Autoriteit
Consument & Markt

Please note that, although every effort has been made to ensure this translation is accurate and consistent, the Dutch version is authentic in case of any dispute or inconsistencies.

ACM drew up and answered these questions about the cookie act with the greatest care. This document offers answers to general questions only, not to individual cases. This document is for informational purposes only.

Contents

Foreword

According to the cookie provision, which has been laid down in Section 11.7a of the Dutch Telecommunication Act (hereafter: Tw), websites must inform visitors, and they must obtain consent before storing or accessing a cookie or other data on computers, laptops or mobile phones. This requirement does not apply to cookies that are necessary for the technical operation of the site or, for example, to analytical cookies that impinge on users' privacy only to a limited extent. ACM regularly receives questions from businesses, government organizations, and other organizations about the cookie provision. Furthermore, other technologies save data and/or gain access to data on computers such as Javascripts or Web beacons. Wherever cookies are mentioned in this document, it also refers to technologies such as those.

This document contains answers to frequently asked questions in order to provide clarity to market participants. This publication is an update of the previous version, which was released in March 2013, and contains several changes to the structure. Also, the information about the prohibition of cookie walls on government websites has been expanded.

ACM does not provide any legal advice. Businesses and website managers themselves are responsible for the practical interpretation of the cookie provision. Consumers that wish to know more about cookies can find more information on ConsuWijzer.[1]

[1] https://www.consuwijzer.nl/.

Autoriteit
Consument & Markt

1 Questions about the act

What are the rules?
Cookies are small text files that are stored on the user's computer or other terminal equipment, when visiting a website. These cookies are able to track users across multiple websites, thereby making it possible to generate customized advertisements. There are cookies that are used in order to have the websites themselves function better, which are called functional and analytical cookies.

The cookie provision contains an information obligation and a consent requirement, except for the exceptions included in the law. Parties that store and/or access cookies must give users clear and specific information about the fact that they are using cookies and about the purpose thereof. In addition, cookies may only be stored and/or accessed if lawful consent has been obtained in advance from the user. Moreover, the cookie provision requires that consent must be obtained for storing cookies on computers or, for example, mobile phones. Government websites are not allowed to use 'cookie walls', with which visitors that do not accept any cookies are denied access to the website.

What is the background of the cookie provision?
The cookie provision was first laid down in Article 4.1 of the Decision on universal service and end user interests (hereafter: BUDE). On June 5, 2012, it was included in Section 11.7a Tw. From that moment on, the standard became stricter as a result of the European e-privacy Directive 2009/136/EC, which was introduced throughout Europe. It was no longer sufficient to *inform* and to offer the option of refusal, as was included in Article 4.1 BUDE. Users would now have to have given *consent* for storing and/or accessing data. Consent must be obtained through a free, specific expression of will that is based on information.

However, the cookie provision caused a lot of frustration among users and website owners. That is why an exception to the information obligation and the consent requirement was introduced in Section 11.7a Tw, as of March 11, 2015. This expanded exception affected cookies that give information about the quality and effectiveness of the provided information-society service, and which will have little or no impact on the user's private life. With the introduction of these new rules, the website owner is no longer required to inform users, nor is he required to obtain consent for storing these analytical cookies. For storing cookies that do not fall under an exception, the website owner must inform visitors in advance, and he needs to ask for consent. These cookies cannot be stored without having informed users and having obtained the necessary consent. In addition, a new, fifth paragraph has been added to the provision, which prohibits government websites from using a cookie wall.

2 Questions about the scope

Do the rules only apply to computers?
No, the rules apply to all terminal equipment. This includes computers, but also other 'smart' devices such as smartphones, consoles, tablets, and televisions.

Do the rules also apply to technologies similar to cookies?
Yes. This provision covers more than just storing cookies. This description not only applies to cookies, but also to Javascripts, Flash cookies, HTML5-local storage, web beacons, and other technologies with which data is stored and/or accessed. Only if no data at all is stored or accessed on a user's terminal equipment, Section 11.7a Tw will not apply. The information in this document about cookies therefore also applies to similar technologies.

Do the rules apply to all cookies?
No. The law contains *exceptions* where the information obligation and the consent requirement do not apply. In those cases, users are not required to be informed or to give consent. These exceptions concern storing and/or accessing data (on users' terminal equipment) that:

- are needed to facilitate communication, for example load-balancing cookies. These cookies are used to distribute data traffic across multiple servers;
- are strictly necessary for the service requested by the user, for example cookies that are needed to make a payment in an online shop or that are used for accessing an online banking environment.
- are aimed at obtaining information about the quality and/or effectiveness of a provided service (for example a website). An additional condition for storing this kind of cookie is that it will have little or no impact on the private life of the user. An example could be analytical cookies. This exception has been in effect since March 11, 2015.

