EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

COMPARATIVE STUDY

ON

DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS

Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28

COUNTRY STUDIES

(Douwe Korff, Editor)

A.2 – DENMARK

BY

Peter Blume

Submitted by:

LRDP KANTOR Ltd (Leader)
In association with

Centre for Public Reform

(Final edit – May 2010)

DENMARK

By Peter Blume

I. Context of Information Privacy

1. Political and economic context.

Denmark is an ordinary Western country with a capitalistic economy. Denmark is however also a welfare state implying that public authorities process huge amounts of personal data. As in other countries the private sector also processes such data today. In general privacy, in particular data protection, is recognized as one of the legal instruments that must regulate these aspects of society.

2. Surveillance context.

There is nothing special in Denmark in this respect.

3. Social attitudes to privacy.

There are no surveys to enlighten this issue. In general the attitude to data protection is positive but only to a certain extent. Is it seen necessary to process data in order to obtain security (crime, terror) this is accepted. It may also be remarked that the young, when they are online, often do not take privacy that seriously.

4. International obligations.

Denmark has ratified the human rights convention which by statute (act 750/1998) is a part of Danish law. Denmark has also (1987) ratified the COE convention 181.

5. Constitutional law.

The Danish constitution (1953) does not contain provisions on privacy. However section 72 provides a procedural protection of the freedom of communication. A public authority may only intervene either on a basis of a court decision or with authority in a statute. Although from 1953 this rule also covers e-mails.

II. Legislation.

1. Definitions and core concepts in the main data protection law

Danish law is founded on the data protection act (429/2000) transposing directive 95/46. The act to a large degree imitates the directive. For this reason it is not necessary to go into many details at this point. Concepts like personal data and processing are defined as in the directive (section 3)

2. Scope of the main data protection law

The act applies to all electronic processing and manual files. Furthermore, in the private sector, it also applies to systematic manual processing (section 1(2) concerning personal data of a private nature (i.e. data that is viewed as private in the penal code section 264d). It furthermore covers disclose of manual data between public authorities (section 1(3), enacted may 2009). It finally covers CCTV surveillance in any form (section 1(8)).

3. Exemptions under the main law

The act does not cover the following (section 2): processing in accordance with article 10 of the human rights convention – processing of a purely private nature – parliament and institutions under parliament – the secret services.

Furthermore the mass media, processing for a journalistic, artistic and literary purpose, are to a large degree exempted.

Certain of the data subject rights do not apply to the police and the courts in criminal proceedings. These rights are regulated in the Administration of Justice act.

4. Territorial scope of the main law

The basic rule (section 4) states in accordance with the directive that that the act applies to controllers established in Denmark carrying out processing in Denmark. The act furthermore applies to third country controllers when their processing is aimed at Denmark (e.g. websites in Danish). – However, it should be added that these rules are very complex and are not easily applied.

5. Other legislation.

Rules on data protection are a part of many Danish statutes. Nobody can probably provide a full account. Major statutes are the following:

- The penal code (1068 of 6.11.2008)
- The statute on financial institutions (897 of 4.9.2008)
- The Public Administration Act (1365 of 7.12.2007)
- The Act on the central personal data register (1134 of 20.11.2006)
- The Act on social services (58 of 18.1.2007)
- The Marketing Act. (1389 of 21.12.2005)
- The act on the DNA profile register (434 of 31.5.2000)
- The Administration of Justice Act. (1069 of 6.11.2008)

6. Data Protection Principles

General considerations

The principles that are part of Danish law are derived from the directive and accordingly the following description is brief.

Besides the issues below it must be mentioned that the principle that processing must be fair and in accordance with a sound purpose (section 5(1+2) are seen as important in Danish practice and may be used to restrict processing that is otherwise lawful.

Purpose limitation.

This principle (section 5(2) is applied fairly often and in particular it is viewed as a restraint on the possibilities of matching data/files. With respect to e-government it is especially important although it to a certain extent may be overridden by special statutes.

Collection limitation.

This principle (section 5(3) is also important in practice and is viewed as a general requirement of proportionality.

Data quality.

No special comments regarding this principle (section 5(4))

Data security.

The rules (sections 41 and 42) on data security are in general outlined in the act and are supplemented by rules in statutory instruments with respect to public administration and the courts. The rules covering physical, organisational and technical security, are relevant both for controllers and processors, and they are the main focus when the DPA conducts audits.

Openness practices.

There are no special rules or practices in this respect. Openness is achieved through the rights of the data subject; see below in 7.

Deletion

Data that are not correct or misleading may be deleted (section 5(4). However, in public administration the practice is to block such data.

Outdated data must be deleted (section 5(5) or placed in an archive (section 14). There is no fixed time but in practice a 5 year limit is followed in many cases.

7. Areas of special concern

Processing of sensitive data.

Processing is regulated in section 7 that conforms with article 8 of the directive. In general the DPA in its practice tries to ensure that sensitive data only rarely are processed without consent in the private sector.

In section 8, formally transposing article 7 of the directive, certain kinds of data are regulated in such a way that they almost are viewed as sensitive. This is data on criminal offences, serious social problems and other data of a clearly private nature.

Automated decisions.

Section 39 is drafted in accordance with the directive but plays a very minor role in practice. This is due to the many exemptions (contract/statute) that removes most of the contents of this rule. The rule could be important not least with respect to e-government but this is unfortunately not the case.

Data matching.

The only rule in the act is section 45 that states that matching for control purposes must be notified to the DPA before it takes place. – See also above in 4.2.

