

REC'D JAN 02 2014

## **Registrar Data Retention Waiver Request (2013 RAA)**

Complete this form to request a waiver of one or more of the data retention requirements specified in the 2013 Registrar Accreditation Agreement (RAA). ICANN's consideration of this request is made pursuant to sections 2, 3, and 4 of the Data Retention Specification to the RAA; a waiver is not automatically granted by submitting this form.

**Registrar name:** Ascio Technologies Inc, Danmark, Filial af Ascio Technologies Inc USA  
**GURID (IANA ID):** 106

**Legal jurisdiction of registrar:** Denmark

**Jurisdiction in which legal conflict has arisen:** Denmark

**Contact person for this request:** Rob Coghill

**Email address for contact person:** rob.coghill@ascio.com

**Telephone number for contact person:** Tel: + 44 (0) 20 7015 9253

Registrar has determined in good faith that the collection and/or retention of the data element(s) specified in the Data Retention Specification to the 2013 RAA, noted below, violates applicable law based upon (check all that apply):

- ☒ a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law (the "Opinion"); and/or
- ☐ ~~a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the data collection and/or retention requirements of this Specification violates applicable law; and/or~~
- ☐ ~~a data retention waiver determination previously granted by ICANN.~~

A copy of the Opinion and governmental ruling or guidance, as applicable, must accompany this waiver request. Please also include any documentation received by your registrar from any governmental authority related to such determination and complete the fields below.

**Cite and provide a copy of the relevant applicable law:**

**Danish Act of Processing of Personal Data of 31 May 2000**

**Briefly describe the relevant applicable law in English (if the text of the law is not in English):**

**Specify the allegedly offending data collection and retention elements:**

**REGISTRATION DATA DIRECTORY SERVICE (WHOIS) SPECIFICATION relating to publication of registrant email address and telephone numbers**

**DATA RETENTION SPECIFICATION** relating to time lengths of retention of personal data specified in section 1.1.1 to 1.1.8 (inclusive) and 1.2.1 to 1.2.3 (inclusive).

If this waiver request is based on a data retention waiver determination previously granted by ICANN (i.e., same law, same jurisdiction, same data retention requirement(s)), please provide the date, registrar name, and URL of the previously posted determination and explain why the determination should also be applied to your registrar:

Not applicable

If this waiver request is not substantially based on a data retention waiver determination previously granted by ICANN (i.e., same law, same jurisdiction, same data retention requirement(s)), please explain the manner in which the collection and/or retention of such data is believed to violate applicable law, and provide a description of such determination and any other facts and circumstances related thereto:

Not applicable

Please note that prior to granting any data retention waiver, ICANN will post its preliminary determination on its website for a period of at least 30 calendar days.

Submitted by:

Signature: PP Apxull Date: 23 DECEMBER  
Print Name: ROB COGHILL Title: REG OPS PRODUCT MANAGER

This form and accompanying materials may submitted by courier or fax to:

Attention: Registrar Accreditation Notices  
Internet Corporation for Assigned Names and Numbers  
12025 Waterfront Drive, Suite 300  
Los Angeles, California 90094-2536 USA

Facsimile: + 1 310 823-8649

If you wish to submit an electronic copy, please email attachments as PDF or DOC/x files to [RAAquestions@icann.org](mailto:RAAquestions@icann.org).

E-MAIL

Ascio Technologies, Inc. Danmark,  
filial af Ascio Technologies, Inc. USA ("Ascio")  
(CVR 25 16 35 32)  
Arne Jacobsens Allé 15  
2300 Copenhagen S

Attn: Andy Southam, Group Legal Counsel

LAW FIRM

SUNDKROGSGADE 5  
DK-2100 KØBENHAVN Ø  
TEL. +45 70 12 12 11  
FAX. +45 70 12 13 11  
DIR. +45 38 77 43 96  
PKV@KROMANNREUMERT.COM

RESPONSIBLE PARTNER:  
PIA KIRSTINE VOLDMESTER

23 December 2013  
File 1026018 PKV/RSC  
DOC NO. 20013141-7

**LEGAL OPINION - THE ICANN 2013 REGISTRAR ACCREDITATION AGREEMENT**

Dear Mr Southam

We have been asked by Ascio to provide a legal opinion as to whether certain provisions in the ICANN 2013 Registrar Accreditation Agreement (the "2013 RAA"), applicable on 1 January 2014, comply with the Danish Act on Processing of Personal Data of 31 May 2000 (the "DPPD"), which implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The DPPD is under the authority of the Danish Data Protection Agency (the "DPA"); therefore, it is the DPA's duty to ensure that the DPPD is abided by. In case of citizen complaints, the DPA can make decisions on whether certain data processing is in accordance with the regulations of the DPPD. The DPA can also take up cases of its own initiative if the DPA suspects a violation of the regulations of the DPPD. The DPA issues criticism in its decisions if a data controller has violated the regulations of the DPPD.