Attention: these rules apply to both first-party cookies and third-party cookies.

Do the rules also apply to intranet?
No. The rules do not apply to intranet. They cover the storing and accessing of data on terminal equipment of *users*. According to Section 1.1, under n, Tw, users are defined as natural persons or legal persons that use a public electronic communication service. Considering its isolated nature, intranet does not fall under this definition of public electronic communication service.

Do the rules also apply to server log analysis?
The rules do not apply to server log analysis. They cover the storing and accessing of data on terminal equipment of *users*. With server log analyses, no data is actively stored or accessed. It involves an analysis of data that the user himself has sent to the server, which is information sent by the user in an initial get / http request. This initial request contains information about the

requested address, the requesting IP-address, user agents and similar limited information. All data that is stored or accessed after the initial request does fall under the scope of Section 11.7a Tw. The data sent through the browser may contain personal information to which the Dutch Data Protection Act (hereafter: Wbp) applies.

Do the rules only apply to Dutch websites?

No. The rules do not apply to Dutch websites only. According to the provision, the norm applies to 'anyone.' This means that anyone that stores data on a user's terminal equipment or wishes to access data that is stored thereon must comply with the regulations, irrespective of that party's location. The key principle here is that this norm's objective is to protect users in the Netherlands. The information obligation and the consent requirement thus apply to both Dutch and non-Dutch websites that (exclusively or partially) target Dutch users. Whether websites do so can be deduced, for example, from the nature of the information that is presented, the option of having the products shipped to the Netherlands, or from the fact that a website is available in Dutch. In that context, the domain name (.nl / .eu / .com / .net / etc.) associated with the website, the language the website is presented in or what target audience the website seeks to reach are not relevant.

3 Questions about the exceptions

Do no-follow cookies fall under the exception of Section 11.7a, paragraph 3, Tw?
The 'no-follow cookie' that is used to register a user's preference not to have any cookies at all can be considered a service requested by a user where it is strictly necessary to store data. This may seem contradictory since the user in question had apparently indicated not to want any cookies stored. In such a case, ACM believes a no-follow cookie can be considered strictly necessary. In such cases however, ACM mandates the following safeguards:

- The user must have been offered a choice between accepting or declining cookies *and* he must have chosen to decline cookies. If the user in question has not taken any action, the website will obviously have to continue informing him about the fact that it wishes to store cookies.
- The website must inform the user that a no-follow cookie will be stored with the sole purpose of registering that user's choice.
- The website may only store a no-follow cookie for that specific purpose. The no-follow cookie can only have information that is strictly necessary for that purpose (for example: no follow=1) and it cannot contain any unique identifiers. It is obviously not allowed to follow (permanently or temporarily) that user with a no-follow cookie using that cookie (or in combination with other technologies) and/or, at any time, to link it with other available information about that user.

In the case of load balancing, do cookies fall under the exception of Section 11.7a, paragraph 3, Tw?
Load balancing is a computer networking technology that makes it possible to distribute workloads across multiple computers. Load balancing can be realized by using a 'load balancer,' among other things. A user's request to view a web page is sent to a load balancing gateway, which forwards the request to one of the available servers. In some cases, it is necessary to send successive requests from the user to the same server. In such situations, a cookie can be used to remember which server was used so that further requests can be sent to the same one as well. The information in such cookies has the sole purpose of identifying the used server, and the cookie is stored until the internet session ends. *In this situation*, the load balancing cookie has the sole purpose of facilitating communication over an electronic communication network, and thus falls under the exception of Section 11.7a, paragraph 3, Tw. For these cookies, users do not need to be informed, and no consent need to be obtained.

Do social-media plug-in cookies fall under the exception of Section 11.7a, paragraph 3, Tw?
Social-media plug-in cookies are cookies that enable social-media users to share websites (or parts thereof) within that social-media network. Plug-ins on the website of, for example, an online store can make it possible to share pages via a social-media network by storing and accessing cookies on the terminal equipment of a user. In principle, these cookies do *not* fall under the exceptions of Section 11.7a, paragraph 3, Tw. Users that are not members of a

social-media network or users that are not logged in on that social-media network do not expect to be connected to any social-media network by means of cookies. Storing cookies with these users is not necessary for providing a requested service. In that case, users will obviously have to be informed, and consent must be obtained before social-media plug-in cookies can be stored.

