FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions Denmark

Birgitte Kofod Olsen
Christoffer Badse
Martin Futtrup

[Copenhagen][Denmark]
February 2009

Contents

Executive Summary

[1]. Grundloven [The Danish Constitution of 1953] contains two provisions, which can be related to privacy and data protection. Section 71 provides for the inviolability of personal liberty. Section 72 states, "The dwelling shall be inviolable."

[2]. Persondataloven [The Act on Processing of Personal Data (PPD)] entered into force on 01.07. 2000 and implements Directive 95/46/EC of 24.10. 1995.

[3]. Datatilsynet [The Danish Data Protection Agency or DPA] exercises surveillance over processing of data to which the PPD act applies. The DPA mainly deals with specific cases on the basis of inquiries from public authorities or private individuals, or cases taken up by the Agency on its own initiative.

[4]. The DPA is established by the Act on Processing of Personal Data. The DPA is a public body consisting of a council and a secretariat. The secretariat consists of a president and 6 other members. The Secretariat has app. 30 employees. In 2007 the DPA received 16, 5 million DKK (app. 2, 2 million €) from public funding.

[5]. The DPA supervises public authorities and private enterprises in Denmark in relation to processing personal data. Decisions made by the DPA are final and may not be appealed by any other administrative body. They may, however, be brought before the courts.

[6]. Staff of the DPA is allowed, without a court order, to enter any premises from which processing operations carried out.

[7]. According to section 43 and 48 of PPD, public and private controllers shall notify the DPA before processing of data is carried out.

[8]. Sections 44 and 49 contains a list of exceptions to the notification duty, such as non confidential data and processing which is necessary to carry out in order to comply with provisions laid down by law or regulations. For processing carried out by the public administration the opinion of the DPA must be obtained before processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual relations, data concerning criminal offences, serious social problems or other purely private matters.

[9]. For private controllers the authorization of the DPA must be obtained before processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual relations, data concerning criminal offences, serious social problems or other purely private matters.

[10]. According to section 59 in the PPD act the DPA may order a private data controller to discontinue a processing operation which is in violation of the act and to rectify, erase or block specific data undergoing such processing.

[11]. The DPA is not able to engage in legal proceedings concerning violations of the PPD act. Criminal proceedings are subject to public prosecution. Violations can however be brought to the attention of the Prosecutors office. Section 70 of the Act on Processing of Personal Data concerns criminal liability for violation of the act.

[12]. It is possible for private persons to lodge complaints to the DPA concerning protection of rights and freedoms concerning the PPD act and regulations issued in accordance with the act, cf. section 58.

[13]. The powers given are sufficient to ensure effective data protection, since the DPA has access to relevant information, access to relevant premises concerning the processing of data and the ability to investigate compliance based on a complaint or on its own initiative.

[14]. According to section 1 the act applies to the processing of personal data wholly or partly by automatic means, and other processing of personal data which forms part or is intended to form part of a filing system. The act also applies to processing of data concerning companies if the processing is carried out on behalf of credit information agencies. The act furthermore applies to processing of personal data in connection with video surveillance. Section 2 of the act deals lists exceptions from the application of the act.

[15]. An exemption from the act is provided in section 2, subsection 5 and 11 for processing performed on behalf of Folketinget [the Danish Parliament] and its related institutions, the Danish Security Intelligence Service (PET) and the Danish Defence Intelligence Service (FE). According to chapter 17 in the Act on Processing of Personal Data the Danish Court Administration supervises processing of data carried out on behalf of Danish courts. According to section 1 subsection 4 the act doesn't apply to processing of data which is performed on behalf of the courts, the police or the prosecution in the area of criminal law criminal law.

[16]. Section 56 of The Act on Processing of Personal Data states that the DPA shall act with complete independence in executing the functions entrusted to it. Neither the Ministry of Justice nor any other public body has instructive authority over the Agency; however, the agency is attached to the Ministry of Justice regarding recruitment of staff and budgetary issues. Furthermore, the Minister of Justice appoints the members of the data council.

[17]. Section 58 of the Act on Processing of Personal Data states that the DPA shall supervise that the processing of personal data is carried out in compliance with the provisions of Act and any regulations issued in accordance with the Act. DPA also has competence to conduct unannounced inspections.

[18]. According to PPD section 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. Exceptions can be allowed under certain conditions.

[19]. The controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, or disclosure.

[20]. The DPA discover quite often breach of security concerning processing of data. The DPA lack the authority to conduct a thorough investigation on possible breach of security. The police must conduct such an investigation.

[21]. According to PPD the controller shall compensate any damage caused by the processing of data in violation of the provisions of PPD 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.

[22]. The liability is culpa with the reversed burden of proof. Section 69 in PPD does only cover economical damages. The Danish act erstatningsansvarslovens [The act on liability for damages] section 26 (1), does cover non-pecuniary damages. However, in cases on data processing this section is seldom used.

[23]. In the literature it has been pointed out that the right to compensation according to PPD section 69 does not include compensation for the loss of integrity as a result of a breach of security.

[24]. According to PPD section 69, a claim of compensation shall be brought before a court of law and not the supervising authority.

[25]. Enforcement of data protection legislation through sanctions and/or compensation payments depends largely on personal initiative of data subjects. Data subjects could be better informed and assisted by the data protection authority (legal advice, consultation, legal representation in court proceedings etc) or by NGOs in practice.

[26]. The media is generally aware of dilemmas, especially on crime prevention and solving and the invasion of private life in the public sphere, especially in the form of CCTV and video-surveillance.

[27]. In general, surveys have shown that it seems that the Danish population does not in particular worry about the issue of privacy. Surveys have shown that the Danish population has in general a fundamental trust in Government and the authorities' handling of data protection and assess that the issue of crime prevention and security is more important than the intangible and abstract notion of privacy.

[28]. The Danish Institute for Human Rights has on several occasions raised concern about the lack of interest among politicians, decision makers and citizens in relation to ensuring effective protection of data protection. Moreover, privacy issues have been raised in connection with the presentation of Bills to Parliament impacting the right to protection of data.

[29]. NGOs have pointed out in relation to Denmark that there exist comprehensive privacy law, that exempts security and defence services and that Data privacy authority is appointed by the Minister of Justice.

[30]. A main issue has been the focus on the counter-terrorism effort and especially how the Intelligence services obtain, register and store information and when there is an obligation to delete the information.

[31]. The Danish Data Protection Agency criticised the National Commissioner of Police in Denmark for an unacceptably high number of errors in reporting on personal data passed to another EU member state or a third country to the Schengen Information System, or SIS database.

1. Overview

[32]. Grundloven [The Danish Constitution of 1953][1] contains two provisions, which can be related to privacy and data protection. Section 71 provides for the inviolability of personal liberty. Section 72 states, "The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute." Section 72 also applies to all kinds of telecommunication and electronic data.

[33]. The European Convention on Human Rights[2] (ECHR) was ratified in 1953 and was formally incorporated into Danish law in 1992.[3] Denmark has on 06.01. 1972 ratified the UN International Covenant on Civil and Political Rights as well as the Optional Protocol allowing the UN Human Rights Committee to receive and consider communications from individuals.

[34]. Denmark is a member of the Council of Europe (CoE) and has, beside the ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms, also ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[4] Denmark has signed the Convention on Cybercrime on 22. 04. 2003, and ratified it on 21.06.2005. The Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems[5] was signed on 11.02. 2004, and ratified on 21.06. 2005. Denmark is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[35]. *Persondataloven* [The Act on Processing of Personal Data (PPD)] entered into force on 01.07. 2000.[6] The PPD act implements the European Union (EU) Data Protection Directive (1995/46/EC) into Danish law. It replaces *lov om private registre* [Private Registers Act of 1978], which governed the private sector,[7] and *lov om offentlige*

[1] Constitution of Denmark 1953, available at < http://www.folketinget.dk/pdf/constitution.pdf >.
[2] Convention for the Protection of Human Rights and Fundamental Freedoms
[3] Act No. 285 of April 29 1992.
[4] Signed January 28, 1981; ratified 23.10. 1989; entered into force 01.02. 1990
[5] CETS No.: 189
[6] Act No. 429 of May 31, 2000 (Persondataloven), available at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=828>
[7] Act No. 293 of June 8th 1978 (Lov om private registre mv)

myndigheders register [the Public Authorities' Registers Act of 1978], which governed the public sector.[8] The law divides personal information into three categories: ordinary, sensitive and semi-sensitive and provides different conditions for the processing of each.[9]

[36]. Other laws regulating the processing of personal information by the public sector include *Forvaltningloven* [the Public Administration Act of 1985],[10] *Lov om offentlighed i forvaltningen* [the Publicity and Freedom of Information Act of 1985],[11] *arkivloven* [the Act on Public Records of 2002],[12] *Straffeloven* [The Criminal Code of 1930][13] and *Lov om tv*-overvågning [Act on Video Surveillance][14]. These laws set out basic data protection principles and determine which data and governmental records are accessible to the public and which should be kept confidential.[15] Sector-specific laws also provide special protections for medical information[16] and credit card details[17] and lay down restrictions on direct marketing (including spam).[18] Provided that they are in accordance with Denmark's international obligations, these laws take priority over the general Data Protection Act.

[37]. *Datatilsynet* [The Danish Data Protection Agency or DPA][19] exercises surveillance over processing of data to which the PPD act applies. The DPA mainly deals with specific cases on the basis of inquiries from public authorities or private individuals, or cases taken up by the Agency on its own initiative.

