Country Report Denmark

ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation

Savin, Andrej

Document Version
Final published version

DOI:
10.2759/26900

Publication date:
2015

COUNTRY REPORT

DENMARK

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Andrej Savin, Copenhagen Business School

Date: 18 August 2014

Contents

Part 1: Management summary

Management summary for Denmark:

- The ePrivacy Directive has been implemented in Denmark through a range of legislative instruments, beginning with the Act on Electronic Communications and Services but leading into more important Executive Order on Provision of Electronic Services and the Cookie Order. This structure could be confusing for outsiders as it involves several acts, all of which are concerned not just with one but with several directives. The use of ministerial orders can be explained by the need to introduce flexibility into the fast-changing area, but avoiding a lengthy and complicated full legislative process.

- The scope of the legislation leaves no surprises. In terms of Article 3, the Directive applies to all services that target Denmark. In terms of Article 5, it applies to services which are established in Denmark. The implementation in terms of the networks, services or providers is largely following the Directive. The guidelines to the implementing Provision Order give a comprehensive explanation of the key terms and how they may be applied in practice.

- Art. 5.3 of the Directive has been the subject of a special ministerial order (the Cookie Order) which has, in turn, been followed by comprehensive and practically-oriented Guidelines. The latter take cognizance of the many different types of cookies and address them (even though the legislation itself does not). The enforcing authority (Danish Business Authority) emphasized that location data is not limited to cookies and that the reality of electronic life may have overtaken the legislation.

- Traffic and location data have been implemented in line with what is required in the Directive. Although the wording is occasionally different, it follows the general direction and the spirit of the Directive.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been implemented in the Market Practices Act. The regime chosen is the strict opt-in regime for emails, automated calling and the fax machines with the possibility to use other means of communication only if the users have not placed themselves on the opt-out list. Guidelines have been published on the website of the Consumer Ombudsman.

Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC (hereafter ePrivacy Directive) has been transposed through the Act on Electronic Communications and Services (Act No. 169 of 3 March 2011), of which the consolidated version is Act No. 128 of 7 February 2014 (hereafter "the Electronic Communications Act" or "the Act"). The consolidated Danish version of the Act is to be found here: https://www.retsinformation.dk/Forms/R0710.aspx?id=161319. The unofficial English version of the Act can be found at: http://erhvervsstyrelsen.dk/file/255024/LOV-nr-169-af-03_03_2011.doc

- The Act is complemented by ministerial orders (Executive Orders). These are specifically called for in Articles 3, 4, 5, 8, 9, 61 and 81 of the Act on Electronic Communications and Services.

- The actual implementation of the ePrivacy Directive is to be found in these ministerial orders as the Act concerns itself with other general telecommunications and electronic commerce issues. In fact, the Act implements a range of different EU Directives, among which are the Access Directive, the Framework Directive, the Universal Service Directive, the Authorisation Directive and others.

- The complete list of all the acts that implement the Directive (Consolidated law, the Act and executive orders with interpretative Guidelines) can be found on: https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058

    - The **general provisions** of the ePrivacy Directive (other than the ones mentioned below) are to be found in the Executive Order on the Provision of Electronic Communications Networks and Services (Executive Order No. 713 of 23 June 2011), https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf, hereafter "the Provision Order".

    - The provisions concerning **cookies** are to be found in the Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment, (Executive Order No. 1148 of 9 December 2011), https://www.retsinformation.dk/Forms/R0710.aspx?id=139279, unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf , hereafter "the Cookie Order".

- The provisions on **unsolicited marketing** have been implemented in the Marketing Practices Act (Act

no 58 of 20 January 2012), unofficial English version at http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act/marketingpractisesact, hereafter "Marketing Practices Act". The Act predates the ePrivacy Directive but was amended accordingly.