However, if a user is logged in on a social-media network, ACM assumes that this user *does* wish to take advantage of the functionalities of social-media plug-in cookies. In that case, these cookies do fall under the exception of Section 11.7a, paragraph 3, Tw.

For website owners, it is difficult to determine beforehand whether or not his users are logged in on a social-media network. An often-used solution is available, which is user-friendly and privacy-friendly. Website owners can use non-active, "gray" social-media buttons. Only after a user deliberately clicks on such a button, this functionality of the website will be activated, and the social-media network can store a cookie.

What cookies fall under the new exception that was introduced on March 11, 2015?
The new exception as of March 11, 2015, has been laid down in b, second sentence of Section 11.7a, paragraph 3, Tw. The cookies that fall under this exception provide information about the quality and/or effectiveness of a provided service. In the Explanatory Notes, the minister gives several examples:

- Analytical cookies: the purpose of these cookies is to analyze and map the use of a certain website, so that the quality and/or effectiveness of the website can be improved.
- Affiliate cookies: these cookies are used to keep track of what ad leads to the purchase of a specific product, so that the party that has displayed this ad (the affiliate) can get a reward from the advertiser.

Attention: these cookies are only exempted from the information and consent requirements if they have little or no impact on the user's private life. This means that the data collected with these cookies can only be used for the abovementioned purposes, and in such a way that it will have little or no impact on the user's private life. If the data is analyzed by a third party, arrangements must be made with this third party so that this data can only be used for the purpose of the website in question. One option could be to sign a data processing agreement with the third party.

Do cookies and scripts that are necessary for the functioning of tag management systems also fall under the exception?
Tag management systems enables website owners to isolate specific content of a website and to save it in a tag. By placing content in a tag, it becomes very easy for website owners to make specific content dependent on all kinds of variables such as consent. So this means that tags could have the rule that certain cookies or marketing campaigns can only be stored after users have given their consent to storing cookies. In that sense, such systems better enable website

owners to comply with their statutory requirements.

Although, strictly speaking, there are no exceptions with regard to tag managers, ACM, considering the above, does see enough reasons to allow such scripts to be stored before consent has been obtained. In that case, informing about the use of such systems will suffice. In that context, website owners must pay attention to the following safeguards:

- the website can only store the tag management script for the specific purpose of tag management;
- the script can only contain content that is strictly necessary for that purpose, and cannot contain any unique identifier(s);
- it should not be possible to track the user using the script (either by itself or in combination with other technologies) or in any other way, either temporarily or permanently and/or, at any point, to link this to other available data about the user. In other words, no personal information can be collected or processed using the script;
- the sole purpose of the script must be to perform tag management activities. This means loading the tags only;
- in the second layer of information, the website is to inform the user of the use of a tag manager, and of the purpose thereof.

4 Questions from users

How will the cookie provision affect ordinary internet users?
As a result of the cookie provision, internet users will be informed and will have to give their consent before websites are allowed to store cookies on their terminal equipment. Internet users are thus given the opportunity to decide whether websites may store or access data on their terminal equipment. Users will consequently have more control over their online privacy. Users can find more information on www.consuwijzer.nl, where they can also file a complaint if the cookie provision is violated.

The law was amended recently. How will these changes affect me as a user?
On March 11, 2015, Section 11.7a Tw was amended. This amendment concerned, among other things, cookies whose purpose it is to measure the quality and/or effectiveness of a provided information-society service (such as a website), and which, when measuring those aspects, will have little or no impact on the user. For users, this means that, when these analytical cookies are stored on the terminal equipment, the website owner is no longer required to inform them, or to ask for their consent. In addition, it is expected that users will have to give their consent less often.

In the parliamentary debate of the amendment, the consent requirement was also discussed. The user's consent can also be deduced from an act, which is the so-called 'implicit consent.' For example, this could be the case if the internet user continues to browse on the website *after* he has been informed clearly and completely about what cookies are used on the website, and that, when continuing to browse, he gives his consent to the storage thereof and/or access thereto.

In addition, websites of government organizations (including semi-governmental organizations) are not allowed to use so-called cookie walls. This means that access to such websites can no longer completely depend on the user's consent for the use of all cookies.

I did not give my consent to have cookies stored on my computer, but I am still seeing ads.
The purpose of the act is not to prohibit ads, but to protect internet user privacy. Even without any consent to store cookies, websites are, at any time, allowed to show users ads, provided that, with these ads, no access is obtained and no data is stored on their terminal equipment.

