where the interests of the data subject speak in favour thereof, the communication may, however, be given in the form of oral information about the contents of the data.

(2) The Minister of Justice may lay down rules for payment for communications which are given in writing by private companies, etc.

Chapter 10

Other rights

35. - (1) A data subject may at any time object in relation to the controller to the processing of data relating to him.

(2) Where the objection under subsection (1) is justified, the processing may no longer involve those data.

36. - (1) If a consumer objects, a company may not disclose data relating to that person to a third company for the purposes of marketing or use the data on behalf of a third company for such purposes.

(2) Before a company discloses data concerning a consumer to a third company for the purposes of marketing or uses the data on behalf of a third company for such purposes, it must check in the CPR-register whether the consumer has filed a statement to the effect that he does not want to be contacted for the purpose of marketing activities. Before data relating to a consumer who has not given such information to the CPR-register are disclosed or used as mentioned in the first clause of this subsection, the company shall provide information about the right to object under subsection (1) in a clear and intelligible manner. At the same time, the consumer shall be given access to object in a simple manner within a period of two weeks. The data may not be disclosed until the time limit for objecting has expired.

(3) Contacts to consumers under subsection (2) shall otherwise take place in accordance with the rules laid down in section 6 of the Danish Marketing Act and rules issued by virtue of section 6 (7) of the Danish Marketing Act.

(4) The company may not demand any payment of fees in connection with objections.

37. - (1) The controller shall at the request of the data subject rectify, erase or block data which turn out to be inaccurate or misleading or in any other way processed in violation of law or regulations.

(2) The controller shall at the request of the data subject notify the third party to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with subsection (1). However, this shall not apply if such notification proves impossible or involves a disproportionate effort.

38. The data subject may withdraw his consent.

39. - (1) Where the data subject objects, the controller may not make him 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.

(2) The provision laid down in subsection (1) shall not apply if that decision:

1. 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; or

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

(3) The data subject has a right to be informed by the controller as soon as possible and without undue delay about the rules on which a decision as mentioned in subsection (1) is based. Section 30 shall be correspondingly applicable.

40. The data subject may file a complaint to the appropriate supervisory authority concerning the processing of data relating to him.

Title IV

Security

Chapter 11

Security of processing

41. - (1) Individuals, companies etc. performing work for the controller or the processor and who have access to data may process these only on instructions from the controller unless otherwise provided by law or regulations.

(2) The instruction mentioned in subsection (1) may not restrict journalistic freedom or impede the production of an artistic or literary product.

(3) The controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act. The same shall apply to processors.

(4) As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions.

(5) The Minister of Justice may lay down more detailed rules concerning the security measures mentioned in subsection (3).

42. - (1) Where a controller leaves the processing of data to a processor, the controller shall make sure that the processor is in a position to implement the technical and organizational security measures mentioned in section 41 (3) to (5), and shall ensure compliance with those measures.

(2) The carrying out of processing by way of a processor must be governed by a written contract between the parties. This contract must stipulate that the processor shall act only on instructions from the controller and that the rules laid down in section 41 (3) to (5) shall also apply to processing by way of a processor. If the processor is established in a different Member State, the contract must stipulate that the provisions on security measures laid down by the law in the Member State in which the processor is established shall also be incumbent on the processor.

Title V

Notification

Chapter 12

Notification of processing carried out for a public administration

43. - (1) The controller or his representative shall notify the Data Protection Agency before processing of data is carried out on behalf of the public administration, cf., however, section 44. The controller may authorize other authorities or private bodies to make such notifications on his behalf.

(2) The notification must include the following information:

1. the name and address of the controller and of his representative, if any, and of the processor, if any;
2. the category of processing and its purpose;
3. a general description of the processing;
4. a description of the categories of data subjects and of the categories of data relating to them;
5. the recipients or categories of recipients to whom the data may be disclosed;
6. intended transfers of data to third countries;
7. a general description of the measures taken to ensure security of processing;

8. the date of the commencement of the processing;

9. the date of erasure of the data.

44. - (1) Processing operations which do not cover data of a confidential nature shall be exempt from the rules laid down in section 43, cf., however, subsection (2). Such processing may further without notification include identification data, including identification numbers, and data concerning payments to and from public authorities, unless it is a matter of processing as mentioned in section 45 (1).