[38]. *Domstolsstyrelsen*[20] [The Danish Court Administration] was established as a new independent government institution on 01.07. 1999. It attends to funding and administrative matters concerning the Danish courts. The Danish Court Administration is headed by a

[8] Act No. 294 of June 8th 1978 (Lov om offentlige myndigheders registre)
[9] Peter Blume et al., Nordic Data Protection 19-20 (DJOEF Publishing Copenhagen 2001)
[10] Act No. 571 of December 19th 1985 (Forvaltningslov)
[11] Act No. 572 of December 19th 1985 (lov om offentlighed i forvaltningen)
[12] Act No. 1050 of December 17th 2002 (Arkivlov)
[13] Act No. 1068 of November 6th 2008 (straffeloven)
[14] Act No. 1190 of October 11th 2007 (lov om tv-overvågning)
[15] Peter Blume et al., supra at 13
[16] Act No. 95 of February 7th 2008 (sundhedsloven)
[17] Act No. 259 of March 28 2008 (lov om visse betalingsmidler)
[18] Act No. 699 of July 17th 2000 (lov om markedsføring [Consolidated Act on Marketing Practices])
[19] Official website of The Danish Data Protection Agency: http://www.datatilsynet.dk/ . English version: http://www.datatilsynet.dk/eng/index.html .
[20] Official website of the Danish Court Administration: http://www.domstol.dk/om/otherlanguages/english/thedanishjudicialsystem/courtadministration/Pages/default.aspx

board of governors and a director. The Danish Court Administration comes under *Justisministeriet* [the Ministry of Justice], but the Minister of Justice has no jurisdiction over it and may not change decisions made by the Danish Court Administration.[21] According to section 67 in the PPD act, the Danish Court Administration supervises the processing of data carried out on behalf of the courts in the same manner as the DPA does in other fields.

[39]. DPA has in a memorandum of 13.09.2004 highlighted a number of privacy problems regarding the application of the Act on Processing of Personal Data vis-à-vis the application of the Act on Prohibition of TV-surveillance.

[40]. The Danish debate suggests a general trust in the public institutions, however a main issue by the media has been the focus on the counter-terrorism effort and especially how the Intelligence services obtain, register and store information and when there is an obligation to delete the information. The same issue has been in focus in relation to how long the police store DNA-profiles. The debates have been supported by relevant judgments from ECtHR, judgments raise serious questions in relation to whether the practice in Denmark is in accordance with international human rights obligations.

[41]. The DPA does seldom intervene directly in the public debates, however the agency provide information and views in regard legislative proposals and has a useful website where journalists and others can obtain information on specific issues, cases and press briefs.

[42]. The Danish Institute for Human Rights (DIHR) as well as other stakeholders comment on a regular basis on privacy issues. One example is a news telegram (dating 5-12-2008) where the DIHR's assessment was referred in relation to the ECtHR judgment S. and Marper v. U.K. (4 12-2008). A politician represented in the Parliament's Standing Committee on Legal Affairs (Retsudvalget) based a question on the analysis in telegram and asked the Minister of Justice to comment. The ministry's conclusion was identical to the DIHR and a promise to amend the Danish legislation was issued.[22] Please also refer to chapter 6. Analysis of deficiencies.

---

[21] Act No. 401 of June 26th 1998 (Lov om Domstolsstyrelsen) [Act on the Danish Court Administration], section 2, subsection 2.

[22] (Question and answer (in Danish) from the Standing Committee on Legal Affairs on December 8, 2008) Besvarelse af spørgsmål nr. 254 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 8. december 2008. Spørgsmålet er stillet efter ønske fra Karina Lorentzen (SF). Spørgsmål nr. 254 fra Folketingets Retsudvalg (Alm. del):

2. Data Protection Authority

[43]. The DPA is established by the Act on Processing of Personal Data. The DPA monitors the processing of data to which this act applies with the exception of the processing of data carried out on behalf of the courts, which is supervised by The Danish Court Administration.[23] The DPA is a public body consisting of a council and a secretariat. The secretariat consists of a president and 6 other members. The Secretariat has app. 30 employees.[24] In 2007 the DPA received 16, 5 million DKK (app. 2, 2 million €) from public funding. Furthermore, the DPA had an income of 0, 4 million DKK (app. 53.333 €) from treating notifications from private data controllers.[25] In the 2008 budget the DPA was granted additional 3 million DKK (app. 400.000 €) from public funding due to an amendment to the Act on Processing of Personal Data which expanded the possibility of video surveillance and a wish to strengthen the legal protection concerning treating personal information.[26] The DPA supervises the processing of personal data established by public authorities and private enterprises in Denmark. It ensures that the conditions for registration, disclosure and storage of data on individuals are complied with. It mainly deals with specific cases based on inquiries from public authorities or private individuals, or cases taken up by the agency on its own initiative. Decisions made by the DPA are final and may not be appealed by any other administrative body.[27] They may, however, be brought before the courts.

"Vil ministeren oplyse, hvorledes ministeren vurderer konsekvenserne for de danske regler af Menneskerettighedsdomstolens dom over Storbritannien i en sag om det britiske Dna-profilregister? Der henvises til Ritzaus telegram af den 5. december 2008: "Dansk dna-register krænker borgere".

Svar:

"[…] På denne baggrund og i lyset af Menneskerettighedsdomstolens generelle bemærkninger om adgangen til opbevaring af dna-profiler, celleprøver og fingeraftryk er det Justitsministeriets vurdering, at der bør tages skridt til at ændre reglerne om opbevaring af dna-profiler, således at disse slettes efter en nærmere angiven periode efter en frifindelse eller påtaleopgivelse. Det er endvidere Justitsministeriets vurdering, at der bør indføres nærmere regler om adgangen til opbevaring af celleprøver og fingeraftryk, herunder med tilsvarende regler om, at disse ikke kan opbevares efter en nærmere angiven periode efter en frifindelse eller påtaleopgivelse.

Justitsministeriet vil i samarbejde med bl.a. Rigspolitiet overveje den nærmere udformning af sådanne regler med henblik på at fremsætte et lovforslag herom i næste folketingssamling."

[23] Act on Processing of Personal Data, Section 55 & 67

[24] DPA Annual report 2007, p. 3. Available in Danish at: http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsrapporter/aarsrapport_2007.pdf

[25] DPA annual report 2007, p. 8

[26] DPA annual report 2008, p. 7

[27] Act on Processing of Personal Data, Section 61

[44]. **Compliance with Article 28(2) Directive 95/46/EC:** According to section 57 of the Act on Processing of Personal Data, the DPA is required to give an opinion before any new orders, circulars or similar general regulations that have an impact on privacy are issued. In the preparatory works to the act it is assumed that the opinion of the DPA is obtained when treating relevant law proposals, however this is not a requirement in the law text. The preparatory works furthermore state that a failure to request the opinion of the DPA as specified in section 57 will not cause an adopted regulation etc. to be invalid.

[45]. **Compliance with Article 28(3) Directive 95/46/EC:** Staff of the DPA is allowed, without a court order, to enter any 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. The DPA has the same access as regards processing operations carried out on behalf of private data controllers which require authorization from the DPA. The DPA may furthermore claim any information of importance to its activities.[28]

[46]. According to section 43 and 48 of the Act on Processing of Personal Data, public and private controllers shall notify the Data Protection Agency before processing of data is carried out. Sections 44 and 49 contains a list of exceptions to the notification duty, such as non-confidential data and processing which is necessary to carry out in order to comply with provisions laid down by law or regulations. For processing carried out by the public administration the opinion of the DPA must be obtained before processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual relations, data concerning criminal offences, serious social problems or other purely private matters. Opinion must furthermore be obtained when processing is carried out for the sole purpose of operating legal information systems, processing carried out solely for scientific or statistical purposes or processing which includes alignment or combination of data for control purposes.[29] For private controllers the authorization of the DPA must be obtained before processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual relations, data concerning criminal offences, serious social problems or other purely private matters.

[28] Act on Processing of Personal Data, Section 62, subsections 1,2 & 3
[29] Act on Processing of Personal Data, Section 45

Furthermore, authorization must be obtained when 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; when the processing is carried out for the purpose of forwarding data in the course of business for assessment of financial standing and creditworthiness; when the processing is carried out for the purpose of professional assistance in connection with staff recruitment; when the processing is carried out solely for the purpose of operating legal information systems, or when data is transferred to third countries.[30] It is possible for the DPA to publish opinions.[31]

[47]. According to section 59 in the PPD act the DPA may order a private data controller to discontinue a processing operation which is in violation of the act and to rectify, erase or block specific data undergoing such processing. The Data Protection Agency may furthermore ban private data controllers use of a specified procedure in connection with the processing of data if the DPA finds that there is a considerable risk that data is processed in violation of the act. The DPA can order private controllers to implement specific technical and organizational security measures to prevent illegal processing of data, accidental or unlawful destruction or alteration of data, disclosure of data to unauthorized persons, abuse of data or other unlawful forms of processing. In special cases The DPA may in special cases issue a prohibitory or mandatory injunction against data processors. This could for instance be relevant if the DPA was unable to issue an injunction against the data controller.[32]

[48]. The DPA is not able to engage in legal proceedings concerning violations of the PPD act. Criminal proceedings are subject to public prosecution. Violations can, however, be brought to the attention of the Prosecutors office. Section 70 of the Act on Processing of Personal Data concerns criminal liability for violation of the act. For instance private controllers' failure to comply with some of the DPA's decisions, requests for relevant information, conditions or prohibitory or mandatory orders are criminal offences, as well as obstruction of the DPA's access to relevant premises. For processing operations carried out on behalf of public authorities it is a criminal offence to violate conditions set by the DPA. Violation of section 70 is punishable by fine or prison up to four months.