- All of the laws (the Act and the executive orders) have been in existence prior to the changes required in the 2009 EU telecoms reform. Consequently, the older versions of the above acts can also be found at: https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058

Concordance table

ePrivacy Directive	Transposed in Danish law by:	URL
Art. 2 (Definitions)	Article 2 of the the Electronic Communications Act, Article 2 of the Provision Order and Article 2 of the Cookie Order.	https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058
Art. 3 (Scope)	Article 1 of the Provision Order, Article 1 of the Cookie Order (for scope) and Article 2 of the Provision Order and Article 2 of the Cookie Order (for definitions)	https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf
Art. 5.1 (Confidentiality)	The general legal basis is found in Articles 7 to 9 of the the Electronic Communications Act but the specific implementation is in Articles 23 and 24 of the Provision Order.	https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf
Art. 5.2 (Business exception)	The general legal basis is found in Articles 7 to 9 of the the Electronic Communications Act but the specific implementation is in Articles 23 and 24 of the Provision Order.	https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf
Art. 5.3 (Cookies)	Article 3 of the Cookie Order	https://www.retsinformation.dk/Forms/R0710.aspx?id=139279 Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf
Art. 6 (Traffic data)	Articles 23 and 24 of the Provision Order	https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-

		udgave.pdf
Art. 9 (Other location data)	Articles 23 and 24 of the Provision Order	https://www.retsinformation.dk/Forms/R0710.aspx?id=137773, Unofficial English version at https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf
Art. 13 (Unsolicited communications)	Article 6 of the Marketing Act	http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act/marketingpractisesact

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

Full name of the authority	English translation of the short name	The part or provision(s) it supervises	URL link to website
Erhvervsstyrelsen	Danish Business Authority	All provisions except the ones specifically listed below	www.erhvervsstyrelsen.dk
Datatilsynet	Data Protection Authority	General data protection	http://www.datatilsynet.dk/
Teleklagenævnet	The Telecommunications Complaints Board	Telecommunications side of the ePrivacy Directive, namely complaints relating to telecoms violations. This will mostly affect corporate players and the government	http://www.teleklage.dk/om-teleklagenevnet
Forbrugerombudsmanen	Danish Consumer Ombudsman	Consumers complaints of general and specific nature, unsolicited communications	www.consumerombudsman.dk
Konkurrence- og Forbrugerstyrelsen	Danish Competition and Consumer Authority	Unsolicited Communications	www.kfst.dk

Explanation:

- *Erhvervstyrelsen* is the main authority named in the Electronic Communications Act and, therefore, the main authority in charge of the ePrivacy Directive. This area used to fall under the competence of an authority called *IT- og Telestyrelsen* (IT and Telecommunications Authority) but this body, along with some others, have been merged into the present one. A section within the Authority now deals with IT issues and is called *Tele og Internet* (Telecoms and Internet).
- The Data Protection Authority maintains its general competence over breach of data protection laws. In cases where a breach of the ePrivacy Directive also constitutes a breach of general data protection laws, this authority will maintain its competence.
- The telecommunications complaints board will have the authority to hear complaints in cases where breaches of the ePrivacy Directive primarily concern telecommunications issues.
- The Consumer Ombudsman has the general capacity to protect consumers, particularly in cases concerning Marketing Practices Act violations
- The Danish Competition and Consumer Authority has the competence to monitor various aspects concerning competition law but also general consumer protection
- The competence seems, therefore, to be split between a number of authorities. There is insufficient case-law to confirm which authority is dominant.

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The Act defines electronic communication **networks** in Article 2(4) as "*Any form of radio frequency or cable based telecommunications infrastructure used for handling electronic communications services*." Public electronic communications networks are those which are "*made available to a number of end-users or providers of electronic communications*" if those are not specified in advance. Public pay telephony as well as broadcasting by any antenna equipment, digital or analogue, are excluded. (See Guidelines to Provision Order, http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf, page 4). On-demand and over-the-net TV and telephony are, therefore, included although doubts exist over cases where TV is bundled with the Internet and provided through the broadband line.

The Act defines **electronic communication services** in Article 2(7) as those "*consisting wholly or mainly in electronic conveyance of communications in the form of sound, images, text or combinations thereof, by means of radio or telecommunications techniques, between network termination points, including two-way and one-way communications*." Public electronic communication services are defined in Article 2(8) as those "*made available to a number of end-users or providers of electronic communications networks or services who have not been specified in advance*." Article 2(9) defines information and content services as those "*to which other end-users get access via electronic communications networks or services on the basis of an individual request*."

Article 2 of the Provision Order defines "*prepaid electronic communications services*" as services where the end- user, "*via purchase of a card or electronic communications services comparable therewith, prepays the combined service, including the current usage*." Value-added services are defined as those which require "*the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof*."