The DPA also conducts inspections of public authorities and private companies in order to determine whether the processing of personal data is carried out in accordance with the DPPD.

If the DPA discovers punishable violations of the DPPD in connection with handling a complaint or an inspection, the DPA is authorised to issue a ban or enforcement notice with respect to the unlawful data processing (which will have the effect of ordering the unlawful activity to cease) or report the violation to the police.

Since Ascio is established in Denmark and determines the means and purposes for processing the personal data arising from its business activities collected in accordance with the 2013 RAA, Ascio's processing of personal data under the 2013 RAA will be subject to the DPPD. We understand that Ascio has contractual relationships with other corporations (resellers) based in other

countries. Whilst applicable data protection authorities in each country may be entitled to investigate and prosecute unlawful data processing, there is a strong argument that Ascio's contractual partners' data processing activities would fall under the jurisdiction of the DPPD on the basis that Denmark is the jurisdiction where the determination for the means and purposes for processing the personal data are carried out (i.e. by Ascio).

We are aware that the 2013 RAA has been subject to correspondence between ICANN and the Article 29 Data Protection Working Party (the "29WP") (see appendices 1 to 3). As you are aware, the 29WP was set up under article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy matters and it is made up of a representative from the data protection authority of each EU Member State, including a representative from the DPA. Whilst the 29WP has no force of law, it is nevertheless seen by the DPA as an authoritative advisory body for data protection and privacy matters in Denmark.

#### WHOIS publication

Pursuant to the terms of the Registration Data Directory Service (WHOIS) Specification of the 2013 RAA, a new requirement is the mandatory publication in the publicly accessible online WHOIS database of registered name holders' e-mail addresses and telephone numbers. The previous requirement for disclosure in the WHOIS database was registrant name and address. We are also aware that new registrant verification procedures will be implemented on 1 January 2014 in an attempt to "clean up" the data that is publicly available through the WHOIS database.

It is a general principle in Denmark that personal data collected and processed must be proportionate. Pursuant to section 5 (3) of the DPPD, *"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."*

Pursuant to the discussion letters between ICANN and the 29WP, namely the Negotiations Summary memo of 4 June 2012 and the 29WP's letter of 26 September 2012, it is our understanding that ICANN's main purpose for the publication of registered name holder details is law enforcement considerations.

Based on the information presented, we are of the opinion that the publication of registered name holder email and telephone numbers will conflict with the domain name holders' right to determine whether their personal data are included in a public directory and if so, which one. Further, it is our opinion that law enforcement considerations do not legitimate such publication and will therefore be regarded as excessive and will thus not be compliant with the DPPD. It would therefore be unlawful under Danish law for Ascio to publish such information on the WHOIS database and any requirement for Ascio to comply with these new requirements will place Ascio at risk of investigation by the DPA and/or potential reporting to the police.

#### Retention

It follows from section 1.1. of the Data Retention Specification of the 2013 RAA that registrars shall retain a category of personal data specified in 1.1.1. - 1.1.8. (mainly contact details at least

as regards 1.1.1 to 1.1.5 and arguably 1.1.6 save that this is for WHOIS database purposes) for a period of two years after the contract for the domain has been ended. Sections 1.1.7 and 1.1.8 are the collection and retention of "types of domain services purchased for use in connection with the registration" and "card on file" data respectively. In addition, registrars are obliged, pursuant to section 1.2 to retain all other types of data specified in 1.2.1. to 1.2.3. *"for no less than one hundred and eighty (180) days following the relevant interaction"*. This data includes "source of payment" data.

Pursuant to the discussion letters between ICANN and the WP, including the 29WP's letter of 6 June 2013 and ICANN's letter in response of 20 September 2013, it is our understanding that the above mentioned retention requirements are mainly based on law enforcement considerations.

