

## **NEW EXECUTIVE ORDER ON COOKIES HAS COME INTO FORCE**

14 December 2011, the Ministry of Business and Growth Denmark's executive order no. 1148 of 9 December 2011 on the requirement for information and consent at the storage of or the access to information on the end user's terminal equipment (the "Executive Order on Cookies") came into force. The executive order has been issued in accordance with the Danish Telecommunications Act which was revised in May 2011.

The most significant aspects of the new rules is that the user must be thoroughly informed on the use of cookies, and that the user in principle must give his consent before already saved cookies are saved or read on the user's equipment. This may imply challenges for website owners, especially for harmless session cookies which are automatically deleted when a user closes a browser window.

### **Purpose**

The purpose of the Executive Order on Cookies is to protect the end user against wrongful storage of information or against the gaining of access to information which is already stored in the terminal equipment of the end user, i.e. computers, smartphones or tablet PCs, cf. Section 1 of the Executive Order.

Normally, cookies are "passive" files stored and accessed on the user's terminal equipment without interacting or manipulating with equipment or information. Service providers or other who store or access cookies may identify users across the users' individual visits to a service and therefore gather knowledge of the users' conduct and preferences. The use of cookies is very common and serves a number of different purposes, i.e. the development of more user-friendly services, personalisation, generation of anal-

yses on the use of a particular website, targeting marketing on individual users based on their conduct.

As a consequence of the rules of the executive order, the end users' terminal equipment is considered a part of their private sphere which is to be protected against unlawful entry.

### **Application**

Within the EU, the laws of the country in which the provider of a service is established apply, and if the provider is established in Denmark, the rules of the executive order apply.

If the provider is established *outside the EU*, the laws of the country where the storage of or the access to information in a user's terminal equipment apply. Therefore, an American website, if it has users in different EU countries, will have to meet the requirements in all of these EU countries. When for example Google or Facebook is established in the EU (i.e. Ireland), the Irish rules will apply with regards to cookies from their websites.

The executive order covers all who store or gain access to information in an end user's terminal equipment.

A provider of a service is equally covered by the executive order's rules in connection with a *third party's* storage of or access to information in an end user's terminal equipment if this takes place through the provider's service (for example through an embedded code).

The service provider must not personally handle the practical and technical compliance with the rules of the executive order. These may be assigned to a third party, but not with regards to the responsibility for the compliance with the rules.

The executive order only applies to the actions consisting in storage of or access to already stored information in an end user's terminal. Therefore, actions taking place before or after the storage of or access to information are not covered by the provisions in the executive order.

The executive order covers any type of *information* which is stored or accessed in the end user's terminal equipment. Therefore, no distinction is made between general information and person-related information. Furthermore, it is irrelevant if the information is semantically meaningful, unintelligible lines of texts, codes or if the information is encrypted.

### **Requirement for consent and adequate information**

The executive order introduces a requirement that physical or legal persons may not store information or obtain access to information which is already stored in an end user's terminal equipment or let third parties store information or obtain access to information if the user has not given his *consent* hereto after having received *adequate information* on the storage of or access to information, cf. Section 3(1) of the executive order.

From Section 3(2), no. 1-5, the specific requirements, which as a minimum must be fulfilled before the information may be described as adequate, appear. Among other things, the executive order makes demands as to the character, purpose, contents and accessibility of the information, including with regards to who stores the cookie, to whom complaints may be made to and to how long the cookie is stored. The information must constitute a knowledge basis which must make the individual user capable of making an actual informed choice.

Consent must be a voluntary, specific and informed indication of will, in which a user agrees to the storage of or access to information in the end user's terminal equipment. The consent being specific implies that a provider may not obtain a broad consent for cookies in general and to broadly defined purposes, but that the consent must be precise and limited.

The requirement for consent is to ensure that the users have actual control of whether information is stored on or accessed from their terminal equipment. For example, an indication of will may be carried out by checking a box, clicking a button, filling out a form or by active use of a service where the user is expected to be aware that storage of or access to information will take place.

### **Exceptions to the requirement for consent**

The requirement for consent is dispensed with where:

- (i) the storage of or access to the information *only* takes place with the purpose of transferring communication through an electronical communications network,
- (ii) the storage of or access to the information is *required* to make the provider of an information society service, which the end user *explicitly* has requested, able to deliver this service, cf. Section 4(1) of the executive order or where

- (iii) it is aimed at providers of internet connections and the storage of or access to the information on the terminal equipment of the end users which may take place at the connection to the internet or the maintenance thereof.

The storage of or access to information in accordance with (ii) is *required* if the storage of or access to the information is a technical condition in order to deliver a service which functions in accordance with the purpose of the service, cf. (2).

The exception in Section 4 (1) no. 1, cf. (2) will, for example, apply in connection with the use of electronic shopping baskets on web shops where it is necessary to recognise the user across page changes, as the shopping basket would otherwise be empty when new pages are displayed. However, the exception does for example not apply to cookies for web statistics or other analyses of the users' conduct on a service.

#### **Breach of the requirement for consent**

Compliance with the rules of the executive order is monitored by the Danish telecommunications authority, cf. Section 20 of the Danish Telecommunications Act (formerly the Danish IT and Telecom Agency and from 1 January 2012, presumably the Commerce Agency (Erhvervsstyrelsen), however, without being subject to directions from the Minister for Business and Growth).

Breach of the rules of the executive order is punishable. In general, a breach will be punished with a fine, cf. Section 5(1). Furthermore, legal persons may be held criminally liable in accordance with the rules of chapter 5, cf. Section 5(2) of the Danish Penal Code.

#### **Implementation of EU directive**

With the coming into force of the executive order, article 5(3) of the Data Protection Directive was implemented, according to which, member states are obligated to ensure that the use of electronic communication networks with a view to storing or obtaining access to information stored in the terminal equipment of a subscriber or a user is only allowed on the condition that the subscriber or the user receives clear and adequate information, among other things with regard to the purpose of the process.

The executive order may be found here (in Danish):

<https://www.retsinformation.dk/Forms/R0710.aspx?id=139279>

The telecommunication authority's guide to the executive order may be found here (in Danish):

<http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-til-oplysninger-pa-andres-udstyr/vejledning.pdf>

If you have any questions or require additional information on the executive order, please contact partner Christoffer Galbo ([cga@mwblaw.dk](mailto:cga@mwblaw.dk)), Attorney Henrik Syskind Pedersen ([hsp@mwblaw.dk](mailto:hsp@mwblaw.dk)) or junior associate Sofie-Amalie Gregaard Brandi ([sab@mwblaw.dk](mailto:sab@mwblaw.dk)).

*The above does not constitute legal counselling and Moalem Weitemeyer Bendtsen does not warrant the accuracy of the information. With the above text, Moalem Weitemeyer Bendtsen has not assumed responsibility of any kind as a consequence of a reader's use of the above as a basis of decisions or considerations.*