Providers are defined in Article 2 of the Act as "*any person who makes products, electronic communications networks or services governed by this Act available to other parties on a commercial basis*." Commercial providers are defined in the same article as those who "*for commercial purposes, offers products or electronic communications networks or services governed by this Act as its main service or as a non-accessory part of its business*."

In general, Danish legislation contains straightforward definitions of the three terms in question, occasionally providing more detail (as is the case for 'services'). These definitions are in line with other relevant legal frameworks (e.g. with regard to general electronic commerce).

4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?
No straightforward answer can be given to this question. The wording itself makes no specific mention of any VoIP, webmail or location based services. It can be inferred from the general definitions (given under the answer to question 3 above) as well as from the context of the Provision Order (in particular, the passages on location data) that such services do fall within the scope of the implementation. There is, in any case, nothing explicit in the text that would prevent from being considered such and, indirectly, through the Provision Order, one can conclude that any non-antenna and non-payphone sending of signals is covered. It is worth remarking that the legislative competence in the area seems to be mixed. While telecommunications services are subject to one legislative regime, electronic commerce falls under another and audio-visual services under yet another regime. This may create uncertainty as to whether one, two or all three apply to the three situations outlined in the question. This has not yet been resolved in Danish practice.

5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?
By way of example: have there been cases where your national law has been applied to a foreign entity?

The answer to this question is not straightforward. The Act does not contain provisions on its territorial scope and the same is true for the Executive Orders that implement the ePrivacy Directive. The generic language of the Act would seem to suggest that it applies in all situations where services are provided on Danish territory, irrespective of the nature of the provider, its corporate seat, ownership structure, etc. The general supervisory/enforcement authority of the Danish agencies confirms this.

The state of confusion in this area has been confirmed in 2009 when Data Protection Agency began exploring its authority over Facebook (see http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook.pdf). The Agency reiterated that "*the Working Party is of the opinion that the national law of the Member State where the user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk*." Somewhat surprisingly, it asked Facebook whether it considered itself a data controller within the meaning of the Data Protection Directive and asked it to appoint a representative for Denmark. This debate has not been brought to a conclusion and the state of suspense remains.

The correct way to interpret the provisions would be to consider that electronic services offered on the Danish territory are covered. In that sense, at least theoretically speaking, a service provider from another country, irrespective of whether this is a EU country or not, would fall under the territorial scope of the Danish laws in all cases where the service is accessed. The Danish Business Authority, however, emphasized that Article 5 only applies to businesses established in Denmark.

No cases have been reported involving an extraterritorial element. It is worth noting that, due to harmonization, intra-EU cases are unlikely to raise serious differences.

6. Please describe and give references to any form of 'guidance' on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

a. No official guidance exists on the Electronic Communications Act. With regard to the Provision Order official guidelines exist: Vejledning til udbudsbekendtgørelsen, of 1 October 2012, available at http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf (in Danish). In this 'order', the authorities explain that some of the laws in the area apply to businesses only while other mainly to consumers. Rather than elaborate on this, they refer to the Telecommunications Law. No further definitions or clarifications are given on networks, services or providers, except one:
The Guidelines (page 6) specifically mention cases where the provision of internet services is packaged with radio and TV provision. This often the case in Europe, where a package containing broadband, internet or regular telephony and cable or internet TV is bundled together and offered at a discount. In those situations, the radio and TV distribution part of the service will be treated as antenna-provided TV and will be taken out of the scope of these laws, even though the Internet itself will be in.

b. No information exists on this.

7. What is your individual view of:
a. the effectiveness of these rules in practice, i.e.do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

a. Danish telecommunications and electronic services providers suffer from the same uncertainties arising out of convergence of technologies that affect other EU states. With regard to the **scope**, there is an obvious lack of clarity as to what the rules apply to (content or services) and in what situations. This is addressed neither in the legal texts themselves nor in the guidelines. Furthermore, the territorial scope (Danish vs EU vs non-EU providers) is left undefined.