Pursuant to section 5 (5) of the DPPD, *"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."*

With reference to the 29WP's letter of 6 June 2013 to ICANN, it is our opinion that the fact that the personal data governed by the sections referred to above can be useful for law enforcement does not legitimise the retention of these personal data for the periods specified as such retention is longer than is necessary for the purposes for which the data is processed (which is for the transaction only). Therefore, the retention requirements concerning personal data in respect of these requirements are not in compliance with the DPPD. It would therefore be unlawful under Danish law for Ascio to retain such information for the time periods specified and any requirement for Ascio to comply with these new requirements will place Ascio at risk of actions by the DPA and/or potential reporting to the police.

--o0o--

In connection with our opinion set forth above, we note that such opinion is given in respect of the DPPD in effect as at the date hereof. We undertake no responsibility to notify you of any change in Danish law or regulations after the date of this opinion although we note that Ascio may have such an obligation. We also note that the opinion set forth above is representative only, and should not be construed as constituting a comprehensive review of the violations of Danish law or regulations.

This opinion is strictly limited to the matters stated in this opinion and is not to be read as extending by implication to any other matters not specifically referred to in this opinion. It is addressed to and is solely for the benefit of Ascio in connection with Ascio's obligations under the 2013 RAA and may not be relied upon by any other person or for any other purpose, nor may it be quoted or referred to in any public document, without our written consent, except that it may be used in connection with Ascio's request for a waiver of one or more of the data retention requirements specified in the 2013 RAA.

KROMANN  
REUMERT

This opinion is governed by and construed in accordance with Danish law.

Yours sincerely

Kromann Reumert



Pia Kirstine Voldmester,  
Partner, attorney-at-law

## ARTICLE 29 Data Protection Working Party



Brussels, 26 September 2012

Dr. Steve Crocker and Mr. Akram Atallah  
Chairman and interim CEO of the Board of  
Directors

Internet Corporation for Assigned  
Names and Numbers (ICANN)  
4676 Admiralty Way, Suite 330  
Marina del Rey, CA 90292-6601

By email to the Director of Board Support:  
[diane.schroeder@icann.org](mailto:diane.schroeder@icann.org)

**Subject: Comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS data**

Dear Mr Crocker and Mr Atallah,

In the context of ICANN's revision of the Registrar Accreditation Agreement (RAA) and the **RAA Negotiations Summary Memo**<sup>1</sup>, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 WP)<sup>2</sup> wishes to respond to your call for input from data protection authorities.<sup>3</sup>

The Working Party limits this contribution to proposed changes in the RAA that will likely affect the personal data protection rights of European citizens that have registered or will register a domain name.

---

<sup>1</sup> **RAA Negotiations Summary Memo**, ICANN Proposed DRAFT 4 June 2012, URL:

<http://prague44.icann.org/meetings/prague2012/presentation-raa-negotiation-issues-04jun12-en.pdf>

<sup>2</sup> **The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data** is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents.

<sup>3</sup> *Can authorities expert in data privacy assist in proposing how ICANN and the Registrars should address the competing legal regimens into a standard that can be uniformly implemented?* **RAA Negotiations Summary Memo**, p. 5.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The Working Party recalls its previous contributions to the process of collecting and disclosing WHOIS data, as included in the Opinion 2/2003 on the application of the data protection principles to WHOIS directories<sup>4</sup> as well as its letters of 22 June 2006 to the Board of Directors of ICANN<sup>5</sup> and of 12 March 2007 to the Chairman of the Board of Directors of ICANN<sup>6</sup> in which the relevant data protection principles have been outlined.

The Working Party notes that the proposed new RAA contains two new requirements for *registrars*, the private corporations that offer internet domain names to the public and that are responsible for maintaining the contact details of domain name holders in the publicly accessible WHOIS database.

#### 1. Annual re-verification of contact details

The first issue is a new requirement for registrars to verify domain name holders' contact details via telephone and e-mail, and to annually re-verify these contact details. The proposed *Whois accuracy program specification*<sup>7</sup> makes it mandatory for registrars to obtain and verify both an e-mail address and a telephone number from all domain name holders and to annually re-verify these details, by either calling or sending an e-mail or SMS with a unique code that has to be verified by the registrant.

Accuracy of personal data is an important requirement in data protection law. However, the necessity to keep personal data accurate may not lead to an excessive collection or further processing of personal data. It is important to distinguish between contact details collected by registrars in the course of a contract, and contact details that have to be published in the WHOIS database.

The problem of inaccurate contact details in the WHOIS database cannot be solved without addressing the root of the problem: the unlimited public accessibility of private contact details in the WHOIS database. It is a fact that these contact details are being harvested on a large scale and abused for spamming. In other words, the way the system is designed provides a strong incentive for natural persons to provide inaccurate contact details. Regrettably, ICANN has decided not to work on alternative layered access models, such as the OPoC model repeatedly proposed as proportionate alternative by the Working Party.