In practice, due to a statement from the legal committee in Parliament from 1991, it is assumed that matching for a control (supervisory) purpose can only take place with authority in statute and that citizens have to be informed about the procedure before it takes place. The DPA enforces these principles.

Direct marketing.

The rules on direct marketing are placed in the marketing act (section 6) and include a prohibition on spam and the possibility of using a Robinson list.

The data protection act also includes some rules (section 6(2-4) and 36) concerning disclosure of data with respect to marketing. When the data are specific or when then are sensitive this presupposes consent. When data are general ("he buys wine) the data subject has a right of objection. The Robinson list also applies.

Originally, private enterprise was very upset by these rules but today they seem to work quite well.

Credit reporting.

Chapter 5 and 6 of the act regulates credit reporting agencies. This is the most detailed rules of the act and the DPA also employs many of its audits in this area. Misuse of data can have immediate consequences for the data subject.

The rules state when an agency may register data (relevant for credit assessment and not sensitive data), for how long data may be kept, to what degree it may be disclosed and to whom (only subscribes), rights of data subjects (information, access) and under which conditions public authorities may disclose data to an agency. – Issues not covered are regulated by the general rules of the act.

It may be noted that the DPA has decided that data may not be registered merely due to consent of the data subject. [in contrast, due to special rules on casinos this is possible in this area!].

Identity information.

Section 11 of the act regulates processing of the personal identity number. This is in general possible in the public sector while it in the private sector as the main rule presupposes consent. The PIN may not in any sector be made public without consent.

Denmark has had the PIN system since 1968. Although people are still aware of the dangers (identity theft) there is in general a relaxed attitude and there are not often incidents.

Use of publicly accessible data.

As a starting point this issue is regulated by the Freedom of Information Act that provides free access to data that is not confidential (sensitive and some ordinary data). The act is expected to be revised within the next couple of years.

A major issue has been the increased number of statutory rules that make more data accessible, often based on the consideration to consumer protection: e.g. doctors that maltreat patients, shops that are unclean, etc. This information is placed on the net and such rules are from the perspective of data protection problematic.

In general it should be added that it is often difficult to explain that the data protection act applies to data that has been made public when this is not due to the data subject.

The Internet.

There are no special rules on the internet but many issues of course relate to the net (see in 5.7.). It is probably not feasible to have such rules. As elsewhere especially social networks are of special concern currently. In general the increased mixture of legal cultures and corporate attitudes mean that it is very difficult to regulate data protection on the net.

8. Cross-border data transfer.

Transfers into Denmark.

There are no rules on data import and no need for such rules. The data protection act covers all personal data located in Denmark regardless of origin and regardless of the nationality of the data subject.

Transfers out of Denmark.

Transfers to third countries are regulated in section 27 that is in accordance with the directive. In some cases (section 50) transfers have to be permitted by the DPA.

A basic condition is that processing is lawful under Danish law. This is also the case for transfers to EU countries.

The Faroe Islands and Greenland are third countries.

9. Rights of data subjects.

The Danish rules are similar to those of the directive.

Informing of data subjects.

Sections 28 and 29 regulate this issue concerning direct and indirect collection of data. In particular the exemptions in respect to indirect collection (sections 29 and 30) have given raise to several cases. The DPA takes in general the position that the exemptions must be interpreted restrictively.

Confirmation of processing.

There are no rules on this besides those mentioned under the previous subheading. It is accordingly merely collection that is informed about.

Access.

The right of access is stated in section 31. In general it is used fairly rarely.

Correction.

This right is stated in section 37. It is not used often. There have been attempts to get the DPA to intervene in especially social cases with respect to soft data (assessments). The DPA has maintained that it is not an ordinary complaint authority and only applies the rule when this is due to data protection considerations.

Notification of disclosure.

This may be covered by section 29 in some cases. According to section 37 there is a right of notification to controllers that have received incorrect data but this possibility is seldom used.

Right to object to direct marketing.

See under "direct marketing" in section 6, above, concerning section 36.

Individual remedies.

A right to damages is provided in section 69. This rule is not applied by the DPA but by the courts, and the rule has in practice had no real importance. It is assumed that there must be a economic loss which is hard to prove and which also seldom is the case.

8. Supervision. Notification and enforcement.

The act is supervised by the DPA (Datatilsynet) that consists of a secretariat headed by the commissioner (director) and a council consisting of 7 members with a supreme court justice as chairman. The DPA is financed through the ministry of justice and may report directly to parliament.

In general only processing sensitive data have to be notified. Certain special data processing situations have also to be notified and require permission, e.g. research databases.

Enforcement takes place through handling of concrete cases and audits.
Section 70 contains criminal sanctions. These are applied sometimes but the level of sanctions, determined by the courts, is quite low.

The main deterrent (and sanction) is the risk of bad publicity.

9. Sectorial (self) regulation and codes of conduct.

There is not much to report on this point. Many (large) corporations aim at ensuring data protection. There are no official codes of conduct or seals etc. [to my knowledge].

III. Summary and conclusions.

The data protection regime is well organized in Denmark and functions fairly effective although data misuse of course occurs.

Data subjects have in general only a faint idea of the law and its contents, but in this data protection does not differ from other law.

Danish law is in accordance with EU-law. In the application of the different rules the interpretation of the rules stated by the Commission and the Court is taken seriously into account. Also the opinions of the Article 29 group play a role in this respect.

- o – O – o -

References.

Peter Blume: Databeskyttelsesret (3.ed. København 2008)

Kristian Korfits Nielsen, Henrik Waaben: Lov om behandling af personoplysninger (2.ed. København 2008)