   With regard to **clarity**, the main legal texts cover various EU directives and refer to executive orders extensively. As a consequence, the implementation of a particular EU directive in this area is often to be found in multiple documents. This is difficult to follow and work with. On the other hand, the guidelines (the Provision Order Guidelines and the Cookie Order guidelines) are written clearly and comprehensively.

b. While it is not likely that the enforcement method and the use of ministerial orders will be changed, it would be possible to issue further guidelines on the issues above. In this context. Most important here may be the clarification of territorial scope.

B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of 'communications' under this legislation? If so, how is it formulated?
The implementation of this provision is split between several acts. The general framework is to be found in Articles 7 to 9 of the Act. These articles, under the title "Secrecy of electronic communications, information security, processing of personal data, assistance for interception etc." provides a general legal framework for information security. Article 7 provides that owners of electronic communication services shall not "*be entitled without authorisation to disclose or utilise information about other persons' use of the network or the service or the content thereof that comes to their knowledge in connection with the provision of electronic communications networks or services*." Furthermore they must take measures to ensure that information about other persons' use of the network is not available to unauthorized persons. Article 152 of the Danish Penal Code covers any violations of this provision. Article 8(1), however, delegates the creation of rules for "minimum requirements for information security and processing" for providers to the Minister for Science, Technology and Innovation. Article 8(2) delegates the creation of the rules for "natural and legal persons' storing of information on end-users' terminal equipment" and access to this information to the same Ministry. Ministerial Order No. 988 of 28 September 2006 (available only in Danish at https://www.retsinformation.dk/Forms/R0710.aspx?id=2445), known as "the Logging Order", was enacted in pursuit of the Data Retention Directive. As such, it modifies the implementation of ePrivacy Directive in its area of applicability. It is not clear what will happen with this law following the recent declaration of invalidity of the Data Protection Directive by the CJEU. Articles 23 and 24 of the Provision Order, entitled "Processing of traffic and location data" specifically require erasure or anonymization of traffic and location data and only allow it in specifically defined cases or upon user's consent.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn't affect "legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication." Please describe the transposition and substance of this exception in your national legislations
Article 23 of the Provision Order permits processing "for the purposes of subscriber billing and interconnection payments." Such storing is permitted "only up to the end of the period during which the bill may lawfully be challenged or payment pursued". This, however, implements Article 6, not 5(2). There does not seem to be a direct implementation of Article 5(2) in Danish legislation. No other elaboration on the subject is offered in any of the other implementation documents.

3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.
Article 10 of the Act obliges providers to arrange the equipment in a manner, which will enable the police to access the information about traffic and to access historical data and, as the text of the Act calls it: "forward-looking data", to intercept and observe, provided that any such action is in compliance with Parts 71 and 74 of the Administration of Justice Act. Further exceptions are provided in the Provision Order, which in Article 23(1) refers to Article 786(4) of the Administration of Justice Act, and Article 24(1), which refers to Article 791 of the Administration of Justice Act. The former allows police access to confidential information as part of an ongoing investigation. Such requests are limited to the general rules on injunctions for securing evidence in criminal matters. The latter deals with the evidence already in police hands and confirms an obligation to destroy it where it is no longer needed. This issue is also directly related to the Danish implementation of the Data Retention Directive, which can be found in the Logging Order. This implementation predates the actual Directive by some 4 years. The Danish law goes well over and above what is required in the Data Retention Directive. Session logging includes more internet packets than required and more information concerning sources and IP address being collected, with the retention limit for data being one year. While this represents a "public policy" exception, and therefore only one part of the question examined here, it is worth noting that this issues is both difficult and controversial. A specific exception exists in relation to marketing electronic communication services (Provision Order, Art 24(3)). This is only possible with prior consent.

4. **a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:** • **Whether the interception of MAC addresses would entail breach of confidentiality;** • **Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;** • **Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?** **b. Is there any other important legislation with regard to the protection of private electronic communications?**
a. Danish legislation does not specifically address automated breaches. The issues mentioned in the question are not expressly addressed anywhere in the implementing framework. b. None other than the legislation already mentioned above.