(2) The Minister of Justice shall lay down more detailed rules on the processing operations mentioned in subsection (1).

(3) Processing for the sole purpose of keeping a register which according to law or regulations is intended to provide information to the public in general and which is open to public consultation shall also be exempt from the rules laid down in section 43.

(4) The Minister of Justice may lay down rules to the effect that certain categories of processing of data shall be exempt from the provisions laid down in section 43. This shall, however, not apply to the categories of processing mentioned in section 45 (1).

45. - (1) Before processing operations covered by the obligation to notify in section 43 are carried out, the opinion of the Danish Data Protection Agency must be obtained where:

1. processing includes data which are covered by section 7 (1) and section 8 (1); or

2. processing is carried out for the sole purpose of operating legal information systems; or

3. processing is carried out solely for scientific or statistical purposes; or

4. processing includes alignment or combination of data for control purposes.

(2) The Minister of Justice may lay down rules to the effect that the opinion of the Agency shall be obtained prior to the start of any other processing operations than those mentioned in subsection (1).

46. - (1) Changes in the information mentioned in section 43 (2) shall be notified to the Agency prior to being implemented. Less important changes may be notified subsequently, at the latest 4 weeks after the implementation.

(2) The opinion of the Agency shall be obtained prior to the implementation of changes in the information mentioned in section 43 (2) contained in notifications of processing operations covered by section 45 (1) or (2). Less important changes shall only be notified. Notification may take place subsequently, at the latest 4 weeks after the implementation.

47. - (1) In cases where the data protection responsibility has been delegated to a subordinate authority and the Agency cannot approve the carrying out of a processing operation, the matter shall be brought before the competent Minister who shall decide the matter.

(2) If the Agency cannot approve the carrying out of a processing operation on behalf of a municipal or county authority, the matter shall be brought before the Minister of the Interior who shall decide the matter.

Chapter 13

Notification of processing operations carried out on behalf of a private controller

48. - (1) Prior to the commencement of any processing of data which is carried out on behalf of a private controller, the controller or his representative must notify the Danish Data Protection Agency, cf., however, section 49.

(2) The notification must include the information mentioned in section 43 (2).

49. - (1) Processing of data shall, except in the cases mentioned in section 50 (2), be exempt from the rules laid down in section 48 where:

1. the processing relates to data about employees, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4); or

2. the processing relates to data concerning the health of employees, to the extent that the processing of health data is necessary to comply with provisions laid down by law or regulations; or

3. the processing relates to data concerning employees if registration is necessary under collective agreements or other agreements on the labour market; or

4. the processing relates to data concerning customers, suppliers or other business relations, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4), or to the extent that it is not a matter of processing operations as mentioned in section 50 (1) 4; or

5. the processing is carried out for the purpose of market surveys, to the extent that the processing does not include data as mentioned in section 7 (1) and section 8 (4); or

6. the processing is carried out by an association or similar body, to the extent that only data concerning the members of the association are processed; or

7. the processing is carried out by lawyers or accountants in the course of business, to the extent that only data concerning client matters are processed; or

8. the processing is carried out by doctors, nurses, dentists, dental technicians, chemists, therapists, chiropractors and other persons authorized to exercise professional activities in the health sector, to the extent that the data are used solely for these activities and the processing of the data is not carried out on behalf of a private hospital; or

9. the processing is carried out for the purpose of being used by an occupational health service.

(2) The Minister of Justice shall lay down more detailed rules concerning the processing operations mentioned in subsection (1).

(3) The Minister of Justice may lay down rules to the effect that other types of processing operations shall be exempt from the provision laid down in section 48. However, this shall not apply to processing operations covered by section 50 (1) unless the processing operations are exempted under section 50 (3).

50. - (1) Prior to the commencement of any processing of data which is subject to the obligation to notify in section 48, the authorization of the Data Protection Agency shall be obtained where:

1. the processing includes data as mentioned in section 7 (1) and section 8 (4); or

2. the processing of data is carried out for the purpose of warning third parties against entering into business relations or an employment relationship with a data subject; or

3. the processing is carried out for the purpose of disclosure in the course of business of data for assessment of financial standing and creditworthiness; or

4. the processing is carried out for the purpose of professional assistance in connection with staff recruitment; or

5. the processing is carried out solely for the purpose of operating legal information systems.