As highlighted in previous letters to ICANN, purpose limitation/finality is crucial to determine whether the processing of personal data is compliant with the provisions of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Data Protection Directive"), as translated in the national laws of the 27 EU Member States. As you explicitly acknowledge in the Negotiations Summary, the request for annual re-verification of domain name holders data as well as the request to verify both the e-mail address as well as the telephone number, originates from law enforcement.

In assessing these proposals, ICANN should be aware that the purpose of collecting and publishing contact details in the WHOIS database is to facilitate contact about technical issues. The original purpose definition reads: "*The purpose of the gTLD Whois service is to*

---

<sup>4</sup> URL: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp76\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp76_en.pdf)

<sup>5</sup> URL: <http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf>

<sup>6</sup> URL: <http://gnso.icann.org/correspondence/schaar-to-cerf-12mar07.pdf>

<sup>7</sup> Whois accuracy program specification, ICANN Proposed DRAFT 3 June 2012, IRI- 39306v3 1, URL:

*provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver."*

In your summary of the debate about (public accessibility of) WHOIS DATA you write:  
*"Over time, WHOIS data has been increasingly used for other constructive and beneficial purposes; (...) However, some WHOIS data uses that have emerged are viewed as potentially negative;(...)." <sup>8</sup>*

The fact that WHOIS data can be used for other beneficial purposes does not in itself legitimise the collection and processing of personal data for those other purposes.

The Working Party finds the proposed new requirement to annually re-verify both the telephone number and the e-mail address and publish these contact details in the publicly accessible WHOIS database excessive and therefore unlawful. Because ICANN is not addressing the root of the problem, the proposed solution is a disproportionate infringement of the right to protection of personal data.

## 2. Data retention

The second issue is a new requirement for registrars to retain data of domain name holders for a period of two years after the contract for the domain has been ended.

The proposed Data retention specification<sup>9</sup> has a very broad scope. It is not limited to the personal data collected for the WHOIS database, but also specifies other categories of data that can be processed by registrars, such as telephone numbers and e-mail addresses not contained in the WHOIS data as well as credit card data (*means and source of payment or a transaction number provided by a third party payment processor*), communication identifiers such as a Skype handle and log files containing the source IP address and HTTP headers, dates, times, and time zones of communications and sessions, including initial registration.

This proposed new requirement does not stem from any legal requirement in Europe<sup>10</sup>, but again, is explicitly introduced by ICANN to accommodate wishes from law enforcement.

The Working Party strongly objects to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of

---

<sup>8</sup> URL: <http://www.icann.org/en/resources/policy/background/whois>

<sup>9</sup> Data retention specification, ICANN Proposed DRAFT 3 June 2012, IRI---33673v4, URL:

<http://prague44.icann.org/meetings/prague2012/presentation-data-retention-03jun12-en.pdf>

<sup>10</sup> The European data retention directive 2006/24/EC imposes data retention obligations on providers of public electronic communication networks and services. Registrars are not such providers and are therefore not

the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.<sup>11</sup>

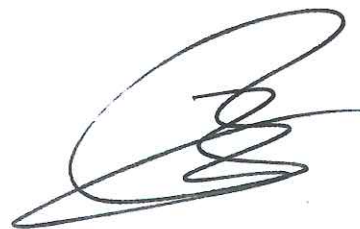
The fact that these personal data can be useful for law enforcement does not legitimise the retention of these personal data after termination of the contract. In fact, such a retention period would undermine the first new requirement, to re-verify the contact details every year. If ICANN would be able to prove the necessity for such a yearly re-verification for the purpose of facilitating technical contact with domain name holders, any data kept beyond one year would in fact be excessive, because apparently to a large extent outdated or otherwise unreliable.

Because there is no legitimate purpose, and in connection with that, no legal ground for the data processing, the proposed data retention requirement is unlawful in Europe. Since the registrars (both within Europe and worldwide to the extent they are processing personal data from EU citizens) are data controllers (responsible for the collection and processing of personal data), the Working Party is concerned that this new obligation will put them in the uncomfortable position of violating European data protection law. The Working Party would deeply regret a situation where data protection authorities were to be forced to enforce compliance and urges you to rethink the proposals.