5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
a. the scope and substance of your national implementation
b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Article 3 of the Cookie Order entails a detailed transposition of Article 5.3 of the Directive. It provides that "*Natural or legal persons may not store information, or gain access to information already stored, in an end-user's terminal equipment, or let a third party store information or gain access to information, if the end-user has not consented*." The user's consent shall only be valid upon presentation of comprehensive information. This is the case if:
"*1) it appears in a clear, precise and easily understood language or similar picture writing,*
2) it contains details of the purpose of the storing of, or access to information, in the end-user's terminal equipment,
3) it contains details that identify any natural or legal person arranging the storing of, or access to, the information,
4) it contains a readily accessible means by which the end-user to will be able to refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end-user should make use thereof, and
5) it is immediately available to the end-user by being communicated fully and clearly to the end-user. In addition, when storing of information or access to information takes place through an information and content service, information to end-users must be directly and clearly marked and be accessible at all times for the end-user on the information and content
service in question."

b. The abovementioned provision itself does not distinguish between types of cookies. The Guidelines to the Cookie Order, however, in Section 2 provides a very detailed overview of which technologies are covered. Emphasizing that the rules are technology neutral, the guidelines stipulates that the Order covers similar technologies, including storing and access of information from USB keys, CDs, CD-ROMs, external hard drives, etc. Not only classic html cookies but any type of cookies, including Flash cookies, Web storage in HTML5, Java script or Microsoft Silverlight. Cookies of different life spans are all covered. First party cookies and third party cookies are separately mentioned. Session cookies and persistent cookies are both covered.

6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Consent is defined in Article 2(1) No. 8 of the Cookie Order as "*any freely given, specific and informed indication of the end user's wishes by which the end-user confirms its agreement to information being stored, or access to stored information being gained*" in the end-user equipment. This definition implies a real choice but this does not mean that the in any other situation, the service provider should provide website functionality without cookies. In other words, it is legal to employ a "take-it-or-leave-it" scenario, where rejection of cookies leads to inability to use the website.

Consent, as should be clear from the five requirements outlined in the answer to question 5 above, must be presented in clear and easy to understand language. The purpose of the storing must be explained and the details of the person storing must be available. The refusal of consent must be made easy. All of the information must be made available "immediately", "fully" and "clearly". The Cookie Guidelines emphasize that the information may be layered but the essential information must be available at once. The Guidelines say that such "essential" information concern "all purposes of cookies and similar technologies" and "who is using cookies and similar technologies".

An indication of the user's wishes can be done by either ticking a box, clicking a button or filling a form or by actively using of a service where it must be clear that there is storing of information. The Cookie guidelines emphasize, in the case of the latter, that it is not merely enough that the site stores tells the user that cookies are used but it must be possible that continued action (e.g. clicking) will trigger their use.

The Guidelines explain that some websites place cookies even before consent is obtained (e.g. for statistical purposes of counting the number of hits a site gets). The legal status of these is not clear and the Danish Business Authority is not enforcing the rules in the absence of official clarification from the Commission.

There is nothing specific on mobile devices although the Guidelines offer examples which are specific to these devices (and even include pictures of an iPhone). This means only that the Agency is aware of the specific nature of mobile communications; the rules itself do not vary.

The Guidelines address the problem of third party cookies, which are stored through the main sites (e.g. various adverts on a web page provided by a newspaper). These third party sites embed their content on the main sites. The Guidelines demonstrate how the consent issue can be resolved by using different technical solutions.

7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?
Article 4(1) of the Cookie Order allows storing of cookies and similar technologies if the storing is 1) for the sole purpose of carrying out the transmission of the communication over an electronic communications network or 2) storing of or access to information is necessary in order for the service provider of an information society service explicitly requested by the end-user to provide this service. The language here is consistent with the requirement of the ePrivacy Directive. The Cookie Guidelines spell these out as: cookies used when connecting to the Internet (for the first) and cookies ensuring the functionality of a service requested (for the second). Article 4(2) says that storing is allowed where such storing is a technical precondition for being able to provide a service: "*Storing of or access to information in an end-user's terminal equipment is necessary, cf. subsection (1), no. 2, if such storing of or access to information is a technical precondition for being able to provide a service operating in accordance with the purpose of the service*." The Guidelines provide examples of electronic shopping baskets, log-in situations, authentication cookies, etc. as examples of exemptions.