Why do I see so many cookie warning banners on the Internet?
Users encounter so many cookie warning banners on the Internet because the law mandates that anyone seeking to store or access data on their terminal equipment should inform users thereof and is required to obtain their consent. The Dutch legislature did not specify how users are to be informed or are how consent has to be obtained. Websites are thus free to determine what solution suits them best, as long as enough information is given, and as long as consent is

obtained through a free, specific expression of will that is based on information. Websites usually save your choice in a cookie, meaning, in principle, you as a user only have to give your consent once. However, this means that, if all cookies are deleted, websites no longer know what choice had been made. As a result, users would have to give their consent again at a later point in time about for the use of cookies.

5 Questions about the implementation by market participants

What are the specifics about informing and obtaining consent?
The information obligation and the consent requirement form the basis of Section 11.7a Tw. These two are inextricably related with one another: without proper information, it is not possible to obtain a valid consent. Pursuant to the Dutch Data Protection Act, any consent that is given in connection with Section 11.7a Tw must be ´*free, specific, and based on information*,´ as with the rules about the spam prohibition of Section 11.7 Tw. Market participants are free to determine in what way consent is obtained and information is given. As with Section 11.7 Tw, consent cannot be obtained by referring (explicitly or implicitly) to, for example, general terms and conditions, privacy and/or permission statements. The information given to users must be completely clear. They need to know why and what they are giving their consent to, as well as the scope of that consent. When obtaining a valid consent, the required information must be easy to find and easy to understand. What information qualifies as such may depend on the target audience that the website wishes to reach.

How do I meet the information obligation?
In order to meet the information obligation of Section 11.7a, paragraph 1, under a, Tw, the user needs to be informed about the purposes for which parties seek to store and/or access data. It is important that the user is informed about why a website stores a cookie, and for what purpose. The user thus knows what they are giving their consent to. This information must always be displayed in a directly visible space on the website, and must be written in language that is appropriate for the website's target audience. The choice of language for the explanation about cookies may thus depend on the website's target audience. Informing by broadly referring to general terms and conditions, privacy and/or permission statements is not enough. ACM recommends naming and explaining all cookies and/or other technologies in the information, including both cookies for which consent needs to be obtained and cookies that fall under the exceptions of Section 11.7a, paragraph 3, Tw. That way, the user is informed as accurately as possible, and is then sooner able to decide about giving his consent. Within the industry, several trade associations have drawn up industry-wide solutions that can be used to inform users about cookies. Please note: you are not allowed to store any cookies if you only inform users. You will also need the user's *consent*. An overview of the elements about which a user must be informed directly is listed below. This concerns at least the following elements:

- The name of the website;
- For what purpose the cookies are used (for example, tracking, displaying advertisements, website improvement, etc);
- The categories of cookies that are stored by or through the website (analytical, tracking, functional);
- The use of other technologies (Javascript/Web beacons);
- Information about what action is required from the user in order to give their consent (for example, approval, yes, continue to browse the website, etc);

- A link to the cookie statement and/or privacy statement;
- The impact, if any, that the cookies might have on the user's privacy.

As a website owner, am I also required to inform and ask for consent with regard to the use of cookies by third parties on my website?
The website owner is the first point of contact for ACM. Website owners usually also ask for consent on behalf of third parties. If all third parties each had to ask for consent within the limited space offered by website owners, the information would become cluttered, and often too much. Another possibility is that each ad of third parties would have to have a separate consent pop-up screen before the ad can be displayed. In practice, it is the website owner that is able to demonstrate to ACM that third-party cookies, too, are stored in accordance with the rules of Section 11.7a Tw. After all, website owners have a certain responsibility for cookies that are stored through their websites.

With regard to the information obligation about the use of cookies, is it enough, in case of third-party cookies, to refer to the information of those third parties?
It is possible that through your website (with your consent), third-party data is stored on the terminal equipment of users. With regard to these third parties too, you will need to meet the information obligation as referred to in Section 11.7a, paragraph 1, under a, Tw. In order to avoid including all information of third parties in your own information, you may refer to that third-party´s information. That third-party´s information obviously needs to meet the statutory requirements, too.

What are the statutory requirements with regard to consent?
In order to meet the consent requirement, there must be consent that, pursuant to the Wbp, is *"a free and specific expression of will, based on information"* with regard to Section 11.7a Tw. This expression of will requires that the user performs an action to give their consent. For example, this could be an informational banner, which provides the user with information in accordance with the requirements as detailed above, and which asks the user to give their consent before the cookies are stored.

