ERHVERVSSTYRELSEN

Guidelines on Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment ("Cookie Order")

2nd version, April 2013

Preface

This is an updated version of the current Guidelines on Executive Order No. 1148 of 9 December 2011 on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment, referred to in the following as the Cookie Order. The Guidelines were originally issued together with the Executive Order when this came into force in December 2011. The Executive Order implements the e-Privacy Directive, which introduces requirements for informed consent by the user of a network service to storing of cookies.

The Cookie Order has got its name after the small text files regulated by the Order and stored on a user's computer or other electronic equipment via the internet etc. Cookies enable recognition of the computer or equipment in connection with the user's navigation in the digital world.

Since the Cookie Order came into force, the rules have been widely debated; both companies and public authorities have pointed out a lack of clarity and considerable technical challenges in observing the EU rules in practice. The purpose of the present updated Guidelines is therefore to help companies and public authorities in getting started and to present a more practical approach to how the rules can be observed.

The updated Guidelines do not change anything in the interpretation of essential requirements for information and consent in relation to cookies and similar technologies, but contain clarifications, especially in connection with the following:

- An introductory text about cookies and their characteristics
- Responsibility for third party cookies
- Examples of the accessibility of information
- What cookies are exempted from the requirement for information and consent
- The Danish Business Authority's supervision of the rules

In addition, the update contains several practical examples and a Technical Guide for companies and public authorities, with inspiration for practical implementation of the cookie rules on Danish websites.

The associated Technical Guide should be seen as an invitation to companies to carry out a more detailed analysis of how their websites use cookies and similar technologies, and to categorise cookies on the basis of their various characteristics. Current Danish legislation includes all types of cookies, but a categorisation of these may be useful for website managers to define the purpose of various cookies employed by the website, thus ensuring that comprehensive information is given to the user. Furthermore, the nature of the cookie may be significant for assessing the requirement for information and consent, taking into account the impact of the cookie in relation to the user's privacy.

The Danish Business Authority is in close dialogue with the Commission and other EU member states to ensure a uniform approach to regulation, which, as mentioned

before, is based on Community law[1]. Thus it is considered important that the Danish interpretation and enforcement of the rules are in line with the views of the Commission and other member states. Our dialogue with the Commission and other member states will continue for the purpose of discussing the rules and the enforcement of these, also in the light of technological developments. In addition, discussions of the Directive are followed up by a forum known as the Article 29 Working Party, which was set up in accordance with the general data protection rules of the EU Data Protection Directive[2]. In this connection, the present Guidelines will be updated to the extent required.

Our dialogue with the Commission and the other member countries shows a broad consensus on how to interpret the EU rules on consent, but in practice some countries enforce the consent requirement in such a way that it is accepted in special cases that cookies may be stored prior to the user having consented to this. Further clarification from the Commission is needed in relation to this practice. Until such clarification is available, the Danish Business Authority will not be enforcing the requirement for prior consent. In its supervision of the rules, the Agency will instead put emphasis on the website owner's efforts to ensure comprehensive information to the user about the website's use of cookies, and the user's ability to accept or refuse cookies.

Danish Business Authority
April 2013

[1]Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC.
[2]Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

1. Introduction

The present Guidelines support the rules of the Cookie Order, under which websites that make use of technologies to store or read information on a user's computer or other IT equipment (known as cookies) are required to obtain the website user's consent before making use of the technology.

The Cookie Order, which came into force on 14 December 2011, implements the e-Privacy Directive[3] as amended most recently in 2009[4], when the requirement for consent was introduced.

The rules have been introduced to increase the protection of privacy when we move into the digital world. Cookies collect data on the user of digital services by accessing the user's computer or other terminal equipment considered to be part of the user's private sphere. The collection of data via cookies makes it possible to recognise the user's computer and follow the user's navigation on the network.

The cookie rules should be read in the light of the rules on protection of personal data where the rules regulate collection of data in a broader sense, not considering whether such information may be used to identify a person.

Companies and public authorities are increasingly making use of the digital platform on the internet, exploiting the possibilities of easier access to customers and users here than in the physical world. At the same time they are challenged by the elusiveness of users on the network and the lack of personal relations in the digital world. The use of technologies such as cookies makes it possible to create relations, with better user experiences and targeted services. Cookies may thus be a great help to the user, for example in case of repeated visits to websites, where settings and data entered by the user are remembered by means of cookies and need not be entered again. Cookies may also be used for tracking the user's navigation on a specific website or across websites, providing a basis for statistics and targeted advertising and services etc. from the website owner itself, or from third parties, e.g. providers of web statistics modules, advertising or media agencies. Cookies contribute to strengthening innovation and development in the digital market.

So the aim of the rules is not to prohibit the use of cookies, but rather to increase the transparency of the processes that support user navigation on the internet, based on data collected from the user, while also ensuring that the user remains in control of the purpose for which such data is used. The rules place emphasis on allowing the individual user to have a real option of choosing or rejecting the storing of cookies. This will ensure confidence in the internet, which is also a decisive factor in the continued development of the digital market.

Cookies are usually passive files that can be stored or accessed in the users' terminal equipment but cannot interact with or manipulate equipment or information.

---

[3]Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[4]Directive 2009/136/EC of the European Parliament and of the Council.

However, as mentioned previously, the knowledge collected via cookies or similar technologies can be used for a wide variety of purposes, e.g. personalisation and development of more user-friendly services, generating analyses about the use of a website or targeting behavioural marketing at the user. Depending on the individual user's personal attitudes, such purposes may be more or less desirable.

Another point is that cookies can be, and often are, set by parties other than the website itself, which is not always obvious to the user and may make it difficult for the user to determine the real purpose. Here it is especially important to ensure that the user is aware that cookies may be passed on from one website to another, tracking the user's navigation on the network. At the same time, it is important that the website owner itself may control what cookies are set and who gains access to the user's data via the website. If the website owner does not have such control, it will be very difficult or impossible to obtain the user's real and informed consent, and there may also be a risk that other stakeholders misuse the user's data or exploit data contrary to the website owner's own interests.

In the light of the various characteristics of cookies and the use of these, which are constantly changing in line with technological developments and the growing digital market, it is necessary to strengthen general information to users in order to meet the purpose of current regulation, under which it is for the users to decide, on an informed basis, whether they will allow access to information.

An analysis made by the Danish E-commerce Association (FDIH)[5] shows that knowledge of cookies is increasing among consumers and that two out of every three consumers know what a cookie is. Those who know about cookies are predominantly senior consumers. In addition, the analysis shows that one half of those who answer yes to knowledge of cookies have also been changing their browser settings actively in order to prevent or limit the acceptance of cookies. However, in the group who answered no to knowledge of cookies, primarily consisting of younger internet users, more than two thirds deny having plans to change their browser settings in the future to prevent or limit the acceptance of cookies.

The analysis shows that there is a great difference in how users feel about cookies and in their attitude as to whether cookies are something you have to live with or something to be avoided. But the increasing user awareness in relation to cookies and the use of cookies is a factor that should be taken into account both by companies and public authorities.

The present Guidelines explain the rules of the Cookie Order, particularly the essential requirements for information and consent, and suggest practical solutions to website owners. The complexity and diversity of digital services today imply that it is neither possible nor desirable to describe in detail how the rules are to be complied with, but together with these Guidelines the Cookie Order defines a framework or range of options within which service providers may find inspiration for solutions that match their specific context. New innovative and user-friendly solutions that increase transparency and control for the users can best be created by the service providers themselves. So the examples included in these Guidelines and in the Technical Guide

[5]FDIH's E-commerce Analysis from 2012.

for companies should be seen merely as examples and not prescriptions for final solutions.

Website owners established in countries other than Denmark should remember that it may not be enough for them to organise their solutions merely under Danish legislation, see the section "Where are specific rules applicable" in these Guidelines. The Danish cookie rules are based on harmonised Community law, but this only sets minimum requirements in connection with the use of cookies and similar technologies. In Denmark, the rules have been implemented in close conformity with the text of the Directive, and no stricter rules have been introduced.

The Guidelines reflect the Danish Business Authority's supervision of the cookie rules, focusing on the efforts of website owners to comply with the rules and create transparency for their users on the network. In the light of the underlying protective considerations, the Danish Business Authority's supervision will focus on what types of cookies are used and their effect in relation to the user's privacy, as well as efforts to ensure control over the website. The Danish Business Authority will measure the efforts of the website on the basis of the five process steps given in the Technical Guide, see chapter 6 of the Guidelines.