[30] Act on Processing of Personal Data, section 50
[31] Act on Processing of Personal Data, section 65
[32] Preparatory works to the Act on Processing of Personal Data. Available in Danish at: http://www.ft.dk/doc.aspx?/search.asp?q=

[49]. Decisions by the DPA may not be treated by other Administrative Authorities.[33] The Decisions may be appealed against through the courts.[34] Furthermore, it is possible to file a complaint to the Parliamentary Ombudsman.[35]

[50]. **Compliance with Article 28(4) Directive 95/46/EC:** It is possible for private persons to lodge complaints to the DPA concerning protection of rights and freedoms concerning the PPD act and regulations issued in accordance with the act, cf. section 58. There is no specific mention of claims concerning national provisions adopted pursuant to Article 13 of Directive 95/46/EC, however, such claims will probably fall within the DPA's mandate in section 58 of the Act. The DPA is a part of the public administration and therefore subject to the general rules laid down in the Act on the Public Administration concerning administrative procedures. According to section 8 in the Act on the Public Administration parties to a case can be represented by others, including associations. A party in an administrative decision has the right to be informed of the outcome of a claim.

[51]. The powers given to the DPA correspond to the requirements of article 28 of Directive 95/46/EC. The powers given are sufficient to ensure effective data protection, since the DPA has access to relevant information, access to relevant premises concerning the processing of data and the ability to investigate compliance based on a complaint or on its own initiative (see sections below). Furthermore, non compliance with decisions and instructions given by the DPA, obstruction of access of the DPA or violation of the Act on Processing of Personal Data are in many cases considered a criminal offence.

[52]. According to section 55 of the Act on Processing of Personal Data the DPA is responsible for the supervision of all processing operations covered by the Act. According to section 1 the act applies to the processing of personal data wholly or partly by automatic means, and other processing of personal data which forms part or is intended to form part of a filing system. The act also applies to processing of data concerning companies if the processing is carried out on behalf of credit information agencies. The act furthermore applies to processing of personal data in connection with video surveillance. Section 2 of the act lists exceptions from the application of the act. According to Section 2, the act should not be applied if this is contradictory to the freedom of expression and

[33] Act on Processing of Personal Data, section 61
[34] The Danish Constitution, section 63
[35] Preparatory works to the Act on Processing of Personal Data.

information as stipulated in article 10 of the European Convention on Human Rights. Neither does the act apply to the processing of data undertaken by a natural person for purely personal activities. The act does not apply to information databases which exclusively include already published and it contains some exceptions for processing of data exclusively for journalistic purposes.

[53]. An exemption from the act is provided in section 2, subsection 5 and 11 for processing performed on behalf of Folketinget [the Danish Parliament] and its related institutions, the Danish Security Intelligence Service (PET) and the Danish Defence Intelligence Service (FE). According to chapter 17 in the Act on Processing of Personal Data, the Danish Court Administration supervises processing of data carried out on behalf of Danish courts. According to section 1 subsection 4 the act does not apply to processing of data which is performed on behalf of the courts, the police or the prosecution in the area of criminal law criminal law.

[54]. As stated above the secretariat of the DPA has app. 30 employees and receives app. 16, 5 million Danish Kroner from public funding. In 2007 the DPA conducted 66 inspections and 5430 new cases were registered concerning inquiries, complaints, law reviews etc.[36] The aim of the DPA is to treat at least 80 percent of the cases within a specified timeframe. The timeframes are for instance complaints concerning credit information agencies (max. 8 months), other complaints (max. 12 months), inquiries (max. 2 months) and law review (max. 1 month).[37]

[55]. The high number of filed complaints compared to the number of staff has as an effect that ex officio investigations and initiation of proactive measures to prevent infringements of the Act on Processing of Personal Data are not carried out at a sufficient level. Information material, i.e. pamphlets and annual reports, are made available on the webpage www.datatilsynet.dk as well as brief guidelines on e.g. use of the internet and tv-surveillance. Reports on temporary issues such as the impact of privacy enhancing technologies (PETs), RFID, biometrics, identity management and the consequences and risks of identity theft. Similarly, recommendations are not prepared and public debate or campaigns raising awareness about data protection are not initiated on these issues by the DPA.

[56]. Section 56 of The Act on Processing of Personal Data states that the DPA shall act with complete independence in executing the functions entrusted to it. Neither the Ministry of Justice nor any

[36] Data Protection Agency annual report 2007, p. 4 & 11
[37] Data Protection Agency annual report 2007, p. 24

other public body has instructive authority over the Agency. However, the agency is attached to the Ministry of Justice regarding recruitment of staff and budgetary issues. Typically, the Director of the DPA is appointed among the staff of the Ministry and returns to a position after a period in DPA. Furthermore, the Minister of Justice appoints the members of the Data Council. The chairman of the Data Council is a Supreme Court judge. This structure is in line with Danish tradition concerning administrative control organs, but may in practice jeopardize the independence of the DPA. This is due to the personal link of the staff to a public authority, but also to the perception among some citizens and experts of the DPA as guided mainly by broader societal interest than in the protection of the individual citizen. Folketingets Ombudsmand [The Danish Parliamentary Ombudsman] has the competence to review and criticise the DPA in cases concerning private citizens. Furthermore Rigsrevisionen [the National Auditors] supervises the DPA.

[57]. As stated above the secretariat of the DPA has app. 30 employees and receives app. 16, 5 million Danish Kroner from public funding. In 2007 the DPA conducted 66 inspections and 5430 new cases were registered concerning inquiries, complaints, law reviews etc.[38] The aim of the DPA is to treat at least 80 percent of the cases within a specified timeframe. The timeframes are for instance complaints concerning credit information agencies (max. 8 months), other complaints (max. 12 months), inquiries (max. 2 months) and law review (max. 1 month).[39] The DPA express a need for additional funding, when the mandate and/or tasks of the DPA has been widened by Parliament..

[58]. The DPA may start inspections or cases on its own initiative, if it finds it necessary. It also has competence to conduct unannounced inspections. As mentioned, the DPA initiated 111 cases on its own initiative and conducted 66 inspections in 2007. In practice routine inspections are usually announced some weeks in advance, since the DPA finds it essential that the relevant employees of the data controller are able to be present during the inspection. The DPA sees routine inspections not only as a control measure, but also as a chance to initiate dialogue with the data controllers. The DPA informs and provides guidance on data protection rules and the practice of the DPA. Inspections are usually based on the processing which the data controller has reported to the DPA. If however the DPA becomes aware of illegal data processing an injunction is issued immediately and if considered necessary the police is

[38] Data Protection Agency annual report 2007, p. 4 and 11
[39] Data Protection Agency annual report 2007, p. 24

notified. This monitoring role of the DPA seems efficient and fulfilling the purpose of controlling compliance and establishing a constructive dialogue.

[59]. The DPA has since 2004 published opinions and decisions which are found to be of general interest to the public. In 2007 the DPA published 16 decisions on its website, all systematized in categories that are easily understandable and accessible Decisions that are not published on the internet are available according to the Danish legislation concerning the right to access to documents issued by public authorities (offentlighedsloven).

[60]. The DPA states that the article 29-group is an independent organ and its opinions are advisory.[40] The opinions of the Article 29 group mainly serves as a source of inspiration. In connection with a question in Parliament to the DPA on the data protection impact of Facebook, and especially the question on whether the data processing on Facebook is covered by the Danish Act on Processing of Personal Data, the DPA referred directly to an investigation on the issue initiated by a working group under the Article 29 group.[41]

[61]. As mentioned above the DPA must be consulted prior to issuing of any new orders, circulars or similar general regulations that have an impact on privacy. It is not a requirement in the legal text that the DPA is consulted before adopting new legislation. However, in practice the DPA is consulted on draft legislation concerning data protection. In 2007 the DPA registered 247 opinions given to draft legislation.[42] DPA is of the opinion that only strong societal reasons should be able to justify an expansion of the access to processing of personal data, beyond the regulations in the PPD. DPA has often actively expressed concerns regarding legislation which weakens the legal protection of citizens compared the PPD act.

[62]. The DPA publishes information pamphlets on various issues relevant to its operations, news concerning initiatives, some decisions by the DPA are posted on the website of the DPA and on the website there is a general guidance to citizens, businesses and public officials concerning data protection issues. For instance in April 2008 the DPA published an information pamphlet concerning the new Danish legislation on video surveillance. The DPA's website contains a section concerning Danish and international legislation on Data Protection. In the section on the website

[40] DPA annual account to the Parliament 2007, p. 37
[41] See http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/udtalelse-til-justitsministeriet-med-svar-til-folketinget-om-facebook/?no_cache=1&cHash=82cbf73ef2
[42] DPA annual account to the Parliament 2007, p. 9

concerning guidance to citizens there is information concerning for instance citizens rights, how to complain to the DPA, TV-surveillance, marketing, etc.

3. Compliance

[63]. According to PPD section 7 (1) No processing of personal data may take place, 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:

- the data subject has given his explicit consent to the processing of such data; or

- 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

- the processing relates to data which have been made public by the data subject; or

-the processing is necessary for the establishment, exercise or defence of legal claims.

[64]. The above listing of sensitive information is exhaustive.

[65]. No data indicating lack of compliance is known.

[66]. According to PPD section 41 (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.

[67]. According to PPD section 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:

- the name and address of the controller and of his representative, if any, and of the processor, if any;

- the category of processing and its purpose;

- a general description of the processing;

- a description of the categories of data subjects and of the categories of data relating to them;

- the recipients or categories of recipients to whom the data may be disclosed;

- intended transfers of data to third countries;

- a general description of the measures taken to ensure security of processing;

- the date of the commencement of the processing;

- the date of erasure of the data.

- Data protection officers are recruited by the Ministry of Justice.