8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users' views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The Danish Business Authority has confirmed on several occasions that, while general compliance exists, there are wide compliance discrepancies between companies and that no company complies 100%. Based on a sample of 50 companies taken in 2013, the Authority found that 48 out of 50 sites informed the users on cookies. 78% had good navigation practices compared to 36% 8 months earlier. (See http://www.atomic.dk/nyheder/overholdelse/danske-hjemmesider-overholder-ikke-nye-cookieregler/801692066)

In practice, most Danish companies use a simple prompt/pop-up banner, which can be ignored. In other words, it is normally possible to simply continue using the site without actually clicking on it. It is not clear whether cookies are, in such situations, actually placed but the evidence suggests that, in some cases at least, they are. A minority of prompts provide detailed information, with dedicated areas of the site explaining the mechanism in plain language. The majority of companies use very reduced information. Some companies still use the old model where no specific information is provided in advance.

9. Please describe and give references to any form of 'guidance' on the interpretation and/or application on these questions provided by: **a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)** **b. national courts through rendering of case law**
a. Very detailed assistance is provided in the Cookie Order guidelines (http://erhvervsstyrelsen.dk/file/253400/cookie-exec-order-guidelines-english-version.pdf) These are published by the Danish Business Authority, which has the main enforcement responsibility. The Guidelines address the Order article-by-article, frequently providing practical examples. The Guidelines have a separate Technical Guide, which describes a five-step process for compliance with the cookie rules. For each of the steps (identifying web property, checking if cookies are set, giving information, removing unwanted cookies, obtaining consent), a detailed explanation is provided (including illustrations). b. No cases have been rendered yet.

10. What is your individual view of:
a. the effectiveness of these rules in practice, i.e.do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

a. It seems that general awareness of the basic requirements of the ePrivacy directive as amended in 2009 exists both in the corporate world and with customers. However, both providers and users are publically voicing complaints. The former because of the impracticality of the extra burden, the latter because of little or no real gain.

   Anecdotal evidence suggests that Danish consumers are comparatively well-informed in matters of Internet safety and electronic commerce. The broadband penetration and speeds as well as other parameters are comparatively high. Consumers rely on public ranking systems (such as Trustpilot) and on- and off line consumer information rather than on cookie alerts. An average consumer may or may not feel that a website is safe, not on the basis of cookie prompts but on the basis of other parameters such as location of the site, its "look and feel" and the nature of the business. The author of this national report, in conversation with ordinary Danes, has yet to find one who claimed that the new rules had benefited them. Most people ignore the prompt, unless it is impossible to proceed with the site. In most situations, this is not the case. On the other hand, the relatively extensive system of consumer protection (which exists since prior to 2002) and keeps being widely used.

   In summary, the 2009 reform is seen locally as being somewhat bureaucratic and lacking in real effect. It is worth emphasizing that this is particularly true after Edward Snowden revelations of 2013 and a number of high-profile pirate attacks. While most users and businesses realize that reinforcing security regarding data storage and collection is of importance, the belief is that the present measures only touch the surface.

   It is this author's belief that the new rules (i.e. the 2009 reform) have had little or no material effect in practice and that true changes may be achieved elsewhere.

b. It is likely that the problems do not lie in the legal instruments themselves but in practicalities of Internet operation. One improvement relatively easily achieved is increased coherence at EU level between the three directives (Data Protection – ePrivacy – Data Retention). As already suggested, the Danish legislation is split between several instruments. It is not impossible to bring more coherence into this framework.

C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.
Traffic data is defined in the Provision Order as "*data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*." This definition does not appear to be in any way different from the one in the Directive.

2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects
Article 23(1) of the Provision Order requires that traffic data be erased or anonymized where data are no longer necessary for transmitting communication. The exceptions are laid down in the Administration of Justice Act. As per Article 23(2), it is permitted to process and store traffic data for the purposes of subscriber billing and interconnection payments but only up to the end of the period during which the bill may lawfully be challenged or payment pursued. As per Article 23(3) processing traffic data regarding subscribers or users for the purpose of marketing electronic communications services or for the provision of value added services, is permitted provided that the user has consented prior to the processing but only to the extent and necessary for such services or marketing. In such cases, users must have the option of withdrawing their consent. Article 23(4) further requires that providers inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in subsections (2) and (3). Where data are processed for the purposes mentioned in subsection (3), information shall be given prior to obtaining consent. The overview of the above provisions confirms that the requirements for lawful processing have not been clearly spelled out but set in negative terms only – in the form of prohibition of certain actions.