(2) In the case of transfer of data as mentioned in subsection (1) to third countries by virtue of section 27 (1) and subsection (3) 2 to 4, the authorization of the Data Protection Agency to such transfer must be obtained, regardless of the processing being otherwise exempt from the obligation to notify by virtue of section 49 (1).

(3) The Minister of Justice may lay down exemptions from the provisions of subsection (1) 1 and subsection (2).

(4) The Minister of Justice may lay down rules to the effect that the authorization of the Agency shall be obtained prior to the commencement of other processing operations subject to the obligation to notify than those mentioned in subsection (1) or subsection (2).

(5) The Agency may when granting an authorization under subsection (1), subsection (2) or subsection (4) lay down specific conditions for the carrying out of the processing operations for reasons of the protection of the privacy of the data subjects.

51. - (1) Changes in the information mentioned in section 48 (2), see section 43 (2), shall be notified to the Agency prior to being implemented. Less important changes may be notified subsequently, at the latest 4 weeks after the implementation.

(2) The authorization of the Agency shall be obtained prior to the implementation of changes in the information mentioned in section 48 (2), see section 43 (2), contained in notifications of processing operations covered by section 50 (1), (2) or (4). Less important changes shall only be notified. Notification may take place subsequently, at the latest 4 weeks after the implementation.

Chapter 14

Notification of processing operations carried out on behalf of the courts

52. The rules laid down in sections 43 to 46 shall apply to the notification to the Danish Court Administration of processing of data carried out on behalf of the courts.

Chapter 15

Miscellaneous provisions

53. Processors established in Denmark who offer electronic processing services must prior to the commencement of such processing operations notify the Data Protection Agency hereof.

54. - (1) The supervisory authority shall keep a register of processing operations notified under sections 43, 48 and 52. This register, which shall, as a minimum, contain the items of information mentioned in section 43 (2), shall be open to consultation by the general public.

(2) A controller must make the information mentioned in section 43 (2) 1, 2 and 4 to 6 concerning the processing operations performed on his behalf available to any person who makes a request to this effect.

(3) The right of access of the general public to the register mentioned in subsection (1) and the information mentioned in subsection (2) may be restricted to the extent that this is necessary for the prevention, detection and prosecution of criminal offences, or where essential considerations of private interests necessitates this.

Title VI

Supervision and final provisions

Chapter 16

The Data Protection Agency

55. - (1) The Data Protection Agency, which consists of a Council and a Secretariat, is responsible for the supervision of all processing operations covered by this Act, cf., however chapter 17.

(2) The day-to-day business is attended to by the Secretariat, headed by a Director.

(3) The Council, which shall be set up by the Minister of Justice, is composed of a chairman, who shall be a legally qualified judge, and of six other members. Substitutes may be appointed for the members of the Council. The members and their substitutes shall be appointed for a term of 4 years.

(4) The Council shall lay down its own rules of procedure and detailed rules on the division of work between the Council and the Secretariat.

56. The Data Protection Agency shall act with complete independence in executing the functions entrusted to it.

57. The opinion of the Data Protection Agency shall be obtained when Orders, Circulars or similar general regulations of importance for the protection of privacy in connection with the processing of data are to be drawn up.

58. – (1) The Data Protection Agency shall supervise, on its own initiative or acting on a complaint from a data subject, that the processing is carried out in compliance with the provisions of this Act and any rules issued by virtue of this Act.

(2) The Data Protection Agency may at any time revoke a decision made in accordance with section 27 (4) or section 50 (2), see section 27 (1) or (3) 2 to 4, if the European Commission decides that transfer of data to specific third countries may not take place or whether such transfers may lawfully take place. This, however, shall only apply where the revocation is necessary in order to comply with the decision of the Commission.

(3) In special cases, the Data Protection Agency may prohibit or suspend the transfer of personal data within the scope of Section 27 (5).

59. – (1) The Data Protection Agency may order a private data controller to discontinue a processing operation which may not take place under this Act and to rectify, erase or block specific data undergoing such processing.

(2) The Data Protection Agency may prohibit a private data controller from using a specified procedure in connection with the processing of data if the Data Protection Agency finds that the procedure in question involves a considerable risk that data are processed in violation of this Act.