2. Rules

Background

The revision of the European telecommunications directives in 2008/2009 introduced an amendment to Article 5(3) of the e-Privacy Directive on the storing of or access to information in users' terminal equipment, e.g. computers, smartphones or tablets. The amendment is notably about a requirement for obtaining consent from the users in connection with the storing of or access to information in the user's terminal equipment.

Article 5(3) of the e-Privacy Directive contains a reference to the Data Protection Directive[6] and should therefore be read together with the general rules on protection of personal data as implemented in Danish law in the Act on Processing of Personal Data[7]. The Act on Processing of Personal Data lays down general requirements in connection with the processing of personally identifiable information.

The amendment to the e-Privacy Directive was introduced to increase protection of the users' private sphere when navigating in a digital world, which was not believed to have been met to a sufficient extent by the rules on protection of personal data or the previous article of the e-Privacy Directive. In addition, the protection of privacy is supported by the Charter of Fundamental Rights of the European Union, which was made legally binding when the Treaty of Lisbon came into effect.

Cookie Order

The amendment to the e-Privacy Directive has been implemented in Danish law under Executive Order No. 1148 of 9 December 2011 on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment (known as the Cookie Order), issued pursuant to section 9 and section 81(2) of Act No. 169 of 3 March 2011 on Electronic Communications Networks and Services.

Purpose and scope

What do the rules protect?
The purpose of the rules is to protect the private sphere of the users. The rules are based on the view that the users' terminal equipment is part of the user's private sphere, which should be protected against unwarranted intrusion.

Terminal equipment means computers and mobile units such as smartphones, tablets etc., in which information can be stored or already stored information be accessed.

The protected person is the user of an electronic communications network or service who does not make such electronic communications networks or services available to other parties on a commercial basis, i.e. all users of a computer or a mobile unit.

[6]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[7]Act No. 429 of 31 May 2000 on Processing of Personal Data.

The protection is associated with the terminal equipment, which, as mentioned above, is regarded as being part of the owner's private sphere.

The rules apply exclusively to publicly available communications networks or services and not to company intranets and similar closed user groups. But the fact that a login is required to get access to a network does not in itself mean that a closed user group is involved where the cookie rules do not apply. This will depend on a specific assessment.

The rules do not take account of cases with several users of the same terminal equipment. Users should be aware that if they lend a computer, tablet, mobile telephone etc. to others or if they use someone else's terminal equipment, then they accept the settings of the equipment, including acceptance of cookies and similar technologies. If the user of the terminal equipment wants to protect against this, it will be subject to agreement between the owner/borrower of the equipment.

This also applies to the extent that a publicly available computer is used, for instance at a library, since a user cannot in general guard against the settings of earlier users. It is the Danish Business Authority's assessment that such use does not come within the protection objective of the cookie rules in relation to the user's private sphere. It is not the responsibility of the website owners to obtain the consent of all users or arrange their websites on the assumption that the site may be accessed from a publicly available computer.

What technologies are covered?
The Cookie Order does not give a specific definition of the technologies regulated by the Order other than the specific description given in section 3(1).

The rules are neutral in terms of technology. The Cookie Order extends beyond storing of or access to information in the users' terminal equipment in connection with internet access: it also includes storing of or access to information from external media such as USB keys, CDs, CD-ROMs, external hard disks etc.

As for the form, type or standard used for storing the information, the Cookie Order covers not only "classic" http cookies, but similar technologies of any type, including Flash cookies (Local Shared Objects), Web Storage (HTML5), Java scripts or cookies set when using Microsoft Silverlight.

Cookies may have different life spans: they may stop at the end of a browser session (i.e. from the moment when the user opens a browser window until this is closed again), or they may last for a longer time and cover several browser sessions, being able to track the user's movements on the internet.

Cookies may also be divided into first party cookies and third party cookies, according to the party placing the cookie on the website.

First party cookies are those placed by the owner of the website, who is the party that the user is interacting with in the first place. Third party cookies are those placed on a

website by a third party, where the third party or others get access to the data collected.

		First party	**Third party**	
		Cookies set by the website visited by the user, the website address appearing from the URL window	Cookies set by parties other than the website visited by the user	
Session cookies	Stopping either during or at the end of a browser session	Examples: • Control of graphics • Visit statistics • User setting • Shopping basket • Payment module • Security procedures for online banking	Examples: : • Statistics • Where a third party provides services as described under the examples of first party cookies, it is essential, in determining if a third party cookie is involved, who has access to the user's data	Both for first and third party cookies, session cookies are often considered to be less intrusive in relation to the user's privacy
Persistent cookies	Lasting for several browser sessions and can follow the user around the network. May last from hours to several years	Examples: • Remembering user settings such as name, address, language and log-in the next time the user visits the website beyond a browser session • Tracking - either recognising users from previous visits or following the user to other websites	Examples: • Tracking	First party cookies for user setting. Considered to be less intrusive in relation to the user's privacy. Tracking cookies - both from first parties and third parties are considered to be more intrusive in relation to the user's private sphere

In relation to the requirement for information and consent, Danish legislation does not distinguish between the various types of cookies, but includes all cookies irrespective of their life span and origin.

As mentioned below, the nature of a cookie may in practice play a part in determining whether the requirement for information and consent has been met, because it is decisive here that the user knows about the function of the cookie, including who is behind the cookie and who gets access from there to collected data.

What actions are covered?

The Cookie Order is only concerned with the action consisting in storing of or access to already stored information in a user's terminal equipment. Actions taking place before or after storing of or access to information in a user's terminal equipment do

not fall within the rules of the Cookie Order. Such actions may instead be covered by the general provisions on protection of personal data.

The following table gives an overview of interfaces between the Cookie Order and the Act on Processing of Personal Data.

Table 1: Areas of application for the Cookie Order and the Act on Processing of Personal Data

	Cookie Order	**Act on Processing of Personal Data**
Protection object:	User's terminal equipment, to be understood as part of the private sphere.	Personal data (not only in terminal equipment).
Types of information included:	All information, without distinction.	In principle only personal data. But information about companies etc. is included in special cases.
Processing operations included:	Storing of or access to information in a user's terminal equipment.	Any processing of personal data within the scope of the Act where other legislation does not contain special rules to be applied instead.
Criteria for processing: (processing authorised)	General rule: Comprehensive information to and consent from the user. Exemption: Section 4 of the Order.	Explicit consent is merely one of several processing criteria.

There is an overlap between the Cookie Order and the Act on Processing of Personal Data with regard to the storing of or access to already stored information in a user's terminal equipment when the information collected is personal data. Here the requirement for informed consent in the cookie rules gives better protection of the user than the rules on protection of personal data, which include a number of situations in which informed consent is not necessary.

In relation to the storing of and access to already stored information which is personal data, in terminal equipment, the Cookie Order will thus rank before the Act on Processing of Personal Data, see section 2 of the Act.

In practice it may happen, however, that there is also other processing of information in addition to storing of or access to already stored information in a user's terminal equipment.

For example when processing operations are transmitted to, collected or further processed on a server. Such processing operations are performed outside the users' terminal equipment and do not fall within the cookie rules. Depending on the specific circumstances, the rules of the Act on Processing of Personal Data might be applicable here.

What information is covered?
The Cookie Order applies to any type of information collected or stored in the user's terminal equipment.

The cookie rules regulate the *means* for collection of data. No distinction is made here between personal and non-personal information.

Nor is it significant whether the information is semantically meaningful, unintelligible text strings, code or whether the information is encrypted.

Example: Storing of or access to already stored information for the use of web statistics

A provider of a website wants to conduct an analysis of how website visitors use the site with a view to improving user experience. For this purpose the provider of the website wants to place cookies in the users' terminal equipment.

The service provider is governed by the requirements of the Cookie Order for information and consent as regards the storing of cookies, and any later access to these cookies in the users' terminal equipment.

If the service provider subsequently wants to analyse the information collected by means of the cookies, such processing falls outside the scope of the Cookie Order. This applies for instance to further processing of the information by the service provider for the purpose of preparing statistics.

Who are governed by the rules?
All parties that store or gain access to information in users' terminal equipment are governed by the rules (see also the section below on where specific rules are applicable).

Websites that address everyone or exclusively companies will thus be governed by the rules in case cookies or similar technologies are used on the site, as websites may basically be accessed by everyone.