[68]. There is no evidence indicating lack of compliance in practice. However, experts have indicated that quiet often the DPA discover breach of security concerning processing of data. The DPA lack the authority to conduct a thorough investigation on possible breach of security. The police must conduct such an investigation.[43]

[69]. The agency is attached to the Ministry of Justice regarding recruitment of staff and budgetary issues. Typically, the Director of the DPA is appointed among the staff of the Ministry and returns to a position after a period in DPA. Furthermore, the Minister of Justice appoints the members of the Data Council. The chairman of the Data Council is a Supreme Court judge. This structure is in line with Danish tradition concerning administrative control organs, but may in practice jeopardize the independence of the DPA.

[43] Ugeskrift for Retsvæsen [Weekly Law Journal] UfR 2008B.327 Datasikkerhed som Menneskerettighed, P. Blume

4. Sanctions, Compensation and Legal Consequences

[70]. According to PPD Chapter 18 on Liability in damages and criminal liability, section 69, the controller shall compensate any damage caused by the processing of data in violation of the provisions of PPD, 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.

[71]. The liability is culpa with the reversed burden of proof. Section 69 in PPD does only cover economical damages. The Danish act *erstatningsansvarslovens* [The act on liability for damages] section 26 (1), does cover non-pecuniary damages. However, in cases on data processing this section is seldom used.

[72]. In legal literature it has been pointed out that the right to compensation according to PPD section 69 does not include compensation for the loss of integrity as a result of a breach of security – the compensation only covers economic damages. According to literature and the decisions of the DPA there are many breaches of the security regulation and requirements in the PPD. [44] The intention by the practice of the DPA to inform of a forthcoming routine inspection is meant to have a preventive impact as well as to create a spirit of cooperation. However, it cannot be ruled out that the notification will result in fewer cases where the DPA will find a violation of the PPD. Illegal activity will be handed over to the police who have much better powers for criminal investigation.

[73]. According to PPD section 70, unless the sanction is more serious in other legislation (e.g. the Criminal Code section 264 d) the sanction for a violation is a fine or imprisonment not exceeding four months.

[74]. According to PPD section 69, a claim of compensation shall be brought before a court of law and not the supervising authority.

[75]. As a point of departure, according to Section 312 of Retsplejeloven [Act on the Administration of Justice], the person/institution loosing a case shall, in data protection cases as in all other cases, unless agreed otherwise, compensate the other part expenses by paying the cost of legal procedures. This is decided in the final judgment by the court.

[44] Ugeskrift for Retsvæsen [Weekly Law Journal] UfR 2008B.327 Datasikkerhed som Menneskerettighed, P. Blume

[76]. Enforcement of data protection legislation through sanctions and/ or compensation payments depends largely on personal initiative of data subjects. Data subjects could be better informed and assisted by the data protection authority (legal advice, consultation, legal representation in court proceedings etc) or by NGOs in practice. However it seems that the DPA is putting more effort into awareness raising activities (please refer to chapter 5. Rights Awareness).

[77]. Trade unions are among bodies which hold personal data as the 'data controller'. Therefore trade unions have the same rights and obligations as employers when it comes to data storage. This means that trade unions are required to comply with the conditions laid out in PDA.

[78]. According to PDA section 7(1) no processing may take place of personal data revealing inter alia trade union membership. Processing is defined as obtaining, recording, holding or carrying out any operation on the data. Most things will be covered, including disclosing data to a third party.

[79]. According to PDA section 7(2)-7(8) to process personal data at least one of the conditions mentioned in these sections need to be met.

[80]. The condition most data controllers will meet is consent of the person the data is concerning.

[81]. Consent is defined in the Act as "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".

[82]. In an opinion made by the Data Protection Agency the Agency stated that The Danish Association of Managers and Executives (Ledernes Hovedorganisation) the Association may disclose data concerning its members to the third part if the data subject (member of the Association) has given his explicit consent to the processing of such data or the processing is necessary for the establishment, exercise or defence of legal claims or the processing is necessary for the controller's compliance with labour law obligations or specific rights. [45]

[83]. The case concerned the processing of data revealing trade union membership to the employers. The Danish Society of Engineers (IDA) raised a question about the distribution of a CD containing personal data concerning IDA´s 60.000 members as a new service to IDA´s members. The Data Protection Agency stated that distribution

[45] www.datatilsynet, case 2004-216-0203, (24.05. 05)

of IDA´s members list containing personal data only may happened if the member has given explicit consent to the processing of such data.[46]

[84]. Data security on trade unions websites was treated by DPA in a case raised by a trade unions member who complained about the trade unions website because the website did not maintained "log out" function. While the Agency treated the complaint the trade union introduced the "log out" function, but the Agency found it necessary to underline that this function is relevant in relation to the question concerning storage of personal data and data security.[47]

[46] www.datatilsynet, casa 2002-214-0046, (17.07 02)
[47] www.datatilsynet, case 2006-214-0143, (10.05.07)

5. Rights Awareness

[85]. The DPA has initiated informal public meetings on different themes e.g Tv-overvågning - Hvad må man? [TV-surveillance – what is allowed?] in cooperation with the Ministry of Justice.[48] Also the DPA has initiated some initiatives based on the European Data Protection Day (28th of January) e.g. published information and educational material. In cooperation with Medierådet for Børn og Unge [The Media Council for Children and Young Persons][49] and Teknologi-rådet [The Danish Board of Technology] among others the website http://www.dubestemmerselv.dk/ [you decide for yourself] has been launched in the beginning of 2009

[86]. The.media is generally aware of dilemmas, especially on crime prevention and solving and the invasion of private life in the public sphere, especially in the form of CC-TV and video-surveillance.

In general, it seems that the Danish population do not in particular worry about the issue of privacy. The Danish population has in general a fundamental trust in Government and the authorities' handling of data protection and assess that the issue of crime prevention and security is more important than the intangible and abstract notion of privacy.

[87]. However, in a recent *Synthesis Report Interview Meeting on Security Technology and Privacy* made by Privacy and Security Technology (PRISE) it is stated in the Executive Summary that Public debate is needed:

In General it was stated:

"The vast majority of the participants emphasises the need for public debate on questions about implementing new security technologies. They find it very important that new security technology is subjected to sincere

[48] http://www.datatilsynet.dk/nyheder/seneste-nyheder/artikel/tv-overvaagning-hvad-maa-man/?no_cache=1&cHash=b165d99b43 (03.02.09)
[49] http://portal.medieraadet.dk/ (03.02.09)

evaluation in an open and transparent process that also includes human rights organisations and technology experts before it is implemented. Citizens, experts and human rights organisations must be involved to some degree all the way from research to implementation."

And especially in relation to Denmark:

[88]. "The Danish report suggests a general trust in the public institutions, and compared to some of the other countries Danes only agitate for mistrust on an institutional level to a lesser extent. At the same time Denmark has not experienced a serious terrorist attack, so even though Denmark is exposed due to the cartoon crises and participation in the conflicts in Iraq and Afghanistan, the Danish participants might be more critical of the need and effect of new security technologies, very much like the Norwegian participants. However, contrary to the Norwegians, the most debated issue was that of camera surveillance which appears to be the symbol of new security technologies in the Danish debate."[50]

[89]. In a survey from 2005 on TV-surveillance by *Det Kriminalpræventive Råd* [the Council for the Prevention of Crime] it was found that "Generally the Danes are positive toward TV-surveillance. Women seem too be more concerned with criminality than men. Citizens with a higher education seem to be more concerned with the interference of privacy"[51].

[90]. Publications

Debate books have been published e.g. the book:

Overvågning eller omsorg - Privatlivets grænser by Birgitte Kofod Olsen and Rikke Frank Jørgensen published 08-09-2005. ISBN: 8761912301.

[91]. Organisations

[50] PRISE (2007) PASR Preparatory Action on the enhancement of the European industrial potential in the field of Security research - Synthesis Report Interview Meeting on Security Technology and Privacy, Anders Jacobi, The Danish Board of Technology and Mikkel Holst, The Danish Board of Technology available at: http://www.tekno.dk/pdf/projekter/prise/p07_PRISE_security_report_citizensmeeting_uk.pdf (19-01-2009) Please also consult the Danish newsletter available at: http://www.tekno.dk/pdf/nummer247.pdf (19-01-2009)

[51] TV-overvågning - Fakta om TV-overvågning i Danmark Det Kriminalpræventive Råd Februar 2005 available in Dannish at: http://www.dkr.dk/ftp_files/WEBDOX/PDF/dkr_mat_083.pdf (03.02.09)

Examples of organisations concerned with privacy issues in Denmark:

[92]. *Teknologi-rådet* (The Danish Board of Technology is an independent body established by the Danish Parliament in 1995.). The Danish Board of Technology was established in order to disseminate knowledge about technology, its possibilities and its effects on people, on society and on the environment. More information available at: http://www.tekno.dk/ (19.01. 2009)

[93]. *Digital Rights* (a NGO aimed at raising awareness of rights in the digital world) more information available at: http://www.digitalrights.dk/index.htm (19.01. 2009)

[94]. *Sikkerhedsbranchen* [The Trade Organisation for Safety and Security] more information available at: http://www.sikkerhedsbranchen.dk/ (19.01. 2009)[52]

[95]. *Institut for Menneskerettigheder* [The Danish Institute for Human Rights – the National Human Rights Institution in Denmark] more information available at: http://humanrights.dk/ and http://menneskeret.dk/ (19-01-2009).