The Working Party has on several occasions expressed an interest in being consulted by ICANN about privacy-related WHOIS issues.<sup>12</sup> We repeat that we are ready to discuss any issue that ICANN feels would be useful in relation to the application of EU and national data protection legislation in respect of WHOIS services and would appreciate it if the relevant ICANN staff would contact the Working Party to ensure that ICANN has a full understanding of the concerns we have expressed.

Yours sincerely,

On behalf of the Article 29 Working Party,

A handwritten signature in black ink, appearing to be 'Jacob Kohnstamm', written in a cursive style.

Jacob Kohnstamm  
Chairman of the Article 29

---

<sup>11</sup> Obligations with regard to the protection of personal data also follow from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the UN Guidelines concerning computerized personal data files (1990).

<sup>12</sup> See also the letter from the WP29 Chairman of 24 October 2007, URL:

Working Party

## ARTICLE 29 Data Protection Working Party



Brussels, 06 June 2013

Dr. Steve Crocker and Mr. Fadi Chehadé  
Chairman and CEO of the Board of Directors  
Internet Corporation for Assigned  
Names and Numbers (ICANN)  
4676 Admiralty Way, Suite 330  
Marina del Rey, CA 90292-6601

By email to the Director of Board Support:  
[diane.schroeder@icann.org](mailto:diane.schroeder@icann.org)

**Subject: Statement on the data protection impact of the revision of the ICANN RAA**

Dear Mr Crocker and Mr Chehadé,

In the context of ICANN's revision of the Registrar Accreditation Agreement (RAA) and the final **RAA Proposal**<sup>1</sup>, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 WP)<sup>2</sup> wishes to provide a harmonised statement concerning compliance with European data protection law.

Following up on our letter of 27 September 2012<sup>3</sup> and previous contributions to the process of collecting and disclosing WHOIS data<sup>4</sup>, this statement specifically addresses the legitimacy of the data retention obligation for registrars, contained in the new RAA.

The Working Party notes that ICANN has included a procedure for registrars to request a waiver from these requirements if necessary to avoid a violation of applicable data protection law. Such a waiver request can be based on written guidance from a governmental body of

<sup>1</sup> ICANN Proposed Final 2013 RAA of 22 April 2013, URL: <http://www.icann.org/en/news/public-comment/proposed-raa-22apr13-en.htm>

<sup>2</sup> The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents.

<sup>3</sup> Article 29 Working Party letter to ICANN, 26 September 2012, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926\\_letter\\_to\\_icann\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf)

<sup>4</sup> URLs: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp76\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp76_en.pdf), <http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf> and <http://gnso.icann.org/correspondence/schaar-to-cerf-12mar07.pdf>

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

competent jurisdiction providing that compliance with the data retention requirements violates applicable law.

In order to avoid unnecessary duplication of work by 27 national data protection authorities in Europe, with this letter, the Working Party wishes to provide a single statement for all relevant registrars targeting individual domain name holders in Europe.

The final proposed Data Retention specification roughly distinguishes between name and contact details for the domain name holder (specified in 1.1.1 to 1.1.7) and all other types of data a registrar might collect (specified in 1.2.1 to 1.2.3), such as logfiles and billing records containing the 'means and source of payment', logfiles about the communication with the registrar including source IP address, telephone number, e-mail address, Skype handle or instant messaging identifier, as well as the date, time and time zones of communications.

Registrars are required to keep the first category of personal data for a period of two years after the contract for the domain has been ended. The second category of personal data must be retained for six months after the contract has ended.

The first category of data includes payment data, defined as: *'card on file', current period third party transaction number, or other recurring payment data.*

The proposed new data retention requirement does not stem from any legal requirement in Europe.<sup>5</sup> It entails the extended processing of personal data such as credit card and communication data by a very large number of registrars. The fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of the contract. Taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data.

Secondly, the Working Party reiterates its strong objection to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.<sup>6</sup>

The fact that these personal data can be useful for law enforcement does not legitimise the retention of these personal data after termination of the contract. Because there is no legal ground for the data processing, the proposed data retention requirement violates data protection law in Europe.

---

<sup>5</sup> The European data retention directive 2006/24/EC imposes data retention obligations on providers of public electronic communication networks and services. Registrars are not such providers and are therefore not subjected to this European data retention obligation.

<sup>6</sup> Obligations with regard to the protection of personal data also follow from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the UN Guidelines concerning

In general, we repeat that the problem of inaccurate contact details in the WHOIS database cannot be solved without addressing the root of the problem: the unlimited public accessibility of private contact details in the WHOIS database. In that light, the Working Party welcomes the growing number of registries in Europe that are offering layered access to the WHOIS data.