The owner of a website is also obliged under the rules in connection with storing of or access to information in users' terminal equipment by third parties if this is done via the provider's service, for example by means of embedded code, in banner advertising, software applications or links.

The owner of the website need not itself be in charge of practical and technical observance of the rules (information and obtaining the consent of a user), but may agree that a third party should handle this on behalf of the service provider. However, the responsibility for compliance with the rules will always lie with the provider of a service no matter what that party might have agreed with a third party, since it is not allowed under the Cookie Order to *let a third party store information or gain access to already stored information* without information to and consent from the end-user.

Under the cookie rules, there is no requirement for concluding a data processing agreement, as is stipulated under the Act on Processing of Personal Data, but it might be expedient where access is allowed for a third party to collect data via one's website to make a written agreement in order to clarify the purposes for which a third party is collecting data on the users, as this purpose must be covered by the information on the website in order for consent by the user to be regarded as being real and comprehensive, see below under the section "Requirement for informed consent".

In case the services of other parties are embedded on an owner's website, for example services obtained via the internet, the agreement with a third party will most often depend on unilateral acceptance of the third party's given business conditions without any opportunity being offered to negotiate contract terms. It should be noted that it may be difficult here to control the third party's use of data collected via cookies or similar technologies, and hence also difficult in the last resort to ensure the user's real and informed consent.

Example: Embedding a comment module on a website

A major news medium wants to embed a module that enables users of its website to comment on the content of the site. For this purpose, the news medium contacts the provider of a comment module that can be embedded on websites. The news medium and the provider agree that the module should be embedded on all the news medium's sites.

The provider of the comment module wants to set cookies in the users' terminal equipment when the users access a website in order to see how much the module is being used. The news medium therefore agrees with the provider of the comment module that the provider should ensure that the rules on storing of or access to information in users' terminal equipment are observed by giving the users comprehensive information and obtaining their consent.

However, the news medium is responsible for the rules being observed in practice and hence for ensuring that no unwarranted storing is made in the users' terminal equipment when these access the website of the news medium, irrespective of what the news medium might have agreed with the provider of the comment module. So this will also apply in case the provider of the comment module is using cookies for purposes other than those allowed by the agreement and communicated to the user.

The owner of a website is responsible for the cookies and similar technologies set in connection with a user's visit on the website.

If the website is linking to other websites or if "share" bars or "like" buttons are used for services such as Facebook or Twitter, it is important to note whether these websites set cookies via links, share bars or like buttons already before the user is linked over to the new website, as it is the website owner, as mentioned above, who is ultimately responsible for the cookies set on their website. Once linking over has taken place via the share bar, the responsibility will pass to the owner of the new website.

It is not required under the cookie rules, but it is recommended to inform the user that the website is being exited and that the sites to which access is provided may be using cookies.

In connection with the establishment of digital platforms used for accessing other websites that appear in the frame of the digital platform, e.g. the Danish Business Authority's business portal "Virk.dk", or "Borger.dk", a citizen portal set up by the Danish Agency for Digitisation, it will be the owner of the individual website accessed via the platform who is responsible for observance of the cookie rules on these websites. The owners of a platform are responsible for cookies set by them.

The same will apply when websites are set up via social media such as Facebook. The social medium will be responsible for the cookies set by the medium, but not for the cookies set by the owner of the website set up in the format of the social medium.

The deciding factor in determining who is responsible for obtaining consent to the use of cookies on a website depends on who has control over the content on the website.

Where are specific rules applicable?
Website owners established in countries other than Denmark should remember that it may not be enough for them to organise their solutions merely to match Danish legislation. The Danish cookie rules are based on harmonised Community law, but this only sets minimum requirements in connection with the use of cookies and similar technologies.

The e-Privacy Directive does not take a position on the geographic scope of the rules, but the European Commission has indicated that within the EU the legislation of the country in which the provider of a service is established will be applicable. In Denmark, our views are essentially parallel to the Commission's interpretation, which follows the "originating country principle" in the E-Commerce Directive[8].

If the provider of a service established in Denmark stores or gains access to information in a user's terminal equipment, the service provider will thus be liable under Danish rules. The Danish rules will also be applicable if the provider of a service established in Denmark lets a third party established in another country store or gain access to information in a user's terminal equipment via the provider's service.

According to the Commission, the provider of a service established *outside the EU* will be subject to the legislation in the country where storing of or access to information in a user's terminal equipment takes place. In its supervision of the rules, the Danish Business Authority will focus on whether the website is addressing Danish consumers in accordance with the jurisdictional principles of international law as to where an action has effect. Emphasis will thus be placed on a number of factors such as language, terms of delivery (e.g. a webshop where delivery can be made to Denmark) etc.

[8]Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Requirement for informed consent

The key point in the amendment to the e-Privacy Directive in 2009 is the requirement for obtaining informed consent prior to placing cookies, which has also been transposed to the Danish rules in section 3 of the Cookie Order.

The Cookie Order contains a definition of consent based on the consent definition in the Data Protection Directive to which the Cookie Directive refers. The same applies to the content of the duty to give information which is also further described in the Data Protection Directive.

The requirements for information and consent should be seen as two complementary elements that support one another and cannot be separated since they have been introduced to ensure that the users can make a real and informed choice about tracking of their navigation on the internet. Consequently, if the information is not comprehensive, the consent will not be a real consent.

In the following, the requirements for information and consent have been dealt with in further detail. A number of practical examples are given and several more follow from the Technical Guide included in the last section of these Guidelines. The examples are merely offered for inspiration as it will still be for the individual website owners to assess how the requirements can best be complied with on precisely their service.

Section 3 of the Cookie Order

3.-(1) 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 thereto, having been provided with comprehensive information about the storing of, or access to, the information.
(2) Information, cf. subsection (1), shall be comprehensive if it meets the following minimum requirements:
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 can 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 accessible at all times for the end-user on the information and content service in question.

Information requirement

What requirements are made for comprehensive information?

Section 3(2) of the Cookie Order lists the requirements that must be met as a *minimum* before the information can be described as comprehensive. Requirements are made for the **character, content and availability of the information**.

Overall, the information is to serve as the knowledge basis that enables the users to make actual informed choices. In some cases it should therefore be considered to include information in addition to what is required under the Cookie Order if this is necessary to enable the users to understand the consequences of their choice.

Solutions must comply with the cookie rules both on websites and on mobile sites - see also the Technical Guide in chapter 6 of the Guidelines.

Requirements for language and text

Section 3(2), no. 1, requires the information to appear *in a clear, precise and easily understood language or similar picture writing*.

This implies that the information should not be given in unnecessary technical or legal terms, and that the user can easily assess the information.

The use of tables or pictorial language, e.g. pictograms, can supplement or replace more traditional text and make the information easier to understand, but must be evaluated on the basis of the user's knowledge of such alternatives.

It is not specified in what language the information should be given. But the language should be chosen with due regard for the users addressed by a service, including in particular the geographic location of these users.

Requirement for information about purpose

Section 3(2), no. 2, requires the information to contain *details of the purpose of the storing of, or access to, information in the end-user's terminal equipment*.

The user is entitled to be informed why information is stored or being accessed and it is not sufficient merely to advise that this is done. This requirement is bound up with the requirement for consent, which must be a *specific* indication of the user's wishes. So an indication like "we use cookies" without further clarification is not considered to comply with the rules.

Information about the purpose of storing or accessing information is essential and should serve to ensure that users are aware of the consequences of their choice. As a result, the purpose should always be described in precise and adequate terms.

If the storing of or access to information has more than one purpose, all purposes should be explained. If several pieces of information are stored or accessed for the

same purpose or on several occasions, it will usually be sufficient to describe the purpose once and not for each piece of information stored or accessed.

In relation to the required indication of purpose, it is important to emphasise here that the description must also include the purpose of any third parties in using cookies.

Example: Information about the purpose of using cookies

The use of cookies is very widespread and may have a variety of purposes, for instance optimising the user experience or design of a service, generating web statistics, or targeting marketing activities at the users.

The information given should describe the purpose of using cookies on the service and not the specific cookies as such.

If for instance a service is using four cookies for optimising the design of the service, while another two cookies are used for handling advertisements and a seventh cookie is used for generating web statistics, it will normally be sufficient to give information about the three different purposes of using cookies and not necessarily about all of the seven cookies employed by the site.