In a report published by the organisation *Privacy International* it is stated in relation to Denmark:

[96]. Comprehensive privacy law, and exempts security and defence services, Data privacy authority is appointed by the minister of justice, and the ministry is also responsible for the budget; Data privacy authority may enter any premise without a court order to investigate under the privacy law; Extensive interception of communications; and use of bugs on computers to monitor activity and keystrokes; and plans are in place to minimise notification; Police require list of all active mobile phones near the scene of a crime; DNA samples may be required from applicants for residency based on family ties; Implemented retention of communications data well before EU mandate, for one year; Police took the DNA of 300 youth protestors in 2007. And regarding the implementing air travel surveillance program, it is stated that the Parliament is over-keen to

[52] Sikkerhedsbranchen has been critical in relation to new legislation making it easier to set up surveillance cameras up in public areas. In 2007, laws were changed so that it no longer became necessary to notify the Danish Data Protection Agency when setting up a surveillance camera.

implement surveillance programs. Furthermore, Danish decree on data retention is being heavily criticized.[53]

[97]. The Minister of Science and Research established an IT Security Commission in 2007 with the purpose of discussing and raising awareness on security and privacy on the internet and in connection with ICT systems. A stakeholder dialogue meeting was held in September 2008 and a public conference on privacy and social network services were held in November 2008.[54] A report containing conference material and recommendations is launched in February 2009.

6. Analysis of deficiencies

[98]. A main issue by the media has been the focus on the counter-terrorism effort and especially how the Intelligence services obtain, register and store information and when there is an obligation to delete the information.

[99]. The same issue has been in focus in relation to how long the police store DNA-profiles.

[100]. The debates have been supported by relevant judgments from ECtHR, judgments raise serious questions in relation to whether the practice in Denmark is in accordance with international human rights obligations, since the practice in Denmark is very similar compared too the two countries in the judgments.[55]

[101]. In principle, PPD covers all handling of personal information in the public, as well as in the private sector. Data processing by the Danish courts are covered by the PPD, while the *Folketing* [the

[53] According to *The 2007 International Privacy Ranking*, Denmark was categorized as an extensive surveillance society. The ranking is available at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597 .

[54] See http://www.it-borger.dk/sikkerhed/nyheder/fokus-pa-privatliv-pa-nettet

[55] ECtHR Case of Segerstedt-Wiberg and Others V. Sweden (Application no. 62332/00), 6-6-2006 -Continued storage (after 30 years) of information by Security Service amounted to a disproportionate interference with their right to respect for private life.
ECtHR Case of S. And Marper V. The United Kingdom (Applications nos. 30562/04 and 30566/04), 4-12-2008 - Retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, failed to strike a fair balance between the competing public and private. Accordingly, the retention constituted a disproportionate interference with the applicants' right to respect for private life and was not deemed necessary in a democratic society.

Parliament] and related institutions are exempted cf. PPD section 2 (5). Other exemptions are stipulated in section 2.

[102]. According to PPD section 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 PPD. Hence, PPD should be understood as to provide a *minimum protection* for the data subject (i.e. an identified or identifiable natural person).

[103]. According to PPD section 2(2) to section 2 (11) the complete list of exemptions is the following:

[104]. Section 2(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.

[105]. Section 2(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.

[106]. In relation to private stakeholders, not only organisations and businesses etc are covered, but also private individuals. An individual which process data of strictly private nature is exempted. Data of private nature could e.g. be list of addresses of family and relatives, an electronic private dairy or correspondence or mail with public authorities.

[107]. Section 2(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.

[108]. By the term "prosecution" is understood chief constables, Public Prosecutors and Director of Public Prosecutions and the Ministry of Justice, but not *Direktoratet for Kriminalforsorgen* [The Danish Prison and Probation Service]. The term "area of criminal law" is not well defined due to lack of case law and explanations in the legal comments, but it is assumed to at least include cases which are under investigation by the police, or cases of involving criminal liability, or the fixing of the sentence, but also activities of a more general

nature. In a case the DPA decided that a list of police informers did fall within section 2(4) of PPD.[56]

[109]. Section 2(5) This Act shall not apply to the processing of data which is performed on behalf of the Danish Parliament and its related institutions.

[110]. Data processing by political parties represented in the Parliament fall with PPD (i.e. not exempted).

[111]. Section 2(6) This Act shall not apply to the processing of data covered by the Act on information databases operated by the mass media.

[112]. Section 2(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.

[113]. This exemption applies to distributed published periodicals and picture and sound programmes by organisations which have a license to conduct radio and television activities.

[114]. Section 2(8) states that the 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.

[115]. According to Section 2(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.

[116]. According to Section 2(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.

[117]. Non-electronic processing of personal data with a journalistic aim is also covered by this section cf. section 1 (2).

[56] Denmark DPA decision 2005-3-2 (udtalelse til Rigsadvokaten).

[118]. Section 2(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.

[119]. An issue also arises since there is a tendency to share information, not only among authorities, but also among especially EU-Countries.

[120]. For obvious reasons Intelligence Services must be able to collect data in an extended manner if it relates to their core mandate. But by widening the scope and mandate of intelligence and security operations, which is the current trend – more fields fall outside the scope of the Act. This could be considered problematic in relation to the protection of privacy.

[121]. One could maybe recommend and enhanced system of control with the Intelligence Services.

[122]. Concerning the journalistic processing of data there exist conflicting interests, namely freedom of information and expression vis-à-vis the right to data protection as explicitly mentioned in PPD section 2(2) and section 2(6) to section 2(10). Because of the increased use of the internet for the distribution of all sorts of publications there exists a trend where the right to privacy will be limited due to an increased focus on the right to freedom of expression. This could lead to an increased acceptance of a violation of the personal integrity of the individual. This is the case – not only for the mass media and professional journalists, but also since more and more people publish sensitive data on weblogs and social communities. Generally, there seem to exist a need for the general l public to be more aware of dissemination of sensitive data about them selves and their friends and relatives, especially on the internet. Freedom of Expression is as a fundamental rights much more widely known, whereas privacy and the loss of it seems very abstract to many. However, when confronted with practical examples most people are well aware of the issues at stake. Rather than new legislation, it is much more an issue of mind setting, which seem to be required in the general public. Areas where amendments in legislation could be required is the area of storage of information by Security Service and retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences.

7. Good Practice

[123]. Communication from DPA on reporting to Schengen Information System

[124]. The Danish Data Protection Agency criticised the National Commissioner of Police in Denmark for an unacceptably high number of errors in reporting on personal data passed to another EU member state or a third country to the Schengen Information System, or SIS database, which provides access to reports on individuals, including immigration, public order or national security grounds. An investigation by the Danish Data Protection Agency in June 2005 found 68 errors out of a base of 443. Article 96 "alerts" on the Schengen Information System (SIS) entered by Denmark.[57] According to DPA, 11 people had incorrectly been declared "undesirable" in Denmark. The DPA concluded that *Rigspolitiet* [the National Commission of the Danish Police] had violated PPD section 5 (4).[58]

8. Miscellaneous

[125]. On 01.06.2007 an Act on TV Surveillance, which replaced the previous Act Prohibiting Video Surveillance was adopted in the Parliament (Act. no. 162 of 1 June 2007). The bill gives private enterprises such as banks, gas stations, hotels, shops etc. extended powers to perform surveillance on areas related to their property. There is no longer a duty to notify the Data Protection Agency prior to installing surveillance equipment.

[126]. On 08.06. 2006, an Act amending the Administration of Justice Act, Act Prohibiting Video Surveillance etc., and Act on Air Traffic (Strengthening of the efforts to fight terrorism etc.) was adopted in Parliament (Act No. 542 of 8 June 2006). The amendment to the Administration of Justice Act gives the Police Intelligence Service increased powers to exchange information with the Defence

[57] Please also refer to http://www.statewatch.org/news/2006/oct/eu-dp.pdf (19-01-2009)
[58] Communication from DPA Undersøgelse af indberetninger i henhold til Schengen-konventionens, Brevdato: 10.06.05: Journalnummer: 2003-851-0048 available at: http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/undersoegelse-af-indberetninger-i-henhold-til-schengen-konventionens/ (19-01-2009)

Intelligence Service and to collect information from other public authorities, e.g. hospitals, schools, libraries, social services etc. without a court order. The amendment of the Act Prohibiting Video Surveillance gives the police increased powers to demand of public offices and private parties that they install and conduct video surveillance. The amendment of the Air Traffic Act obliges airline companies to register and keep data on passengers and crews for one year and to provide the Police Intelligence Service with electronic access to the data, without a court order.[59]

[127]. The government has decided not to propose legislation concerning phone scanning. The report entitled "Danish society's initiatives against and preparedness for terror" was prepared in October 2005 by a working group with participation from a number of Ministries and the Police Intelligence Service, among others, and contained a recommendation that it be made legal for police to scan the contents of telecommunication within a defined area. The government's Action Plan on combating terror from 2005 stated that the government would decide politically on the recommendation when the Standing Committee on Administration of Criminal Justice had had the chance to deal with the question. The Standing Committee on Administration of Criminal Justice delivered its remarks on the recommendation in September 2006.Among its conclusions, the Committee finds that phone scanning amounts to a particularly serious intrusion into the secrecy of correspondence, since this measure will also entail sweeping access to communication among individuals who are not or could not be suspected of any criminal wrongdoing. The Committee found that this fact spoke in favour of underlining that substantial reasons would have to obtain before establishing a rulemaking such an encroachment possible. Furthermore, the Police Intelligence Service informed that the Standing Committee on Administration of Criminal Justice has established that phone scanning can in fact be undertaken according to existing legislation based on the principle of emergency law.

[128]. The government has subsequently decided not to propose legislation on phone scanning.[60]

[129]. Statistics detailing police intrusion into the secret of correspondence

[130]. Police statistics from 2006 show that the Courts approved police intrusion into the secrecy of correspondence in 3,477 out of 3,572 prior requests. The major part of these requests involved drug-

[59] More information available at: http://www.edri.org/edrigram/number4.14/denmark (19-01-2009) - contribution by Rikke Frank Joergensen - Digital Rights Denmark

[60] Reference: The Ministry of Justice: Press statement of 21 December 2006.

related crimes (2,369 requests, out of which 2,290were approved); 52 requests were related to cybercrime; 2,054 requests regarded phone taps; and 1,806 concerned retrieval of telecommunications records.