Yours sincerely,

On behalf of the Article 29 Working Party,

A handwritten signature in black ink, consisting of a large, sweeping loop followed by several smaller, more intricate strokes.

Jacob Kohnstamm  
Chairman



The Internet Corporation for Assigned Names and Numbers

20 September 2013

Mr. Jacob Kohnstamm  
Chairman, Article 29 Data Protection Working Party  
European Commission  
JUST-ARTICLE29WP-SEC@ec.europa.eu

**Subject: Statement on the data protection impact of the revision of the ICANN RAA**

Dear Chairman Kohnstamm,

Thank you for your letter of 6 June 2013 regarding ICANN's Registrar Accreditation Agreement (RAA). We appreciate your input, on the provisions of the RAA affecting the processing of personal information.

We also appreciate your observations regarding the need to ensure that any retention of personal data beyond the term of the contract must be proportionate to the legitimate aim pursued

As you may be aware, the ICANN Board approved the 2013 RAA on 27 June 2013. The new 2013 RAA, adopted after a long period of negotiations, includes such improvements as:

- Establishment of a registrar point-of-contact for reporting abuse.
- Verification and validation of WHOIS (domain registrant) data.
- Clear establishment of registrar responsibility for reseller compliance.
- Enhanced compliance tools that include broader suspension and termination tools, clarification of audit rights, access to information to facilitate ongoing investigations and annual certification requirements.

The 2013 RAA, which was supported by the Governmental Advisory Committee (GAC)<sup>1</sup> in its Beijing Communiqué and is based in part on the 2009 GAC Endorsed Law Enforcement Recommendations, also includes additional and changed obligations for retention of data related to domain name registrations. While the 2009 RAA required registrars to keep many

---

<sup>1</sup> The GAC is the mechanism through which governments of the world provide advice to the ICANN Board on matters of public policy. There are currently over 130 member states or territories of the GAC, including the European Commission as well as many European countries.



points of data for three years past the life of the registration, the 2013 RAA actually reduces this retention requirement and creates a dual-tiered system.

Some items of data are required to be retained for only two years past the life of registration (items 1.1.1 – 1.1.8). For those items of data that are more likely to invoke data privacy concerns (items 1.2.1 – 1.2.3), registrars are only obligated to retain those items for six months after the time of relevant transaction. This two-tiered retention cycle was formulated with Registrars in recognition of some of the data retention and privacy concerns that are raised within your letter. For clarification, the six-month time period is not measured from the end of the registration, but rather from the relevant transaction.<sup>2</sup>

It is important to note that the nature and genesis of the data retention obligations. The obligation to maintain billing information is a long-standing obligation in the RAA. It serves legitimate purposes beyond those recently identified by the law enforcement community, such as helping registrants resolve problems related to their domain name accounts with Registrars. For example, ICANN has referred to billing information for consumer protection purposes, such as in situations where a registrar has failed to protect the interests of the registrants. Although the law enforcement community representatives requested RAA amendments during the recently concluded negotiations, the 2013 RAA does not create a new mechanism by which law enforcement personnel can access billing information. Instead, law enforcement is still required to follow applicable law and process (such as seeking a subpoena, if appropriate) if it wishes to access this information.

ICANN fully understands the need to respect applicable data protection laws. Even with the careful crafting of retention schedules, both ICANN and the Registrars recognize that the variety of data protection schemes around the world, as well as privacy and data retention laws, may require affording registrars the opportunity to deviate from the standard retention schedule set forth in the RAA. As a result, ICANN has identified the need to revise the ICANN Procedure for Handling Whois Conflicts with Privacy Law (at <http://www.icann.org/en/resources/registrars/whois-privacy-conflicts-procedure-17jan08-en.htm>) to more broadly handle issues including data retention. In addition, the Procedure will have to be modified to allow for ICANN's contracted parties, including Registrars under the 2013 RAA, to invoke the procedure without having proceedings initiated against them.

Until those revisions are made, there is a waiver procedure available through the data protection specification to the 2013 RAA. We understand that your letter is part of an effort to assist Registrars in invoking the interim waiver procedure. ICANN will shortly be releasing

---

<sup>2</sup> For example, if a registration was created on 1 June 2013, the means and source of payment information and log files for that 1 June 2013 transaction must only be retained for six months, regardless of the length of the registration.