Information identifying who is setting cookies

Section 3(2), no. 3, requires the information to contain *details that identify any natural or legal person arranging the storing of, or access to, the information.*

Users must be able to identify the party arranging the storing. In many cases this will be the provider of the service, but where the provider of a service lets a third party store or gain access to information in a user's terminal equipment via the provider's service, it must also be possible for the user to identify that third party. The exact indication of the third parties that set cookies may be given on a subpage, see the section of the Guidelines below on layered information.

As for information stored or being accessed in users' terminal equipment by an organisation, e.g. a company or another legal person, the information to be indicated must identify the organisation and not its employees.

What specific information must be available for users to identify the person(s) undertaking the storing will vary from service to service and depend on the parties involved.

Right to refuse cookies

Section 3(2), no. 4, requires the information to contain *a readily accessible means by which the end-user can 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.*

Users must be able to refuse consent or withdraw a consent already given. This is intended to support real user control and the voluntary basis of the user's consent. For this purpose there must be a readily accessible means by which to refuse cookies and clear, precise and easily understood guidance on how users should make use of this. See also below under the section "Requirement for consent", where it is pointed out that there is no requirement for a website to be accessible or function without cookies.

In some cases it may be relevant to refer to guidance and tools prepared by others. It is not required in the Cookie Order that guidance or tools for refusing or withdrawing consent should be available on the service that stores or gains access to information. What the service has to make readily accessible to the user is the access to guidance and tools.

Requirement for availability of information

Section 3(2), no. 5, *requires the information to be 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 accessible at all times for the end-user on the information and content service in question.*

To ensure real user control, it is necessary for the information to be immediately available to the users and easy to access. It is also a condition that users can withdraw a consent already given. How the information is best made available will depend on factors such as the design and structure of the service, for which reason it will vary from service to service.

Information may be layered

It may be expedient to make use of layered information, but it must be ensured that the users get information on essentials at once, such as the purpose of using cookies, at the same time being linked to more detailed information. The use of pictograms or other clearly marked entries to the information may support this, but cannot serve as immediately available information alone.

The initial indication of the purpose of using cookies should include information on third party cookies, as the party receiving the data is of significance for the user. For example, if purposes such as direct marketing are indicated, it must also appear that direct marketing will be from a third party. The precise indication of third parties may be given on a subpage.

In addition, a service may distinguish between how the information is presented to the users *before* the users give or refuse consent, and how the information is presented *after* the users have given or refused consent.

On information and content services, including websites and other online services that store or access information in a user's terminal equipment, the information must remain available to users via direct and clearly marked access on the information and content service in question.

This implies that users employing such services must have access at any time to the information, and that such access should be easy to find and use. It may be considered to meet the requirement by placing such access within the context of other permanent elements on a service. The use of pictograms or similar features may also be considered in this context.

The requirement for consent is discussed in further detail below. As can be seen, consent may be given in different ways, including also by an active action. The requirement for information may vary in terms of explicitness and availability, according to the form of consent involved. However, the requirement as to what information must be given for the information to be considered comprehensive does not vary.

Essential information to be given to the user at once is:

- All purposes of cookies and similar technologies

- Who is using cookies and similar technologies on the website

Example: Comprehensive information - layered with essential information first

A service on the network offering the user the possibility of comparing products and prices for various categories of goods is using cookies to register the number of users on the website and to register where the user comes from. On the website there are banner ads for various manufacturers related to the product categories mentioned on the website. The banner ads are provided by third parties and use cookies for registering the ads that are clicked on by the user, thus making it possible to identify the users' interests and target the advertising.

Example: Initial information to the user:

*"We use cookies for statistics and for targeted marketing from ourselves and our advertisers - **see details here**. **Read more here** about our use of cookies, including how to opt out of the use of cookies."*

Requirement for consent

As mentioned above, the most important change in the rules is the requirement for obtaining informed consent from the user when using cookies or similar technologies, as stated in section 3 of the Cookie Order.

Consent is defined in section 2(1), no. 8, of the Cookie Order:

Section 2(1), no. 8, of the Cookie Order

2(1), no. 8, Consent: ***Any freely given, specific and informed indication of the end-user's wishes*** *by which the end-user signifies its agreement to information being stored, or access to stored information being gained, in the end-user's terminal equipment.*

As services and their users differ widely, there will be great differences in how a consent can best be obtained.

The requirement for consent is intended to ensure that users have real control of whether information is stored or accessed in their terminal equipment. When consent is to be obtained, it is therefore essential to be mindful of the user's control options, including the user's actual ability to assess the purpose of storing or accessing information.

Basically, the rules give services a wide range of options for choosing how consent can best be obtained in a way that works well within their specific context.

That the consent must be **freely given** implies that users must have a real choice. It is not a requirement that websites should be able to function without the use of cookies or similar technologies, so refusal of cookies might imply that the user's only option is to leave the site. Obviously companies have an incentive to ensure that their website is available, but it is not unlawful to have solutions that reject users who do not want to accept the use of cookies.

For public websites there may be other considerations since access to public services is expected to be available to all.

That consent is voluntary also implies that users must have the opportunity to withdraw a consent already given, see also section 3(2), no. 4, of the Cookie Order on the requirement for information.

That the consent must be **specific** implies that the consent must be precise and well-defined. However, the consent need not be related to each individual storing of or access to information in the users' terminal equipment. Instead the consent should be linked with the purpose underlying the storing of or access to information, see also section 3(2), no. 2, of the Cookie Order on the requirement for information.

If storing of or access to information is used at a later date for purposes extending beyond what has been the subject of an earlier consent, a new consent covering the new purpose must be obtained.

That the consent must be **informed** is supported by the requirements for information in section 3(2) of the Cookie Order, where, not least, the purpose of the storing is essential. As part of an informed consent, the users should also be informed of the consequences of their choice or refusal. Such consequences might be for instance that

users cannot get access to the service or certain parts of it as described above if refusing consent, or that the consent will result in third parties being allowed to store or access already stored information in users' terminal equipment.

The **indication of the user's wishes** is a key element in obtaining the consent. A service provider must identify an active action on the part of its users that can reasonably be interpreted as an indication of their wishes on an informed basis. However, it should be emphasised that a wish can be indicated in a variety of ways, and that the rules of the Cookie Order do not take a specific position on how it should be expressed.

An indication of the user's wishes can be many things, *for example*:

- ticking a box, clicking on a button or filling in a form in connection with relevant information on a service,

- active use of a service where it must be expected that the user is informed that there will be storing of or access to information (in case this has not been refused).

The Commission has informed the Danish Business Authority that active use of a service as described above is in conformity with the e-Privacy Directive and is accepted in most member countries. The deciding factor is that an active action can be identified, for example that there are additional clicks on the page and that the users are aware that they accept cookies by this action, which means that it is not enough merely to state in general terms that the website is using cookies; it must be pointed out that cookies are set for example when the user continues to click.

The ways in which consent can best be obtained will differ widely. The individual service itself is best qualified for choosing a solution that meets the requirement for consent and offers the users of the service a real ability to express their wishes on an informed basis.

The complexity and diversity of digital services do not make it possible to define more precisely how users should express their wishes in specific cases. The requirement for consent as stated in the Cookie Order therefore allows services a wide range of options for developing new and innovative solutions that increase user control and transparency.

Example: Consent

*"We use cookies for statistics and targeted marketing from ourselves and our **advertisers**. **Accept cookies** / **Refuse cookies**. Read more **here** about our use of cookies, including how to opt out of cookies again."*

*"We use cookies for statistics and targeted marketing from ourselves and our advertisers. If you continue to click on this page, you accept that cookies are set for these purposes. **Read more here about our use of cookies, including how to opt out of the use of cookies."***

If users choose not to give their consent to information being stored or choose to withdraw consent, the Cookie Order, as mentioned above, does not require that users should still be allowed access to content on a service.

The Danish Business Authority is aware that the requirement for prior consent may be a technical challenge for some websites that set cookies already when the user accesses the site, especially to ensure statistics on how many visitors there are on a website and where they come from.

The Directive sets a basic requirement for informed consent. Some countries have chosen to enforce the consent requirement in such a way that it is accepted in certain exceptional cases that cookies may be stored before the user has consented to this. The UK points out in their guidelines on the rules that consent should as far as possible be obtained before cookies are set, but it is accepted that this is not always done. Where it is not possible to obtain consent before cookies are stored, the UK guidelines emphasise, however, that companies should make an effort to ensure information for the users and their ability to consent to/refuse cookies as early as possible, and it is also considered important that companies should limit the access to session cookies.