(3) The Data Protection Agency may order a private data controller to implement specific technical and organizational security measures to protect data which may not be processed against processing, and to protect data against accidental or unlawful destruction or accidental loss, alteration, and disclosure to any unauthorized person, abuse or any other unlawful forms of processing.

(4) The Data Protection Agency may in special cases issue a prohibitory or mandatory injunction against data processors, see subsections (1) to (3).

60. – (1) The Data Protection Agency shall make decisions in relation to the relevant authority in cases concerning section 7 (7), section 9 (3), section 10 (3), section 13 (1), section 27 (4), sections 28 to 31, section 32 (1), (2) and (4), sections 33 to 37, section 39 and section 58 (2).

(2) In other cases, the Data Protection Agency shall give opinions to the authority acting as controller.

61. No appeals may be brought before any other administrative authority against the decisions made by the Data Protection Agency under the provisions of this Act.

62. – (1) The Data Protection Agency may require to be furnished with any information of importance to its activities, including for the decision as to whether or not a particular matter falls under the provisions of this Act.

(2) The members and the staff of the Data Protection Agency shall at any time, against appropriate proof of identity and without any court order, have access to all premises from which processing operations carried out on behalf of the public administration are administered, or from which there is access to the data subject to processing, and to all premises where data or technical equipment are stored or used.

(3) Subsection (2) shall apply correspondingly as regards processing operations carried out on behalf of private data controllers to the extent that such processing is covered by section 50 or is carried out in connection with video surveillance.

(4) Subsection (2) shall also apply to processing operations carried out by processors as referred to in section 53.

63. – (1) The Data Protection Agency may decide that notifications and applications for authorizations under the provisions of this Act and any changes therein may or shall be submitted in a specified manner.

(2) An amount of DKK 2,000 shall be payable in connection with the submission of the following notifications and applications for authorizations under this Act:

1. Notifications under section 48.
2. Authorizations under section 50.
3. Notifications under section 53.

(3) Notifications as referred to in subsection (2) 1 and 3 shall be deemed to have been submitted only when payment has been effected. The Data Protection Agency may decide that authorizations as referred to in subsection (2) 2 shall not be granted until payment has been effected.

(4) The provisions of subsection (2) 1 and 2 do not apply to processing of data which takes place exclusively for scientific or statistical purposes.

(5) Where a processing operation shall both be notified under section 48 and authorized under section 50, only a single fee shall be payable.

64. – (1) The Data Protection Agency may, on its own initiative or at the request of another Member State, check that a processing operation of data taking place in Denmark is lawful, irrespective of whether or not the processing operation is governed by the legislation of another Member State. The provisions laid down in sections 59 and 62 shall be correspondingly applicable.

(2) The Data Protection Agency may further disclose data to supervisory authorities in other Member States to the extent that this is required in order to ensure compliance with the provisions of this Act or those of the data protection legislation of the Member State concerned.

65. The Data Protection Agency shall submit an annual report on its activities to Folketinget (the Danish Parliament). The report shall be made public. The Data Protection Agency may also make its opinions accessible to the general public. Section 30 shall be correspondingly applicable.

66. The Data Protection Agency and the Danish Court Administration shall co-operate to the extent required to fulfil their obligations, particularly through the exchange of all relevant data.

Chapter 17

Supervision of the courts

67. – (1) The Danish Court Administration shall supervise the processing of data carried out on behalf of the courts.

(2) Such supervision shall include the processing of data as regards the administrative affairs of the courts.

(3) As regards other processing of personal data, the decision shall be taken by the competent court. Such decisions may be appealed against to a higher court. As regards special courts or tribunals whose decisions cannot be appealed against to a higher court, decisions as referred to in clause 1 of this subsection may be appealed against to the division of the High Court within whose jurisdiction the court or tribunal is situated. The period allowed for appeal is 4 weeks from the date on which the individual concerned has been notified of the decision.

68. – (1) The provisions of sections 56 and 58, section 62 (1), (2) and (4), section 63 (1) and section 66 shall apply to the exercise by the Danish Court Administration of its supervision under section 67. The decisions of the Danish Court Administration are final and conclusive.