Chairman Jacob Kohnstamm  
20 September 2013  
Page 3

documentation regarding the specific requirements for invoking the waiver procedure, which will include requirements for identification of the specific laws or regulations upon which the waiver request is based. ICANN will require Registrars to follow the requirements for invocation of the waiver process prior to consideration of any requests. ICANN will consider all relevant documentation, including any further documentation provided by the Article 29 Data Protection Working Party, as part of its evaluation of waiver requests.

Thank you for continuing to engage in the ICANN community dialogue regarding data protection and privacy concerns. We recognize your important role in the European Union.

With such a continued dialogue in mind we suggest that a discussion, on the RAA 2013 and related matters, might be useful. The Article 29 Working Party may be aware that ICANN has initiated work to identify a replacement system to the Whois system, and is therefore interested in dialoguing with interested parties. Nigel Hickson, our European Vice President, based in Brussels, would be more than happy to initiate this discussion. He can be contacted on [nigel.hickson@icann.org](mailto:nigel.hickson@icann.org).

Best regards,

A handwritten signature in blue ink, consisting of several loops and a long horizontal stroke extending to the right.

John O. Jeffrey  
General Counsel and Secretary



[Forside](#) / [In 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](#)

Opdateret: 04.01.13

## **Compiled version of the Act on Processing of Personal Data**

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.

# **The Act on Processing of Personal Data**

## **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., cf. 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., cf. 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.

(2) This Act shall not apply where this will be in violation of the freedom of information and expression, cf. 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. 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, cf. 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, cf. 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, cf. 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, cf. 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 dstraint, 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, cf. 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, cf. 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, cf. 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, cf. 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), cf. 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), cf. 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), cf. 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), cf. 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, cf. 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 Minister 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.

76. - (1) This Act shall come into operation on 1 July 2000.

(2) The Public Authorities' Registers Act, cf. Consolidation Act No. 654 of 20 September 1991, and the Private Registers, etc. Act, cf. Consolidation Act No. 622 of 2 October 1987 are hereby abolished.

(3) The members of the Register Council shall step in as members of the Data Protection Council until the Minister of Justice has appointed the members of the Data Protection Council.

(4) Order No. 160 of 20 April 1979 on the rules of procedure of the Register Council, etc. shall apply to the activities of the Data Protection Agency until they are abolished or replaced by rules issued by virtue of this Act.

(5) Decree No. 73 of 5 March 1979 which provides that regulations for registers, etc. drawn up by virtue of the Public Authorities' Registers Act shall not be published in the Law Gazette is hereby abolished.

(6) Complaints or control cases filed before 24 October 1998 shall be dealt with in accordance with the rules applying until now. The Data Protection Agency shall exercise the powers vested in the Data Surveillance Authority under these rules.

(7) The Data Protection Agency shall otherwise perform the tasks which are according to the legislation performed by the Data Surveillance Authority.

77. - (1) As regards processing operations carried out on behalf of private individuals or bodies and which were commenced before 24 October 1998, the rules laid down in Chapter 13 must be implemented by 1 October 2000 at the latest.

(2) As regards processing operations carried out on behalf of public authorities and which were commenced before 24 October 1998, the rules laid down in Chapters 12 and 14 must be implemented by 1 April 2001 at the latest.

(3) Processing operations commenced before 24 October 1998 may continue without authorization for 16 weeks after the coming into operation of this Act if authorization is required under the rules laid down in Title II or the provision laid down in subsection (7).

(4) Processing operations commenced on 24 October 1998 or later, but before the coming into operation of this Act, may continue without prior notification, opinion or authorization for 16 weeks after the coming into operation of this Act.

(5) Notification according to the provision laid down in section 53 shall take place within 16 weeks after the coming into operation of this Act.

(6) The Minister of Justice may lay down rules concerning prolongation of the time limit mentioned in subsections (1) and (2).

(7) The Supervisory Authority may in exceptional cases and on application decide that processing operations commenced before the coming into operation of this Act may continue, irrespective of the rules on processing laid down in Title II.

**78.** - (1) Processing operations which have been notified before the coming into operation of this Act under section 2 (3) second clause of the Private Registers, etc. Act may continue until 1 October 2001 in accordance with the rules applying until now. The Data Protection Agency shall exercise the powers vested in the Data Surveillance Authority.

(2) Processing operations as mentioned in subsection (1) shall comply with sections 5, 41 and 42 of the Act. As regards such operations, the data subject may demand rectification, erasure or blocking of data which are inaccurate or misleading or which are stored in a way which is incompatible with the legitimate purposes pursued by the controller. The Data Protection Agency shall supervise the processing under the rules laid down in Part 16 of this Act.