[131]. *UN Human Rights Committee Concluding Observations.* The Committee noted that, under the Aliens Act, article 40c, the Immigration Authorities may require DNA testing of an applicant and the persons with whom the applicant claims family ties on which a residence permit is to be based. The Committee stated that DNA testing may have important implications for the right of privacy under article 17 of the Covenant. The Committee noted that Denmark should ensure that such testing is used only when necessary and appropriate to the determination of the family tie on which a residence permit is based (art. 23).[61]

[61] CCPR/CO/70/DNK Concluding Observations 31.10 2000 on Denmark

Annexes

Annex 1 - Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	Not available	n.a.	n.a.	13,9 million DKK (1,85 mil. €)	15,4 DKK (2,05 €)	14,7 DKK (1,96 €)	16,1 DKK (2,15 €)	15,4 DKK (2,05 €)
Staff of data protection authority	30	37	31	33	31	31	29	33
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	96	112	202	114	110	112	95	113

Number of inspections initiated by data protection authority at own initiative	23	76	116	71	68	61	63	66
Number of data protection registrations	1395	7081	3711	1970	2616	2740	2599	3668
Number of data protection approval procedures	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Number of inquiries and complaints received by data protection authority	509	1029	785	910	965	1100	1076	1022
Number of complaints upheld by data protection authority	App. 45	App. 186	App. 56	App. 78	App. 59	App. 82	App. 123	n.a.
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.

Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	U.2008.727/2S
Decision date	06.12. 2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	U.2008.727/2S, *Sø- og Handelsretten* [Copenhagen Maritime and Commercial Court]
Key facts of the case (max. 500 chars)	The store employee CL was subject to video-surveillance by his employer from the private residence of the employer for app. a half hour to forty five minutes. The surveillance was not motivated by work or safety reasons.
Main reasoning/argumentation (max. 500 chars)	The surveillance led to a collection of information (images) of CL for other purposes than CL was aware of. It was therefore in breach of the PPD act section 5 subsection 1 and 2 concerning good information practices which specifies that the collection of information must be for specified, explicit and legitimate purposes.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Compensation for moral damages 25.000 DKK (app. 3.333,33 €)
Proposal of key words for data base	Illegal video surveillance of employees

Case title	U.2007.334Ø
Decision date	30. 10. 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	U.2007.334Ø, Østre Landsret [Eastern High Court of Denmark]
Key facts of the case (max. 500 chars)	A company had on a website concerning compulsory sales posted an a sales presentation in which the social security number of two persons was visible in several places for a period of 7 days. The social security numbers are likely to have been available at the land registry's office since mortgage letters with social security numbers were registered.
Main reasoning/argumentation (max. 500 chars)	It is however considered a publication within the meaning of the PPD act that the social security numbers on the site were made available to anyone with internet access. It can not be regarded as an explicit consent to the publication that they have signed mortgages, which they knew would be registered and there is therefore a violation of the PPD Act, Section 11,subsection 3. The defendant company is criminally responsible.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The company was sentenced a fine of 3,000 DKK (app. 400 €) according to the PPD act, section 70, subsection 5, no. 1, cf. Section 11, subsection 3.
Proposal of key words for data base	Illegal publishing of social security numbers

Case title	Concerning Ministry of Employment memo on legal aspects of the collection of information for control of the disbursement of cash, etc.
Decision date	16..08. 2006

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Opinion from the Danish Data Protection Agency, case no: 2006-329-0024
Key facts of the case (max. 500 chars)	In connection with the evacuation of Danish citizens from Lebanon during the hostilities in July 2006, the Ministry of Foreign Affairs and the Ministry of Employment enquired with the Data Protection Agency concerning the possibilities of releasing data on Danes evacuated from Lebanon to other authorities in order to check certain issues.
Main reasoning/argumentation (max. 500 chars)	Concerning cash social benefits, the DPA found that only municipalities have authority to collate data from registers in order to check information about financial issues. There is no statutory authority for a general, cross-referential collation in order to check information concerning other issues, e.g. information about travels abroad. In relation to unemployment benefits, the DPA found that the relevant provision in the Unemployment Insurance act allows cross referential collation of information from another public authority, e.g. concerning individual travel in order to perform a general investigation as to whether the benefits have been rightly disbursed.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	DPA had no objections to the Ministry of Foreign Affairs attesting to other public authorities whether a certain individual had been evacuated; under the condition that the requesting authority can prove that it has the authority to perform such checks of individuals. The DPA adds that since the inquiry from the ministry is of a general character the opinion of the DPA is only guiding. The DPA will make a binding decision if a specific case is brought up.
Proposal of key words for data base	Release of data concerning Danish citizens evacuated from Lebanon.

Case title	U.2006.1474H
Decision date	10.02 2006

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	U.2006.1474H, *Højesteret* [Supreme Court judgment]
Key facts of the case (max. 500 chars)	A large number of copyrighted musical works were made available from two Internet servers. The owners of the servers, A, were subscribers of the network operator T. The owners of the musical works, R, had not given permission to make the works accessible, and they were not aware of A's identity. R asked the court to prohibit T to transmit copyrighted works for which R has exclusive rights. T argued, inter alia, that they had no knowledge or understanding of the content of the information that was communicated to and from the servers via the Internet and that they did not control the content.
Main reasoning/argumentation (max. 500 chars)	
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Supreme Court found that A had performed extensive violations of copyrights without permission, by making copyrighted works available to the public on the servers. T's transmission of works entailed temporary reproduction, and when this production was not done on the basis of a legal source, the transmission meant that T violated copyrights and violated R's rights.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	T was prohibited from transmitting copyrighted works to which R had exclusive rights.
Proposal of key words for data base	

Case title	Examination of reports under the Schengen Convention
Decision date	10.06. 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Case no. 2003-851-0048 The Danish Data Protection Agency

Key facts of the case (max. 500 chars)	
Main reasoning/argumentation (max. 500 chars)	The Schengen Joint Supervisory Authorityhas launched an investigation into reports to the Schengen Information System (SIS) under the Schengen Convention art. 96 of undesirable aliens. In this connection, the Schengen Joint Supervisory Authority requested The DPA to examine whether the Danish alerts on unwanted aliens in accordance with the Schengen Convention, Article 96 has been in compliance with the Convention. In this respect, the DPA requested the Danish National Police to submit evidence to the reports made by the Danish side in accordance with Article 96 of 1 quarter of 2004.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The DPA criticised the National Commissioner of Police in Denmark for an unacceptably high number of errors in reporting on personal data passed to another EU member state or a third country to the Schengen Information System, or SIS database, which provide access to reports on individuals, including immigration, public order or national security grounds. An investigation by the DPA in June 2005 found 68 errors out of a base of 443 Article 96 "alerts" on the Schengen Information System (SIS) entered by Denmark. According to DPA, 11 people had incorrectly been declared “undesirable” in Denmark.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The DPA concluded that *Rigspolitiet* [the National Commission of the Danish Police] had violated PPD section 5 (4).
Proposal of key words for data base	Schengen

Case title	U.2005.1639V
Decision date	23.02. 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	U.2005.1639V , *Vestre Landsret* [Western High Court of Denmark]
Key facts of the case (max. 500 chars)	A, who was employed by B, was in April 2002 announced a warning because of his woeking performance. In connection with a colleague C's dismissal in September 2002 A and C exchanged some e-mails on B's computer facilities, and in one of them A spoke ill of B's Finance director D. After B had been aware of these mails B dismissed A.

Main reasoning/argumentation (max. 500 chars)	It was not proven that A's working performance was dissatisfying. The mail was sent in a private correspondence with C, and A had reason to believe that it would not be read by others. Therefore and because of the less serious nature of the content termination of A could not be justified. A was entitled to compensation. It was found that B by chance became aware of the e-mail correspondence, and it was not possible to establish that the e-mail was private without reading the correspondence. There was therefore no violation from B's hand, which could lead to a claim for compensation.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Damages for wrongful dismissal, 81.715,69 DKK (app. 10895 €). Since A had not suffered any financial loss by B's reading of the correspondence, there was no basis for damages under the PPD, Section 69.
Proposal of key words for data base	

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Data Protection Agency

Case: No. 2003-851-0048

Available at:

: http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/undersoegelse-af-indberetninger-i-henhold-til-schengen-konventionens/ (10-03-2009)

Undersøgelse af indberetninger i henhold til Schengen-konventionens

Brevdato: 10.06.05

Journalnummer: 2003-851-0048

Den Fælles Tilsynsmyndighed Schengen har iværksat en undersøgelse af indberetninger til Schengen-informationssystemet (SIS) efter Schengenkonventionens art. 96 af uønskede udlændinge. I den forbindelse har Den Fælles Tilsynsmyndighed anmodet Datatilsynet om at undersøge, hvorvidt danske indberetninger vedrørende uønskede udlændinge, jf. Schengen-konventionens artikel 96, er sket i overensstemmelse med konventionen.

Baggrunden for Den Fælles Tilsynsmyndigheds initiativ er bl.a., at der kan konstateres store forskelle på antallet af indberetninger medlemslandene imellem. Eksempelvis havde Italien pr. 1. februar 2003 foretaget 335.306 indberetninger i SIS, Tyskland 267.884 indberetninger, Holland 9.363 indberetninger og Sverige 4.454 indberetninger.

I den anledning anmodede Datatilsynet ved brev af 21. september 2004 Rigspolitiet om at fremsende dokumentation for de indberetninger, der var sket fra dansk side i henhold til artikel 96 i 1. kvartal i 2004.