Further clarification from the Commission is needed in relation to this practice. Until such clarification is available, the Danish Business Authority will not be enforcing the requirement for prior consent. In its supervision with the rules, the Agency will instead put emphasis on the website owner's efforts to ensure comprehensive information to the user on the website's use of cookies, and the user's ability to accept or refuse cookies.

Consent via browser settings is not recognised in Denmark at the present time, and only in a few of the other EU member countries. The general attitude is that the browser solutions available in the market today do not protect against the use of cookies to a sufficient degree where the user has opted out of it. With the existing browsers, it is not possible to differentiate one's consent to a sufficient degree, so in reality it will either be "yes" to all cookies, or "no" to all cookies, and subsequently the user might experience considerable limitations with regard to the content of various services on the network.

Basically the consent will continue until circumstances change. The user must have easy access at all times to withdrawing the consent.

Exemptions

Section 4 of the Cookie Order contains two exemptions from the requirement for informed consent by the user prior to the use of cookies. If the purpose is collection of data that falls within the exemption rules, current legislation does not require either information or consent. However, it might be recommended also in this case to give information and obtain consent, seeing that complete transparency means increased confidence in the internet and may therefore be of advantage to an e-trader or provider of services on the network. Also here it should be assessed whether the situation might fall within the rules on protection of personal data.

Section 4 of the Cookie Order

4.-(1) Notwithstanding section 3, natural or legal persons may store information, or gain access to information already stored, in an end-user's terminal equipment if:

1) storing of or access to information is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or

2) storing of or access to information is necessary in order for the provider of an information society service explicitly requested by the end-user to provide this service.

(2) 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.

In its interpretation of the exemption rules, the Danish Business Authority is placing emphasis on the opinion of the Article 29 Working Party, mentioned in the preface, which published a document in June 2012 regarding the exemption rules of the e-Privacy Directive following the amendment in 2009. It is important to emphasise here that this is not a legally binding document, but the Working Party's interpretations are widely supported by the European Commission and broadly by member states. A link to the Article 29 Working Party's Opinion is included in chapter 5 "Links to legislation and directives".

First exemption: Cookies used when connecting to the internet

It is the Danish Business Authority's assessment that **section 4(1), no. 1**, is solely addressing internet service providers and the storing of or access to information in users' terminal equipment that might be undertaken as part of connecting to the internet and maintaining the connection.

Second exemption: Cookies ensuring the functionality of a service requested by the user

In contrast, **section 4(1), no. 2**, has a wider scope.

To fall within the exemption rule in section 4(1), no. 2, two requirements must be fulfilled. In the first place, the user must have *explicitly requested the service*. Secondly, the storing of or access to information in the user's terminal equipment must be *necessary* in order to provide this service. Both requirements must be fulfilled.

The user's navigation on the network or visit to a specific website cannot be taken as an expression of a general request for the services offered there.

Whether storing of information or access to already stored information is necessary is dealt with in further detail in **section 4(2)**, under which storing or access must be a *technical precondition* for being able to provide a service operating *in accordance with the purpose of the service*.

To be a technical precondition, the service should not be able to function without using the cookie or a similar technology. At the same time it is important that there should be a clear connection between the "necessary" technology and the user's explicit request for the service.

As for the purpose of the service, emphasis should be on the purpose for which *users* access the service or the website.

Cookies or similar technologies that fulfil the requirements for being covered by the exemption must not be used to serve other purposes. In that case the user must be informed and give its consent to such other purposes.

It is of significance in assessing whether cookies can be exempted from the requirement for informed consent to determine if they are session cookies or persistent cookies and where they come from. Persistent cookies will rarely fall within the exemption provision.

Examples of exemptions under section 4

Electronic shopping baskets

- The use of electronic shopping baskets in webshops where it is necessary to be able to recognise the user across page breaks (reloading of the webshop) as the basket would otherwise be empty when a new page is shown. Storing of a cookie or a similar technology is thus a technical precondition for being able to provide the service (e-business) that the user has explicitly requested (accessing the webshop and placing goods in the shopping basket). The shopping basket also works in accordance with the purpose (to buy goods) for which the user accesses the webshop.

Log-in situations

- The use of log-in (for example online banking, public self-service solutions or access to special networks), where cookies ensure that the user is logged in via user names/passwords and remains logged in without having to enter such codes again. It is important to emphasise that what is exempted is merely the log-in function itself, but not necessarily cookies set through activities after the log-in function.

Other exemptions:

User-defined browser settings - e.g. selection of country, language or font size.
- These cookies may be exempted from the requirement for informed consent to the extent that they are expressly activated by the user, e.g. by clicking on a button or ticking a box and are not used for other purposes and for a longer time than a browser session.

Authentification cookies
Cookies used for verifying the user's identity for access to secure websites,

User validation cookies
Cookies used for protecting against (repeated) errors on log-in.

Multimedia player cookies
Cookies used for adjusting network speed or image quality and for activating playback of video or audio files.

Plug-ins to social media
Cookies that make it possible either to share the content of a website or "like" the content via the social medium. The cookie is set merely to direct the user on to the social website and log in there. It has only significance for users of social networks who are already logged in there. If the cookie is used for tracking the user around the network, it will not be included.

Load balancing
Cookies used for allocating users to a specific server in order to balance access to a service.

It is the Danish Business Authority's assessment that cookies remembering that a user has said "no" to cookies are exempted from the requirement for informed consent since it expresses a wish by the user and is necessary in order to remember the setting.

3. Self-regulation

The complexity and diversity of digital services do not make it possible or efficient to define more precisely how the rules should be observed. Together with the present Guidelines, the Danish rules provide a framework or range of options within which service providers can work to find solutions that match their specific context.

New innovative and user-friendly solutions that increase transparency and user control can best be created by the service providers themselves. In the light of this, the European Commission has indicated that it would like to see development of self-regulation as an element in observing the rules.

Self-regulation initiated by trade organisations or other stakeholders, if established in a sensible way, has a number of advantages, e.g.

- greater flexibility and adaptability in relation to development and adjustment of solutions,
- greater practical and technical insight in the field regulated by the rules,
- broader protection of service users in relation to the minimum statutory regulations,
- increased transparency, recognisability and consistency for users of the services provided, and
- increased confidence in the services provided.

What elements should be included in self-regulation?
The European Commission has indicated that the following minimum elements should preferably be included in self-regulation of the area:

- Information and effective transparency about what happens in the user's terminal equipment.
- Obtaining consent in an appropriate form of affirmation.
- User-friendly solutions.
- Effective enforcement, including
    - easily understandable and simple complaint procedure for the users, and
    - effective sanctions.

The Cookie Order takes account of and provides scope for the European Commission's wish to develop self-regulation as an element in observing the rules.

The Danish Business Authority has been in close dialogue with several trade organisations, which have shown an interest in promoting the new rules and have worked actively to ensure adoption of serviceable cookie solutions.

4. The Danish Business Authority's supervision of the rules

The national regulatory authority in Denmark (now the Danish Business Authority) will supervise compliance with the rules of the Cookie Order, see section 20 of Act No. 169 of 3 March 2011 on Electronic Communications Networks and Services. The Danish Business Authority is not subject to instructions from the Minister for Business and Growth in handling the supervisory activities of the Authority.

Failure to observe the rules of the Cookie Order may be punishable by a fine, see section 5 of the Cookie Order.

So far, the Danish Business Authority's supervision has been based on providing information and guidance to companies and public authorities, which have experienced the change of the cookie rules as a paradigm shift breaking away from the existing structure of websites and use of the network.

The Guidelines have now been updated as an element in the Danish Business Authority's forward-looking strategy for its supervision. Here our focus will be on efforts by companies to ensure complete compliance with the rules.

In the spring of 2013, the Danish Business Authority will launch an information campaign primarily addressing companies and website owners. The campaign will support the Guidelines and supplement these with simple recommendations, for example on how to identify and analyse websites, giving practical examples of cookie solutions.

The discussion in the present Guidelines on real user control on the network and the degree of invasion from cookies will be reflected in our supervision strategy and evaluation of specific solutions.

With this aim in mind, the Danish Business Authority will be targeting its supervision of rules, focusing initially on companies and public authorities that have made little or no effort to meet the statutory requirements. In the light of the underlying protective considerations, the Danish Business Authority's supervision will focus on what types of cookies are used and their effect in relation to the user's privacy, as well as efforts to ensure control over the website. The Danish Business Authority will measure the efforts of the website on the basis of the five process steps given in the Technical Guide, see chapter 6 of the Guidelines.