3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?
Article 23(1) of the Provision Order requires that traffic data be erased or anonymized "where data are no longer necessary for transmitting communication". The exceptions are contained in the Administration of Justice Act. The latter, as indicated above, goes wider than the moribund Data Retention Directive.

4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?
No such cases have been reported by the Danish Business Authority and the author is not aware of any relevant judicial case law.

5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
The rules seem to be straightforward. The requirement for anonymization of traffic data is clear. A problem may be in the lack of evidence on the extent to which traffic data is really anonymized. The problems may lie in the data retention rules and this is on the government side, not on the corporate side. The Danish government has recently confirmed that there is no need to significantly revise the retention laws (see http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/) This is the position that remains controversial in both business and consumer circles.

D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.
Location data are defined in article 2 of the Provision Order as "*Data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a public electronic communications service*." This definition does not seem to be different from the provided in the Directive.

2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users' devices, usually when they download applications?
Pursuant to Article 24 of the Provision Order, location data can only be processed when it has been made anonymous or "*when the subscriber or user has consented to the processing".* In the latter case, only to the extent and duration necessary "*for providing a value added service*". Providers processing location data must inform the subscribers or users, "*prior to obtaining their consent, of the type of location data other than traffic data which will be processed*." Furthermore, providers must inform the subscribers of the "*purposes and duration of the data processing*" and if the data will be transmitted to a third party "*for the purpose of providing a value added service*". Where the user's consent had been obtained, the user must continue to have the option of by "*using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication*". The processing of data must be "*restricted to persons employed by or acting under the authority of the provider of the network or service or of the third party providing the value added service*". The implementation does not contain discrepancies with the ePrivacy Directive and appears to be straightforward. It is not clear from the text of the Order whether third parties who harvest data are covered. A strict reading would suggest so, in which cases the anonymization and consent requirements would apply to them in the same manner as they apply to any other provider. The Provision Guidelines do not address this point.

3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?
The general requirement of Article 24(1) allows processing if data are anonymised. This is one of the two requirements, the other being informed consent. No other mention of anonymisation is made.

4. Please describe and give references to any form of 'guidance' on the interpretation and/or application on 'location data rules' provided by: **a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)** **b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?**
a. The Guidelines for the Provision Order have been issued on 1 October 2012: "Vejledning til udbudsbekendtgørelsen" Danish version on (http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf), no English translation exists. The Guidelines were published by the Danish Business Authority, the same one that issued Cookie Guidelines. The Guidelines take an article-by-article approach, are over 60 pages long and fairly comprehensive. The text is mostly clear and understandable to non-experts, although fewer examples have been given than in Cookie Guidelines. Two appendices have been provided in the Guidelines. The first concerns the requirements for contract content re Article 9 (Common terms for commercial provisions of electronic communication networks and services to end-users). The second concerns information given to consumers in cases of prepaid electronic services. b. No cases exist on this issue.

5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
The rules are relatively straightforward and follow the letter and spirit of the ePrivacy Directive. It is difficult to assess the effectiveness of these rules'. The reports of abuses of location data are widespread. A significant number of these relate to harvesting of such data by third parties. Neither the European nor the national legal framework has a clear answer to this challenge. The author of this report feels that, although the rules may be clear and logically consistent, they are not successfully targeting the problem which would require a rehaul of the entire data protection system and would also need technological and societal solutions entirely independent of any legal intervention. In other words, the law is a necessary but not sufficient precondition for eliminating the problem.

E. Unsolicited commercial communications

1. As to 'unsolicited direct marketing communications' (as dealt with in article 13 of the ePrivacy Directive) please describe: **a. the scope and substance of your national implementation** **b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.**

a. The rules have been implemented through the Danish Marketing Practices Act (Consolidated version: Lovbekendtgørelse nr. 1216 af 25. september 2013, unofficial version available in English http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act/marketingpractisesact).
Article 6 covers unsolicited communications:

> (1) *A trader must not approach anyone by means of electronic mail, an automated calling system or facsimile machine with a view to the sale of products, real property, other property, labour and services unless the party concerned has requested him to do so*.
> *(2) Notwithstanding subsection (1), a trader that has received a customer's electronic contact details in connection with the sale of products or services may market his own similar products or services to that customer by electronic mail, provided that the customer has the option, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in the event of subsequent communications.*
> *(3) A trader must not approach a specific natural person using other means of remote communication with a view to sales as referred to in subsection (1) if the person concerned has declined such communications from the trader, if it may be seen from a list prepared each quarter by the Central Office of Personal Registration (CPR) that the person concerned has declined communications for such marketing purposes, or if the trader, by consulting the CPR, has become aware that the person concerned has declined such communications. Telephone communications are also subject to the regulations governing unsolicited communications in the Act on Certain Consumer Agreements.*
> *(4) Subsection (3) does not apply if the person in question has previously requested the communication from the trader.*
> *(5) The first time a trader makes a communication as referred to in subsection (3) with a specific natural person who is not on the CPR list, the trader shall inform him clearly and comprehensibly of his right to decline communications from the trader as referred to in subsection (3). At the same time, the person concerned shall be offered an easy manner of declining such communications.*
> *(6) No payment may be requested for receiving or noting information to the effect that a request under subsection (1) is being revoked or that communications as referred to in subsection (3) are being declined.*
> *(7) The Minister for Business and Growth may lay down more detailed regulations governing the trader's duty to provide information under subsection (5) and duty to offer an opportunity to decline communications as referred to in subsection (3).*

This is the opt-in regime, which is expressed in somewhat clearer terms than in Article 13 of the ePrivacy Directive. Overall, the implementation follows the spirit of the Directive.
The overall idea is that no unsolicited communication by email, fax or auto-calling machines can be sent unless the user had requested it (paragraph 1). The exception (paragraph 2) is for traders that already have information from previous transactions and would like to use it again. They can do so, provided the users can opt out at any point before the initial transaction or after the subsequent advertising. A trader must not pursue consumers who have already opted out or have put their names on the official opt-out registers with other means of unsolicited communications than in paragraph 1 (paragraph 3), although this is not the case if a person had already previously requested info from the trader (paragraph 4). In cases where the person is not in an opt-out register, it is necessary for a trader to explain the options available to the natural person to decline communications (paragraph 5).

b. The system introduced is the opt-in system with relatively detailed explanations given to the customers and a reduced number of options for the trader. The language used is more detailed and more precise than that in the ePrivacy Directive, although the spirit is followed. The main principle is that consumers must opt in.

2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.
For electronic mail, automated calling systems or facsimile machine, as per Article 6 of the Marketing Practices Act, the requirements are different than the Directive, depending on three situations: - Marketing is allowed where the user requests it (or has in the past for some other product or service in the same company) - Marketing is allowed where the user is not on the opt-out list and initiates the transaction and the marketing is not by email, fax or auto-calling systems - Marketing is forbidden for users on the opt-out list This is a more precise definition than the one provided in the Directive, but it is fully within what Article 13(3) allows.

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?
Yes, pursuant to Article 6 of the Marketing Practices Act, a) where the consumer had already contacted the seller in case of a previous transaction and b) where the consumer initiates the transaction.

4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.
The law applies to all methods of unsolicited communication, without discrimination, i.e. it is technology neutral. The specific opt-in regime, however, is only in force for emails, auto-calling machines and faxes. The other methods are under a strict opt-out in the sense that a placing of a name on the Register will always have the result of prohibiting unsolicited communication, in respect of any method. No other distinction is made in the law.

5. Please describe and give references to any form of 'guidance' on the interpretation and/or application on rules on 'unsolicited direct marketing communications' provided by: **a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)** **b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?**
a. Unlike general provision of electronic services and cookies, there are no official guidelines, other than those provided on the internet. These guidelines are provided on the website of the Consumer Ombudsman: http://www.forbrugerombudsmanden.dk/Sager-og-praksis/Markedsfoeringsloven/Markedsfoeringsloven-i-praksis, English version on http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act. The Ombudsman also provides other guides on the same page, such as information on how to lodge a complaint: http://www.consumerombudsman.dk/About-us/complaintprocedure. The information is clear and detailed but is geared towards non-experts. b. No case-law exists in this area.

6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
The rules are clear, well-written and effective. The number of complaints to the authorities over unsolicited advertising is low and the awareness of the rules and their effect both in the general population and on providers is high. Of the different areas addressed in the ePrivacy Directive, this is probably the most effective one.