Ved brev af 28. oktober 2004 fremsendte Rigspolitiet det ønskede materiale.

Det fremgik heraf, at der i 1. kvartal 2004 i en række tilfælde fejlagtigt var sket indberetning til SIS.

På denne baggrund anmodede Datatilsynet ved brev af 17. december 2004 Rigspolitichefen om at gennemgå samtlige de indberetninger, der er sket fra dansk side i henhold til artikel 96, for at sikre, at der ikke i andre tilfælde fejlagtigt er sket registrering i SIS. Datatilsynet anmodede endvidere Rigspolitichefen om at oplyse, om de konstaterede fejl vedrørende indberetninger foretaget i 1. kvartal 2004 havde givet anledning til ændrede sagsgange, kontrolprocedurer eller lignende.

Ved brev af 3. maj 2005 er Rigspolitiet fremkommet med en udtalelse. Det fremgår heraf, at Rigspolitiet har gennemgået samtlige 443 sager, hvor udlændinge er blevet opdateret i SIS som uønskede, jf. udlændingelovens § 58 g.

Gennemgangen har omfattet de domme/administrative afgørelser, der ligger til grund for indberetningerne, registreringerne i Det Centrale Kriminalregister og SIS samt forkyndelsen for udlændingene af indberetningen til SIS.

Rigspolitiet har i forbindelse med gennemgangen af sagerne konstateret følgende:

- I 22 tilfælde er der fejlagtigt sket indberetning til SIS. Sagerne vedrører primært EU-statsborgere eller udlændinge, der er dømt for strafbare forhold, der ikke opfylder betingelserne i udlændingelovens § 58 g for indberetning i forhold til den pådømte lovovertrædelse eller straffens længde.
- I 17 tilfælde er der korrekt sket indberetning til SIS, men i forbindelse med opdateringen i SIS og Det Centrale Kriminalregister er der sket tastefejl, eller indberetningerne har ikke været fuldstændige i forhold til de obligatoriske felter, der skal udfyldes i SIS.
- I 7 tilfælde er der korrekt sket indberetning til SIS, men det har efterfølgende vist sig, at de pågældende var kendte under falsk navn, og dette er ikke blevet berigtiget i SIS, da man blev bekendt hermed, eller de pågældende er blevet indberettet under 2 identiteter.
- I 11 tilfælde er der korrekt sket indberetning til SIS, men der er fejlagtigt ikke taget skridt til, at Udlændingestyrelsen kan foretage konsultation i medfør af Schengen-konventionens artikel 25.
- Gennemgangen af de domme, der ligger til grund for indberetningerne til SIS, har endvidere vist, at dommene i 11 tilfælde er forkerte i forhold til udvisningsspørgsmålet. I 3 af de pågældende tilfælde er der – i overensstemmelse med indholdet af de afsagte domme – sket indberetning til SIS, men dommene har vist sig at være afsagt forkert i forhold til udvisningsspørgsmålet, og indberetningerne til SIS har som følge heraf ikke været korrekte. I 8 af de pågældende tilfælde har indberetning til SIS fundet sted i overensstemmelse med domfældelsen i forhold til det strafbare forhold i de afsagte domme, men henvisningerne til udlændingelovens udvisningsbestemmelser i dommene har været fejlagtige, således at dommene burde have været foranlediget berigtiget, førend indberetning til SIS fandt sted.

- I et mindre antal sager, hvor der er sket korrekt indberetning til SIS, har det vist sig, at forkyndelsen for udlændingen af indberetningen til SIS ikke har fundet sted i overensstemmelse med Rigspolitiets interne retningslinjer herom.

Rigspolitiet har oplyst, at man har taget de fornødne skridt til at rette de konstaterede fejl. Det er desuden oplyst, at de interne retningslinjer i Rigspolitiets Udlændingeafdeling vedrørende sagsgange og kontrolprocedurer i forbindelse med behandling af sager om indberetning i medfør af Schengen-konventionens artikel 96 vil blive præciseret.

Endvidere har Rigspolitiet anmodet Rigsadvokaten om at indskærpe over for politikredsene, at anklagemyndigheden i sager, hvor udvisning kan komme på tale, dels nedlægger en korrekt udvisningspåstand, dels ved modtagelse af afsagte domme nøje gennemgår disse, herunder henvisningen til udlændingelovens udvisningsbestemmelser, med henblik på at sikre, at dommenes afgørelse om udvisning er korrekt i forhold til det pådømte forhold, og om nødvendigt tage skridt til berigtigelse heraf.

I den anledning skal Datatilsynet – efter at sagen har været behandlet i Dataրådet – udtale følgende:

1. I henhold til § 2, stk. 1, i lov om Danmarks tiltrædelse af Schengenkonventionen gælder bestemmelserne i Schengen-konventionens afsnit IV (Schengen-informationssystemet) her i landet. Afsnit IV i konventionen omfatter artiklerne 92-119 og vedrører Schengen-informationssystemet.

Af § 2, stk. 2, i tiltrædelsesloven fremgår, at Rigspolitichefen er den centrale myndighed, der efter konventionens artikel 108, stk. 1, er ansvarlig for den nationale del af SIS.

Rigspolitiet er tillige dataansvarlig i forhold til persondatalovens regler og har i overensstemmelse med persondataloven anmeldt den nationale del af Schengen-informationssystemet til Datatilsynet.

Datatilsynet er tilsynsmyndighed i forhold til persondataloven og er desuden ifølge tiltrædelseslovens § 2, stk. 2, tilsynsmyndighed efter Schengenkonventionens artikel 114 og 128.

Datatilsynet påser ifølge persondatalovens § 58, stk. 1, af egen drift eller efter klage fra en registreret, at behandlingen finder sted i overensstemmelse med loven og regler udstedt i medfør af loven. Tilsynet kan efter lovens § 62 kræve enhver oplysning, der er af betydning for dets virksomhed.

Efter Schengen-konventionens artikel 114 fører Datatilsynet tilsyn med databasen i den nationale del af SIS og kontrollerer, at behandlingen og anvendelsen af de oplysninger, der er optaget i SIS, ikke krænker de berørte personers rettigheder. Til dette formål skal Datatilsynet have adgang til databasen i den nationale del af SIS.

Datatilsynet kontrollerede på baggrund af Den Fælles Tilsynsmyndigheds initiativ et udsnit af de danske indberetninger, nemlig de 20 indberetninger der var foretaget i 1. kvartal 2004.

Da dette udsnit viste, at der i en række tilfælde fejlagtigt var sket indberetning til SIS, anmodede Datatilsynet Rigspolitiet om at gennemgå samtlige de indberetninger, der er sket fra dansk side.

Rigspolitichefen har som ønsket af Datatilsynet gennemgået de nævnte sager. Datatilsynet har i den forbindelse noteret sig, at gennemgangen har omfattet såvel de domme/administrative afgørelser, der ligger til grund for indberetningerne, som registreringerne i Det Centrale Kriminalregister og SIS samt forkyndelserne for udlændingene af indberetningen til SIS.

Det er på denne baggrund Datatilsynets opfattelse, at Rigspolitiets redegørelse er egnet til at danne grundlag for tilsynets bedømmelse af de skete indberetninger.

2. Oplysninger om uønskede udlændinge, der nægtes indrejse, optages ifølge Schengen-konventions artikel 96 i SIS på grundlag af nationale indberetninger.

I Danmark findes kriterierne for indberetning af uønskede udlændinge i udlændingelovens § 58 g, og indberetningerne foretages af Rigspolitiet.

Ifølge udlændingelovens § 58 g indberetter Rigspolitichefen en udlænding, der ikke er statsborger i et Schengenland eller et land, der er tilsluttet Den Europæiske Union, som uønsket til Schengeninformationssystemet, hvis

1. udlændingen er udvist af landet i medfør af § 22, § 23 eller § 24, nr. 1,
2. udlændingen er udvist af landet i medfør af § 24, nr. 2, og den pågældende er idømt ubetinget straf af mindst 1 års fængsel eller anden strafferetlig retsfølge, der indebærer eller giver mulighed for frihedsberøvelse, for en lovovertrædelse, der ville have medført en straf af denne varighed,
3. udlændingen er udvist af landet i medfør af § 25,
4. udlændingen er meddelt afslag på opholdstilladelse efter § 10, stk. 1 eller 2, nr. 1 eller 2,
5. udlændingens opholdstilladelse er inddraget i medfør af § 19, stk. 2, nr. 2 eller 3, eller
6. udlændingen har fået udstedt visum efter § 4 eller § 4 a og er udvist af landet i medfør af § 25 b efter at have fået afslag på en ansøgning om opholdstilladelse efter § 7.

Det følger af udlændingelovens § 58 h, stk. 1, at Udlændingestyrelsen forestår konsultationer med myndighederne i et andet Schengen-land i medfør af Schengen-konventionens artikel 25.

Hvis Udlændingestyrelsen efter de i § 58 h, stk. 1, nævnte konsultationer finder, at en i medfør af § 58 g indberettet udlænding bør slettes som uønsket i Schengen-informationssystemet, sletter Rigspolitichefen ifølge § 58 h, stk. 2, den pågældende i Schengen-informationssystemet.

Det følger af Schengen-konventions artikel 105, at den indberettende kontraherende part har ansvaret for, at de oplysninger, der optages i Schengeninformationssystemet, er korrekte og aktuelle, samt at de er lovligt indberettet.

3. Datatilsynet må konstatere, at såvel den undersøgelse, der stikprøvemæssigt blev foretaget vedrørende 1. kvartal 2004, som den efterfølgende gennemgang af samtlige indberetninger, har vist, at der på en række punkter er sket fejl i de danske indberetninger til SIS.