As mentioned above, in its supervision of the rules the Agency will put emphasis on the website owner's efforts to ensure comprehensive information to the user on the website's use of cookies, and the user's option of accepting or refusing cookies. However, at the present time the Agency will not be focusing on whether cookies are withheld until the user has given its consent.

5. Links to legislation and directives

Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment:
http://erhvervsstyrelsen.dk/file/253401/cookie-exec-order-english-version.pdf (in English)

Directive on privacy and electronic communications (e-Privacy Directive, 2002/58/EC):
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (in English)

Directive 2009/136/EC, amending the e-Privacy Directive:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF (in English)

Act No. 169 of 3 March 2011 on Electronic Communications Networks and Services (the Telecommunications Act):
http://www.erhvervsstyrelsen.dk/file/255024/LOV-nr-169-af-03.03.2011.doc (in English)

Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive, 95/46/EC): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:da:HTML (in English)

Act on Processing of Personal Data: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ (in English)

Article 29 Data Protection Working Party: Opinion on Cookie Consent Exemption: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (in English)

6. Technical Guide

The following chapter contains a Technical Guide for companies, authorities and organisations. The Technical Guide describes five steps for compliance with the cookie rules. The five steps are solely meant as inspiration for owners of websites when auditing their website to ensure compliance with the cookie rules.

At the end of the Technical Guide, selected technical expressions have been described in more detail.

The five process steps are as follows:

1. **Identifying web property**
2. **Checking if cookies are set on the website**
3. **Giving comprehensive information**
4. **Removing unwanted, unknown and unnecessary cookies**
5. **Obtaining consent**

1st step - Identifying web property

The first step is to identify everything placed under your own website or sites, i.e. everything that makes up your web property. Danish companies and organisations have developed a great number of websites and other internet-based services for which they are legally responsible. This may typically be the company's or organisation's website on various domains with associated subdomains, product or service sites, campaign sites, etc. Most owners have purchased additional web property on a current basis, but in practice very little have been removed again from the internet. Being in control of all sites and homepages is a precondition of being able to fulfil the cookie rules.

There may be spin-off advantages in auditing your web property, as potential savings may be derived in areas such as software licences, support, infrastructure and complexity by consolidating your web property, e.g. by reducing the number of domains owned.

Check list for auditing your web property:

A. Start by making a list of the domains registered to your company, authority or organisation. An inventory may often be obtained from the IT department, marketing department or accounts department. It may be an advantage to go several years back, as domains may have been purchased for several years at a time.

   Trademarks that are no longer active should also be reviewed, as there may still be associated domains that have been overlooked.

When the complete list of your web property is ready, it may be an advantage to assess if there is consolidation potential by closing down or combining web services or domains.

B. Determine if there are mobile versions of websites.

C. Determine if there are web services/sites/facilities provided by a third party.

It is important to know which web services have been provided by bureaus, partners, suppliers or other third parties and whether they use cookies since you are directly responsible as a website owner for compliance with the cookie rules in relation to the use of cookies on your website.

Thus it should be checked what cookies are set from the content provided by your present and former business partners; what type of information is collected by their cookies; and what companies receive information from the cookies being set - both the final data owner and various data intermediaries. Data intermediaries should be understood here as any or all persons that may potentially get access to or use the information held in any of the cookies in question.

It is recommended to get information from external providers about any cookie being set by what they deliver and also to formalise the information where possible in a supplement to any existing service contract. It is essential to include the following information:

- In relation to which 'website' (not domain) have cookies been implemented (whether set directly by yourself or as part of a service you have added, purchased or included in other ways).

- For each cookie set, the following should be specified*:*
  - *Purpose of the cookie*
  - *What data the cookie is collecting*
  - *Type/category of the cookie in question*
  - *Who is the final recipient of data from the cookie*

D. Determine if there are campaign services (recruiting sites, events, etc.) which are no longer in use.
It is very common in connection with various events to set up specific websites associated with one's site. Identification of your web property should include such websites even if they are no longer in use, but are still accessible on the internet.

2nd step - Checking if cookies are set

To be able to give comprehensive information and obtain consent on an informed basis, it is necessary to get an overview of which cookies are set on all parts of your web property. In this connection, the following points should be noted:

A. Understand your application of web addresses.

B. Check each web address thoroughly and allow for the fact that cookies can be set by means of different technologies, e.g. FLASH, HMTL5 and JavaScript.
C. In relation to addresses leading elsewhere (known as redirects and forward domains), then be sure that you have checked the entire path followed by the users' browser up to the content.
D. Forms and web applications must be checked.
E. Mobile versions of websites may have very different cookies in relation to the 'ordinary' website.

Re A. Understand your application of web addresses

It is important to know precisely which content/'websites' are shown from each domain. A *domain* may control many different websites depending on how the address is written. It is therefore important to know if different content is shown depending on whether http or https is used in the address; whether 'www' (or variations thereof) is used in the address; and if mobile versions of the website are shown. The examples below are all based on the fictitious domain 'siteaddress.com' and show that the domain can direct the user to eight different *sites* (web addresses), each of which may have widely differing content and thus be setting widely differing cookies.

http://www.siteaddress.com	http://m.siteaddress.com	http://siteaddress.com
http://siteaddress.com	http://news.siteaddress.com	http://ww2.siteaddress.com
https://www.siteaddress.com	https://mobile.siteaddress.com	

Re B. Check each web address

When checking a web address, you may do it manually or by means of a software tool designed for this.

If you wish to check a web service manually, this must be based on precise knowledge about the website, its way of working, and how to use the various technologies that can set cookies.

If you have such precise knowledge, then a manual check should be structured and include the most visited pages, the pages that the users usually visit first and the pages from which the users usually leave the website. Thus it is not sufficient only to check new content being published.

If you do not have such precise knowledge, it is recommended that the entire web service should be checked by means of a suitable software tool.

When choosing a software tool, it may be recommended to assess the following factors:

a) Technical capability: does the tool also identify cookies set via FLASH, JavaScript, HTML5, etc.
b) How special areas (such as advanced forms, functionalities and log-in areas) are supported.

c) Whether the solution may assist in providing security for the web property that you own.

Re C. Redirects

An important area not to be overlooked is the user's 'journey' up to the content on the website. Many companies and organisations have purchased domains that have no content in themselves, but are intended to direct the user to a specific page, for example on the main website. These domains should also be part of the audit to determine if the organisation's web services set cookies.

3rd step - Giving comprehensive information

The minimum requirements for information follow directly from the cookie rules and include requirements for the *nature, content* and *availability* of the information.

Besides the content requirements given in the Cookie Order, it is important to think of the recipient of the information, allowing for factors such as language and technical detail.

Described below are a number of factors to be remembered when preparing information for the user:

A. Ensure clear navigation, indicating that the web service is setting cookies and for what purposes
B. The navigation must function satisfactorily
C. Comprehensive information about cookies
D. Specific cookie information
E. Describe how it is possible to refuse giving consent

Re A - Clear navigation

Navigation refers to the design of the website and the way in which the user is guided to the cookie information on the page.

- First and foremost, it must be clear to the user that the web service is setting cookies, information in this respect being clearly discernible from other text on the page, e.g. by a banner or active textboxes.

- Users visiting the web service for the first time must be informed unambiguously that cookies are used, the purpose of these, and by whom cookies are set, before the cookies are placed.

- The information must be given prior to placing the cookies, but it is not a statutory requirement that the user should have the information immediately when visiting the website.

- When cookies have been accepted or refused, the text may be minimised to a permanent link on the page where more about cookies can be read and consent

or withdrawal be decided. It must be possible for the user to access the information about cookies at any time during the visit to the website.

- On subsequent visits where the visitor's unit is recognised, it must be possible for the user to get immediate access to detailed information about the website's cookies at any time.

- Where subpages are used, it must be easy for the user to be directed to such subpages to get more information about the web service's use of cookies and the options available to the user for controlling such use.

- The user should be directed from the navigation on to the page that describes the web service's use of cookies in a uniform way irrespective of the user's location on the web service. The information must be accessible at all times.

- Where a user gets access to a website or web service via a domain that redirects the user to the site or web service, it must be ensured that the final site or service gives the user comprehensive information with the option of consent to the use of cookies.

Any provision of information about cookies plays an important role in terms of whether the web service complies with the cookie rules, the main principle being that the user should be able to make an informed choice.