**79.** Consent which has been given in accordance with the rules applying until now shall apply to processing operations carried out after the coming into operation of this Act if the consent satisfies the requirements laid down in paragraph 8 of section 3 of this Act, cf. paragraph 1 of section 6, paragraph 1 of section 7 (2), section 8 (2)-(5), paragraph 2 of section 11 (2) or subsection (3) or paragraph 1 of section 27 (3).

**80.** Act No. 572 of 19 December 1985 on public administration, as amended by Act No. 276 of 13 May 1998, shall be amended as follows:

1. Section 5 (3) shall read as follows:

"(3) The competent minister may lay down rules on public access to be informed of registers as mentioned in subsection (2) which are not covered by the Act on the processing of personal data. In this connection rules on the payment of a fee may be laid down."

**81.** Act No. 430 of 1 June 1994 on information data bases operated by the mass media shall be amended as follows:

1. In section 3, subsections (1) and (3), and section 6 (1) the term "Data Surveillance Authority" shall be replaced by "Data Protection Agency".

2. The following provision shall be inserted as a new section 11 a:

"**11 a.** The necessary security measures shall be taken to prevent data in information data bases accessible by the general public from being altered by unauthorized persons."

3. Paragraph 1 of section 16 (1) shall read as follows:

"1. violates sections 4, 5, 7, 8 (1), paragraphs 2 and 3 of section 9, section 11 (1) and (3) or section 11 a."

4. Section 17 shall read as follows:

"**17** - (1) A mass media shall compensate any damage caused by a processing operation in violation of the rules laid down in this Act unless it is proven that the damage could not have been averted by the diligence and care which can reasonably be required in connection with processing of data. The general rules of the law of tort and compensation shall be applicable.

(2) The general rules of law on criminal liability shall be applicable in cases covered by this Act.

(3) Criminal liability under the rules laid down in Chapter 5 of the Penal Code may be imposed upon companies and similar bodies (legal persons)."

**82.** The Danish Land Registration Act, cf. Consolidation Act No. 622 of 15 September 1986, as amended most recently by section 2 of Act No. 1019 of 23 December 1998, shall be amended as follows:

**1.** In section 50 d (1) the term "Data Surveillance Authority" shall be replaced by "Danish Court Administration".

**2.** Section 50 d (2) and (3) shall read as follows:

"(2) The Danish Court Administration shall supervise the registers of land charges, etc. under the Act. No appeal can be brought against the decisions of the Court Administration.

(3) The Minister of Justice shall lay down more detailed rules about this supervision in consultation with the Danish Court Administration."

**83.** This Act shall not extend to the Faroe Islands, but may by Royal Decree be given effect for the processing of data by the constitutional authorities subject to any deviations following from the special conditions in the Faroe Islands. Nor shall this Act extend to Greenland, but may by Royal Decree be given effect subject to any deviations following from the special conditions in Greenland.

-----  
Act No. 280 of 25 April 2001, section 7 amending section 70 (1)-(4) of the Act on Processing of Personal Data, contains the following commencement provision:

**11.**

---

(2) Paragraphs 2 and 3 of section 1, and sections 6-8 shall come into operation on 1 July 2001.

Act No. 552 of 24 June 2005, section 6 amending section 47 (2) of the Act on Processing of Personal Data, contains the following commencement provision:

**12.**

This Act shall come into operation on 1 January 2007.

Act No. 519 of 6 June 2007, section 2 amending sections 1, 36, 62 and 70 of the Act on Processing of Personal Data and inserting Chapter 6 a on video surveillance, contains the following commencement provision:

**3.**

This Act shall come into operation on 1 July 2007.

Act No. 188 of 18 March 2009, section 1 inserting section 72 a of the Act on Processing of Personal Data, contains the following commencement provision:

**2.**

This Act shall come into operation on 1 April 2009.

Act No. 503 of 12 June 2009, section 2 amending the Act on Processing of Personal Data, contains the following commencement provision:

3.

This Act shall come into operation on 1 July 2009

Act No. 422 of 10 May 2011, section 2 amending the Act on Processing of Personal Data, contains the following commencement provision:

3.

This Act shall come into operation on 1 July 2011.

DATATILSYNET

BORGERGADE 28, 5

1300 COPENHAGEN

PHONE +45 3319 3200

FAX +45 3319 3218

E-MAIL [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)