Datatilsynet må således konstatere, at Rigspolitiet i et antal tilfælde har foretaget indberetning til SIS, uden at betingelserne i udlændingelovens § 58 g er opfyldt.

Herudover er det Datatilsynets opfattelse, at Rigspolitiet ikke har levet op til kravene i Schengen-konventionens art. 105, idet Rigspolitiet ikke har sikret, at de oplysninger, der optages i Schengen-informationssystemet, er korrekte og aktuelle, samt at de er lovligt indberettet.

Det er desuden Datatilsynets opfattelse, at Rigspolitiet ikke har levet op til persondatalovens § 5, stk. 4, hvorefter behandlingen af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysninger, og der endvidere skal foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Datatilsynet har noteret sig, at Rigspolitiet har taget skridt til at rette de konstaterede fejl.

Datatilsynet har endvidere noteret sig, at Rigspolitiet vil præcisere de interne retningslinjer vedrørende sagsgange og kontrolprocedure i forbindelse med behandling af sager om indberetning i medfør af Schengen-konventionens artikel 96.

Endelig har Datatilsynet noteret sig, at Rigspolitiet har anmodet Rigsadvokaten om at indskærpe over for politikredsene, at anklagemyndigheden i sager, hvor udvisning kan komme på tale, dels nedlægger en korrekt udvisningspåstand, dels ved modtagelse af afsagte domme nøje gennemgår disse, herunder henvisningen til udlændingelovens udvisningsbestemmelser, med henblik på at sikre, at dommenes afgørelse om udvisning er korrekt i forhold til det pådømte forhold og om nødvendigt tage skridt til berigtigelse heraf.

4. Sammenfattende kan Datatilsynet konstatere, at der i de 443 danske indberetninger af uønskede udlændinge til SIS er sket fejlagtig indberetning i 25 tilfælde, og at der herudover er sket forskellige fejl i yderligere et antal tilfælde.

Indberetningerne til SIS vil kunne få alvorlige konsekvenser for den pågældende person, idet en person efter konventionens artikel 5 som hovedregel ikke vil kunne få tilladelse til at indrejse i og opholde sig i Schengen-området.

På den baggrund er det Datatilsynets opfattelse, at der er tale om et uacceptabelt højt antal fejl, og tilsynet finder således resultatet af undersøgelsen kritisabelt.

5. På denne baggrund har Datatilsynet i brev af dags dato orienteret Justitsministeriet om de konstaterede tilsidesættelser af Schengen-konventionen, udlændingeloven og persondataloven.

6. Datatilsynet forventer at offentliggøre dette brev på sin hjemmeside. Tilsynet vil endvidere orientere Den Fælles Tilsynsmyndighed om resultatet af gennemgangen.

Data Protection Agency

Case: No. 2006-329-0024

Datatilsynets udtalelse

Available at:

http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/vedroerende-beskaeftigelsesministeriets-notat-om-juridiske-aspekter-i-forbindelse-med-indhentning-af-o/ (10-03-2009)

Vedrørende Beskæftigelsesministeriets notat om juridiske aspekter i forbindelse med indhentning af oplysninger til brug for kontrol med udbetaling af kontanthjælp m.v.

Brevdato: 16.08.06

Journalnummer: 2006-329-0024

Ved e-post af 15. august 2006 har Beskæftigelsesministeriet anmodet om Datatilsynets eventuelle bemærkninger til ministeriets notat om juridiske aspekter i forbindelse med indhentning af oplysninger til brug for kontrol med udbetaling af kontanthjælp m.v. Ministeriet har desuden spurgt, om Datatilsynet har bemærkninger til et notat om hjemmel til indhentning af oplysninger fra andre myndigheder om ind- og udrejse til brug for kontrol med udbetaling af dagpenge m.v., herunder hjemmel til registersamkøring.

1. Af § 11 a, stk. 2, i lov om retssikkerhed og administration på det sociale område fremgår, at kommunerne uden samtykke til brug for en enkelt sag eller til brug for generel kontrol kan kræve oplysninger fra andre offentlige myndigheder og arbejdsløshedskasser om økonomiske forhold om den, der ansøger om hjælp.

Datatilsynet er enig med Beskæftigelsesministeriet i, at kommunerne i medfør af § 11 a, stk. 2, i lov om retssikkerhed og administration på det sociale område alene har hjemmel til at foretage registersamkøring i kontroløjemed for så vidt angår oplysninger om økonomiske forhold.

§ 11 a, stk. 2, i lov om retssikkerhed og administration på det sociale område giver således efter Datatilsynets opfattelse ikke hjemmel til kontrolsamkøring med oplysninger om andre forhold – f.eks. oplysninger om ophold i udlandet.

2. Af lov om arbejdsløshedsforsikring § 91, stk. 9, fremgår at

”Direktøren for Arbejdsdirektoratet kan til brug ved administrationen af denne lov indhente oplysninger fra andre offentlige myndigheder og arbejdsløshedskasser, herunder oplysninger om enkeltpersoners indkomstforhold i elektronisk form, bl.a. med henblik på registersamkøring i kontroløjemed. Oplysningerne kan videregives til en arbejdsløshedskasse for så vidt angår vedkommende arbejdsløshedskasses egne medlemmer. Beskæftigelsesministeren fastsætter nærmere regler om, hvilke oplysninger der kan videregives. Oplysningerne er undergivet tavshedspligt i arbejdsløshedskasserne. Straffelovens § 152 og §§ 152 c-f finder anvendelse.”

I det notat, som Beskæftigelsesministeriet har fremsendt, konkluderes det, at der efter bestemmelsens ordlyd og bemærkningerne hertil, både i lov 387 af 13. juni 1990 og lov 372 af 22. maj 1996, vil være hjemmel til at samkøre oplysninger fra en anden offentlig myndighed om f.eks. personers ind- og udrejse med henblik på generel kontrol af, om dagpenge er udbetalt med rette. Det er i den forbindelse anført, at oplysninger om manglende ophold i Danmark er en relevant oplysning til brug for kontrollen af, om en person har ret til dagpenge m.v., idet det er en betingelse for dagpengeret, at den pågældende står til rådighed og har bopæl og opholder sig i Danmark.

Datatilsynet er enig i Beskæftigelsesministeriets vurdering af, at § 91, stk. 9, i lov om arbejdsløshedsforsikring mv. giver mulighed for at samkøre med oplysninger fra en anden offentlig myndighed om f.eks. personers ind- og udrejse med henblik på generel kontrol af, om dagpenge er udbetalt med rette.

Datatilsynet forudsætter, at Arbejdsdirektoratets behandlinger i forbindelse med en eventuel samkøring sker under iagttagelse af persondataloven. Der henvises i den forbindelse til det nedenfor anførte.

3. Persondataloven skal iagttages af de myndigheder, som modtager oplysninger med henblik på kontrolsamkøring.

Myndighedernes behandling af de modtagne oplysninger skal således bl.a. ske under iagttagelse af de grundlæggende krav i persondataloven, reglerne om datasikkerhed og reglerne om de registrerede personers rettigheder.

Af persondatalovens § 5, stk. 2, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål (finalité-princippet).

Det følger endvidere af § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Samtidig skal reglerne om datasikkerhed i persondatalovens § 41, stk. 3, og sikkerhedsbekendtgørelsen iagttages.

En udmøntning af princippet i § 41, stk. 3, er bl.a. sket i sikkerhedsbekendtgørelsens § 11, stk. 1, hvoraf det følger, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. Af § 11, stk. 2, følger endvidere, at der kun må autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

De nævnte regler medfører efter Datatilsynets opfattelse, at myndighederne må tilrettelægge databehandlingen således, at de ansatte ikke har adgang til oplysninger, der principielt ikke er brug for.

Efter en eventuel samkøring mellem et register modtaget fra en anden myndighed og myndighedens egne oplysninger bør de ansatte hos den modtagende myndighed efter Datatilsynets opfattelse alene have adgang til oplysninger om de personer fra den anden myndigheds register, som er omfattet af den kontrollerende myndigheds sagsområde. Dette kan f.eks. ske ved, at myndigheden lader samkøringen ske hos en databehandler, der sørger for, at kun oplysninger om de personer, som der er en sag på hos den kontrollerende myndighed, er tilgængelige for dennes medarbejdere.

Det er endvidere Datatilsynets opfattelse, at antallet af medarbejdere, der har adgang til resultatet af samkøringen, skal begrænses mest muligt.

Datatilsynet kan herved endvidere henvise til tilsynets principielle stillingtagen til den praktiske tilrettelæggelse af kommunernes kontrolsamkøringer. Kopi af omtalen af sagen i Registertilsynets årsberetning 1990 vedlægges til orientering. Registertilsynet lagde bl.a. vægt på, at der blev udviklet et nyt skærmbillede til det såkaldte Sagshenvisnings- og Advissystem, hvortil kun sagsbehandlere på de områder, der var opfattet af samkøringshjemlen, ville få autorisation, ligesom det var en forudsætning for, at der var adgang til skærmbilledet, at der var oprettet en sag på den pågældende borger i kommunen.

4. Datatilsynet har i brev af dags dato besvaret en forespørgsel fra Udenrigsministeriet om mulighederne for at videregive oplysninger om evakuerede danskere fra Libanon til andre myndigheder. Kopi af Datatilsynets svar vedlægges til Beskæftigelsesministeriets orientering.

Det tilføjes, at Datatilsynets udtalelse er af vejledende karakter, og at tilsynet må forbeholde sig sin stillingtagen i tilfælde af en eventuel klage.

Datatilsynet forventer i løbet af kort tid at offentliggøre dette brev på sin hjemmeside.