To ensure clear information, it may be useful to follow the standard '**Web Accessibility Guidelines**'.

The standard 'Web Content Accessibility Guidelines' can be downloaded here: http://www.w3.org/TR/WCAG10/full-checklist.html.
(Note: Version 2.0 of the standard is currently under implementation.)

Re B - Requirement that the navigation should function satisfactorily

Once you have good navigation, the next step is to ensure that it works. The more complicated the navigation, the more exposed it is to errors and mistakes.

Examples of key factors to be considered:

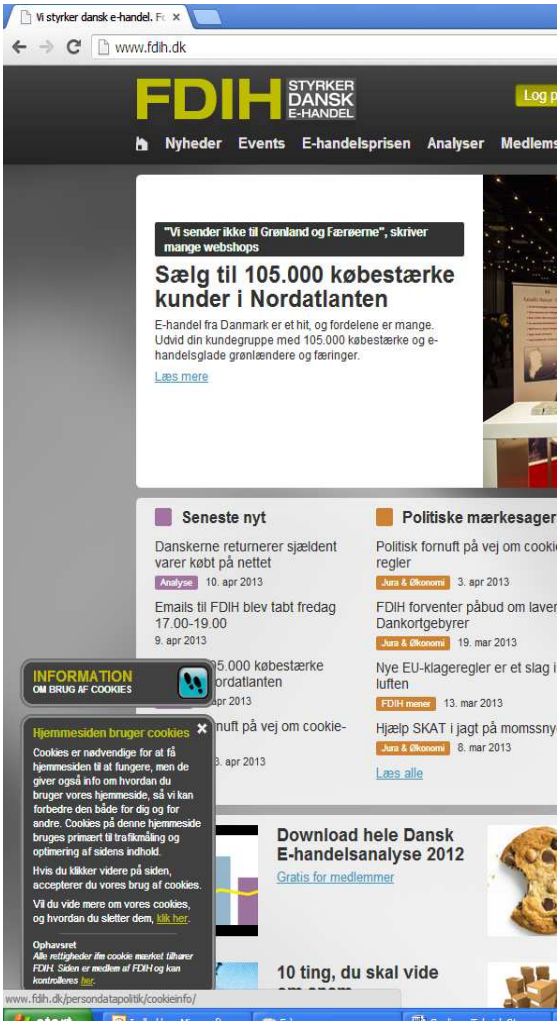
- Are there any limitations in terms of accessibility?
- Does the navigation work on all pages of the web service?
- Does the navigation also work in other contexts, for example a mobile version of the web service?
- Does the navigation also work when you get to the web service for example via a redirect?

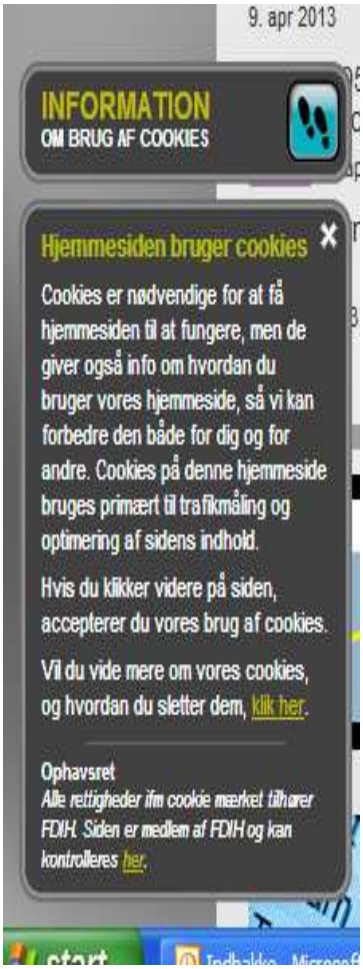
A very frequent choice of navigation is to use a banner, for example placed at the top of the page, linking to a subpage for more detailed information. However, it is important to check that the solution chosen will not interfere with search engine indexing and hence organic searching.

Practical examples of clear navigation

Each of the examples illustrates a good solution in relation to 'clear navigation', but does not necessarily meet all requirements for informed consent, see more details under *"Comprehensive information about cookies"*.

a) The Danish E-commerce Association (FDIH) has prepared a cookie solution which is being offered to the members of the association. It is an example of clear navigation in relation to cookie information and is illustrated below, as shown on the website for the members of the association.





The text contains essential information about the purpose of cookies on the site and links to a subpage with more information about the site's cookie policy, including how to opt out of cookies. The solution obviously requires that no other cookies are used for purposes other than those indicated, including cookies from third parties, as this does not appear.

Once the user has accepted or refused cookies, the information will disappear from the screen, but the small footprints appear clearly on the page throughout the user's visit.

b) **Example of navigation on a mobile unit**

The example shows how the navigation may appear on the first visit via a mobile unit.

Example of how to give detailed information about cookies. The example shown requires the functionality to be available both on the fixed and the mobile websites. There may be limitations in connection with the use of opt-out on the mobile. These should be assessed where relevant.

Re C - Comprehensive information about cookies

As was mentioned in the Guidelines section on information required, it is permitted to layer information for users so that the essential information to be provided under the Cookie Order (purpose of cookie, indication of who is setting cookies, including third parties setting cookies or having access to data via cookies) is given in the first cookie text displayed to the user, possibly with links to subpages with more information.

It may be considered to use subpages for stating an actual cookie policy, which may support user confidence in the website and hence the company or organisation in general.

Below is a list of the mandatory requirements for information (indicated by M), and recommendations (indicated by R) which may be used for stating a cookie policy:

- **[M] Purpose of using cookies**
- **[M] Identify who is setting cookies**
- **[M] Easy access to withdrawing consent**
  Under the cookie rules, there must be easy access for the user to refuse consent or withdraw consent, which should appear from the first text presented to the user, but may be explained further on a subpage in connection with a more detailed description of the website's cookie policy. It is recommended to point out to the user that in principle cookies are only deleted on a forward-looking basis unless the user is actively deleting cookies, see below.
- **[R] Deleting cookies**
  It can be recommended to make the user aware of cookies set earlier and indicate how to remove such cookies. To the extent that the service is using special cookies in connection with Flash/LSO technology etc., it may be clarified how a user can control cookies set in this manner. It is necessary not least in this area in view of the limited scope existing at present for offering 'site' based methods for refusing consent.
- **[R] Contact information** indicating the point to which questions or complaints may be addressed. It may also be stated how a complaint will be dealt with and within what timescale.

Re D - Specific cookie information

It is for the individual web service to decide how detailed they wish to describe their cookies once they have provided an adequate description of the purpose and origin of the cookie / who has access to data collected via the cookie.

For increased transparency and consumer confidence, a more detailed description may be considered, informing the user about technical characteristics of a cookie etc., including its name and life span.

The cookie rules do not provide for a categorisation of cookies on the basis of their characteristics and origin, but a categorisation may be recommended to enable a better overview of the cookies that are used, thus making information to the users easier.

A more detailed cookie description, including a categorisation of cookies, may also be useful in relation to supervision of the rules, where a detailed account of a website's use of cookies may be required.

Users may for example be provided with the following characteristics (or parameters) for each cookie on the web service in question:

Element	**Suitable level of detail**
Categorisation	One of the five categories shown in the categorisation table below.
Purpose	What is the purpose of the cookie. It is likely to be one of the following: i. Advertising ii. Analysis iii. Media management iv. Navigation v. Performance / networking vi. Pricing vii. Social network viii. Questionnaire ix. User preferences x. Profiling
Domain from which it is set	The domain setting the cookie. In the case of Google Analytics, the host domain is the one setting the cookie.
Name of cookie	The 'technical' name that the issuer has given it.
Final data owner	Name of the company which is the final recipient of data from the cookie. In the case of DoubleClick, Google (which owns DoubleClick) is the correct information.
Expiry date	Life span of cookie. May be for example 'browser session' or the date on which the cookie expires. In case a cookie has a life span of less than 24 hours, its life span may be indicated in hours.
Description	Ordinary text description of what the cookies does.

- **[R] Categorisation of cookies**

Cookies may be divided into various categories, which will give a better overview of the website's use of cookies and may help in providing better information to the user.

Below are examples of cookie categories that refer to different types of cookies.