(2) The opinion of the Danish Court Administration shall be obtained when Orders or similar general legal regulations of importance for the protection of privacy in connection with the processing of data carried out for the courts are to be drawn up.

(3) The Danish Court Administration shall publish an annual report on its activities.

Chapter 18

Liability in damages and criminal liability

69. The controller shall compensate any damage caused by the processing of data in violation of the provisions of this Act unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data.

70. - (1) In the absence of more severe punishment being prescribed under other legislation, any person who commits any of the following offences in connection with processing carried out on behalf of private individuals or bodies shall be liable to a fine or prison up to 4 months:

1. violation of section 4 (5), section 5 (2) - (5), section 6, section 7 (1), section 8 (4), (5) and (7), section 9 (2), section 10 (2) and (3) first clause, section 11 (2) and (3), section 12 (1) and (2) first clause, section 13 (1) first clause, sections 20 - 25, section 26 (1), (2) second clause, and (3), section 26 a, section 27 (1), section 28 (1), section 29 (1), section 31, sections 33 and 34, section 35 (2), sections 36 and 37, section 39 (1) and (3), section 41 (1) and (3), section 42, section 48, section 50 (1) and (2), section 51, section 53 or section 54 (2);

2. failure to comply with the Data Protection Agency's decision under section 5 (1), section 7 (7), section 13 (1), second clause, section 26 (2), first clause, section 27 (4), sections 28 and 29, section 30 (1) section 31, section 32 (1) and (4), sections 33-37, section 39, section 50 (2) or section 58 (2);

3. failure to comply with the requirements of the Data Protection Agency under section 62 (1);

4. obstruction of the Data Protection Agency from access under section 62 (3) and (4);

5. failure to comply with conditions as referred to in section 7 (7), section 9 (3), section 10 (3), section 13 (1), section 27 (4), section 50 (5) or any terms or conditions stipulated for an authorization in accordance with rules issued by virtue of this Act; or

6. failure to comply with prohibitory or mandatory orders issued in accordance with section 59 or in accordance with rules issued by virtue of this Act.

(2) In the absence of more severe punishment being prescribed under other legislation, any person who in connection with a processing operation carried out on behalf of public authorities violates section 41 (3) or section 53 or fails to comply with conditions as referred to in section 7 (7), section 9 (3), section 10 (3), section 13 (1), section 27 (4) or any other terms or conditions for an authorization in accordance with rules issued by virtue of this Act shall be liable to a fine or prison up to 4 months.

(3) In the absence of more severe punishment being prescribed under other legislation, any person who in connection with a processing operation governed by another Member State's legislation fails to comply with the decisions of the Data Protection Agency under section 59 or to fulfil the requirements of the Data Protection Agency under section 62 (1), or obstructs the Data Protection Agency's right of access under section 62 (3) and (4) shall be liable to a fine or prison up to 4 months.

(4) Any rules issued by virtue of this Act may stipulate punishment in the form of a fine or prison up to 4 months.

(5) Criminal liability may be imposed on companies, etc. (legal persons) pursuant to the rules laid down in Chapter 5 of the Danish Penal Code.

71. Any person who carries on business or is engaged in business activities as referred to in section 50 (1) 2 to 5 or section 53 may on conviction of a criminal offence be deprived of the right to carry on such business activities provided that the offence committed gives reasonable ground to fears of abuse. Section 79 (3) and (4) of the Danish Penal Code shall also apply.

Chapter 19

Final provisions, including commencement provisions, etc.

72. The competent minister may in special cases lay down more detailed rules for processing operations carried out on behalf of the public administration.

72 a. The Minster of Justice may lay down more detailed rules regarding protection of personal data in connection with police work and legal cooperation in criminal cases within the European Union, etc.

73. The Minister of Justice may lay down more detailed rules concerning certain categories of processing operations carried out on behalf of private controllers, including rules to the effect that specific categories of data may not be processed.

74. Trade associations and other bodies representing other categories of private controllers may in cooperation with the Data Protection Agency draw up codes of conduct intended to contribute to the proper implementation of the rules laid down in this Act.

75. The Minister of Justice may lay down rules which are necessary for the implementation of decisions issued by the European Community with a view to implementation of the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, or rules which are necessary for the application of legal acts issued by the Community in the field covered by the Directive.

[…]