Table of cookie categorisation

Category	**Description**
Technically necessary	These cookies are essential to the functionality of services on the website that the user has explicitly requested. It may be for example cookies required for the function of a shopping basket.
Settings	These cookies are used for supporting settings entered by the user. Examples are display settings for login areas.
Categories 1 + 2 comprise cookies usually exempted from the requirement for information and consent.	
Operation & optimisation	These cookies are used for managing the web service, for example adding customer feedback and collecting data for the use of web analysis. Any form of cookie that has potential for being used for tracking a user's navigation, searches, access pages or exit pages does not belong to this category.

Marketing, anonymous tracking across web services	These cookies are used for tracking visitors across several web services. They may be used for building up a profile of search and/or browsing patterns for any or some visitor(s).
Marketing, targeted advertising	These cookies are used for tracking a user's browsing habits and activity. The information collected can be used for showing individually adapted content. These cookies can be used for collecting personal information and/or selling data to third parties. The category also includes any cookies or groups of cookies that may be used for influencing the provision of products or services made available to a visitor on the web service (either directly or indirectly) or that may be used for influencing the price to be presented to a user. Any cookie that may be used in this way must be identified clearly and uniquely and its purpose must be indicated as "pricing".

4th step - Removing unwanted, unknown and unnecessary cookies

It is good practice to decide if you yourself consider the cookies used on your web service to be unwanted, unknown or perhaps unnecessary.

By deciding on what cookies are used on your web services, you can be sure that it is within your command what happens and what data is collected and to whom it is sent.

Besides being sure to live up to current regulations governing cookies, you may have some other benefits, such as:

– Improved speed on the website
– Protection against inappropriate transmission of data

5th step - Obtaining consent

As described above under the section on required consent in these Guidelines, consent may be obtained by the user explicitly accepting or refusing the use of cookies, for example by clicking on a button or ticking a box, or by merely clicking on to a given page. Both situations require that the user has received comprehensive information beforehand.

By following the process steps described above, it should be possible to ensure that the user of your website can make a sufficiently informed choice on acceptance or refusal of cookies.

Technical aspects to be noted in relation to the requirement for consent:

1. It is only possible to delete cookies set from one's own domain.
2. It is only possible to prevent third party cookies from being set by changing or leaving out content that sets the cookies in question.
3. Deletion of cookies requires that JavaScript is switched on in the user's browser. A server-based solution may change what is shown on the page no matter whether JavaScript is switched on or off.

To be noted about third party cookies
Some service providers that embed content on your web services allow you to adapt their service to your needs. Common examples of this are:

a. YouTube, which has a separate web service at the address www.youtube-nocookie.com that will only set cookies when the user is clicking on 'play' to start playback.
b. AddThis offers the setting option "data_use_cookies" which prevents it from setting cookies if assigned the value 'false'.

Method to ensure that cookies are not set when the user has refused
It is an explicit requirement that a web service should omit setting cookies that the user has refused. To make this possible in practice, it is recommended to add the required code to the pages of the web service or on the server.

To understand the user's settings (consent or non-consent) you need to 'parse' (analyse the syntax of) the cookie to which the setting applies. Indication of the value is very simple as the cookie uses the value 'true' for consent (also known as opt in) and 'false' for refused consent (also known as opt out). The following examples of code show that consent to cookies has been given in categories 2, 3 and 4, while consent has been refused for cookies belonging to category 5:

2=true&3=true&4=true&5=false

The following JavaScript is checking the user's settings:

```
functioncookieLevelConsent(level) {
var m = document.cookie.match(
"^(.+;)? *wscrCookieConsent=([^;]+&)?" + level + "=(t|f)");
return m ? (m[3] === "t") : null;
}
```

By placing this code at the top of your style sheet file or as part of a JavaScript file being called by all pages, you make the functionality available on all pages of your website. Subsequently you can call cookieLevelConsent() with the desired setting level to check the user's setting. The function returns the values:

1. null - the user has not indicated any setting,
2. true - the user has given its explicit consent,
3. false - the user has actively refused to give its consent.

Use of this code on a webpage makes it possible for the page to respond in accordance with the user's settings for consent.

Code set from the server page will function in nearly the same way: You 'parse' the value of the cookie and then decide if you wish to show parts of the page or you wish to show other content instead.

An example of such a page layout is shown below. The marked areas set third party cookies from an external domain, which means that the owner of the web service does not have the option of deleting these cookies. A solution may be to show other content if the user has refused consent to the cookies in question.

The marked field with share bars for social media can be replaced with icons or links managed by the web service owner itself.

The advertisement highlighted above may show an image from the web service's own domain (a 'locally served image'), which may then link to the third party site with a tracking id in the URL, or it may show an advertisement not setting cookies.

Practical example of consent management

A practical example of consent management has been given on www.sitemorse.com. The solution has exclusively been included for inspiration.

If you click on the cookie icon on the right in the browser, a panel emerges showing how many cookies there are of each type (grouped according to purpose) and there is clear information about each cookie. There is also a button ('opt out') that the user may activate if wishing to refuse consent.

Example of how to manage 'twitter' cookies

It is recommended to manage cookies from Twitter via changes on the server page. Consider how it will affect your web service and if you wish to offer the users an alternative.

"Twitter" cookies are widely used and appear in many contexts (auto logins / 'tweetthis' etc.) and it may currently be difficult to clarify the extent and usage of tracking from the company.

Below is an example of a change made on the server page. It might equally well have been made with JavaScript. The example shows that as soon as a user has refused consent to a type of cookie, new cookies will not be set and the content of the web page will change.

If, in the practical example above, you go back to the main page http://www.sitemorse.com/ and click on a news article (the three newest ones are shown at the bottom left-hand corner), then a Twitterfeed is seen to the left.

If a user then clicks on the cookie icon, proceeds to cookie category 4 and refuses consent there by clicking 'opt out' and is clicking ok,

--> twitter.com cookie guest_id is already set,

Now proceed to delete this cookie in your browser (open settings etc.)

Reload the page,
The twitter feed will now be replaced by a simple "Follow us" link,

--> No twitter.com cookie

Example of managing Addthis.com cookies
If you go back to http://www.sitemorse.com/ and click on a news article there (the three articles at the bottom left-hand corner of the page) then you will see the Twitterfeed to the left and AddThis icons under the article.

Now open the cookie panel and refuse consent to category 5 cookies by clicking the 'opt out' button. Then click OK,

--> addthis.com cookie is already set,

Now proceed to delete this cookie in your browser (open settings etc.)

Reload the page,
The AddThisfeed will look the same, but now the setting of AddThis has been changed to not setting cookies.

--> No addthis.com cookie is set

How:
This was done via JavaScript.

What we demonstrated:
When a user has refused consent, the setting in AddThis can be used to prevent cookies from being set.

Technical definitions

Iframe
An embedded frame placing other HTML content on a page. An Iframe can show content from another element, and a user can choose to print it.

LSO - Locally Shared Objects or Flash Cookies
Data which websites using Adobe Flash may store in a user's browser. LSOs are used by all versions of Adobe Flash Player.

Mobile and fixed websites

A website intended to be seen from a computer screen is also called a fixed website. The parallel to fixed websites is mobile websites, which are often subdomains under the fixed website with the purpose of making it effective to use the website for a mobile unit.

Parsing
To 'parse' is to analyse the syntax of a cookie. Parsing is required to add code in a way that enables the page to respond in accordance with the user's settings for consent.

Registered domains
A domain name is a text string defining a domain on the internet. Thus a company's list of registered domains will be a list of all the domains that the company has purchased.

Sector analysis
A sector analysis is an analysis of a sector or a group. It may be for example an analysis of the occurrence of cookies within a particular trade.

Exit pages
The expression is used to describe the website pages from which the users leave the website.

Landing page
The expression landing page is used about the pages on a website that users meet with in the first place. Often it will be the homepage, but it may also be pages that appear frequently in searches or are being linked to from other sites.

Ultimate data owner
The ultimate data owner is the final recipient of data from a given cookie, possibly after the cookie has passed through various data intermediaries. The ultimate data owner is typically the company that has written the cookie.

Web accessibility
To ensure that everyone is able to access information on the internet, a standard known as 'Web Content Accessibility Guidelines' has been made. The standard can be downloaded here: http://www.w3.org/TR/WCAG10/full-checklist.html
If the standard is complied with, it is ensured that all users will be able to access information and that the web service does not discriminate against any functional or mental disabilities.

Web property
Web property is an expression referring to the sum of all the domains, subdomains, services etc. for which a company or a person is legally responsible.