Attention: if users press a 'more information'-button or a similar button, it cannot be deduced from this act alone that users agree to the storage of cookies. Consent can neither be deduced from leaving and revisiting a website, from refreshing the page, from inaction after entering the URL address, or from merely entering the URL address.

What additional requirements apply with regard to implicit consent?
According to the Explanatory Notes to the amendment of March 11, 2015, consent apparently can also be deduced from certain actions on the website, which is referred to as 'implicit consent.' Such actions include browsing deeper into the website *after* the internet user has been clearly and fully informed about cookies that are stored, and that their continued usage of the website constitutes consent for storing and/or reading cookies. However, such implicit consent requires an explicit action. The user must therefore actually click on content of the

website before such implicit consent can be deduced. Merely scrolling or swiping on the website is not enough for implicit consent. The concept of 'browsing deeper into the website' must be interpreted narrowly in order to tie in as much as possible with the interpretation of the Wbp with regard to consent. It must be completely clear to the website owner that the user genuinely intended to give their consent to the storage of cookies. Furthermore, it must be clear to the user that their consent to the storage of cookies can be deduced from the fact that they continue to use the website. The user must be informed about this in a directly visible location.

Who are required to obtain the user's consent?
Anyone who stores or accesses data on a user's terminal equipment must have obtained consent to do so. When visiting a single website, this can be different parties. It can be the website owner, but also a third party that has agreed with the website owner to store or access cookies on his website. It is up to these parties to decide whether consent must be obtained multiple times or that the website obtains consent on behalf of all parties. Website owners are the contacts for the information about cookies that their website offers and about the data that is stored and accessed when visiting the website. After all, users visit the website of the website owner, not the websites of the advertisers. The website owner therefore cannot duck his responsibility to avoid third parties from storing and/or accessing data on his website without the user's consent.

Can I, as a private party, deny access to users who don't give consent?
Websites are not required to grant users access, and such access may, in principle, be made dependent on accepting a cookie. If a user does not give consent for storing a cookie, it is possible that the website in question does not function properly. Other interests of the website owner, too, may lead to a situation where the website owner chooses to make access to the website dependent on giving consent. This way, it can be prevented that access to the website is only granted if the user gives its consent for storing tracking cookies that save the user's interests so that personalized ads can be displayed. This is how users pay for visiting the website in question.

Despite the fact this is not a very customer-friendly way to extract consent from users, the website owner is, in principle, free to set up his website this way. ACM wishes to emphasize that the use of a cookie wall is against the spirit of the act, even though it is allowed in most cases. After all, the cookie provision seeks to offer users a choice with regard to their privacy and the use of his personal details on the Internet. If websites offer users access only if all cookies are accepted, then users are actually restricted in their choices.

In what situations are private parties not allowed to deny individuals that did not give their consent access to the website?
There are situations where the use of a cookie wall by a private website owner is not allowed. This is the case if the user's consent was no longer 'free', because the user has such an enormous interest in visiting the website that not visiting the website could bring about

significantly negative effects. The legislature has identified three situations in which there are, in any case, significantly negative effects, meaning there is thus no free consent in the case of the use of a cookie wall:

1. As a result, the user is unable to carry out a statutory duty properly;
2. As a result, the user is unable to exercise a legal right; or
3. As a result, the user is only able to enjoy suboptimal health care.

Can I, as a government website, deny access to users who don't give consent?
Websites of government organizations (including semi-governmental organizations) are not allowed to use so-called cookie walls. Under Section 11.7a, paragraph 5, Tw, legal persons that have been established under or pursuant to civil law cannot deny users that have not given consent for storing or accessing data access to the website. This includes public bodies and special legal persons that have been established under or pursuant to the law, and that are not legal persons as referred to in Sections 2:2 and 2:3 of the Dutch Civil Code (BW). Legal persons that offer a service on behalf of a legal person that has been established pursuant to civil law are not allowed to use a cookie wall either. The deciding factor in this context is the extent to which actions are taken on behalf of a legal person that has been established pursuant to civil law. This has to be a legal person that has been established with the purpose of performing a statutory duty. This does not include legal persons that only for a small part perform a statutory duty or legal persons that receive subsidies from the government but that do not perform any statutory duty.

What is the best way to obtain the consent of my website's users?
The legislature deliberately gave market participants the freedom to decide in what way websites can obtain their users' consent. In practice, many websites choose to inform their users and obtain their consent, for example, by using pop-ups, floating boxes, information banners or an overlay. Website owners are thus free to select a method that fits the website's concept and its users. What is crucial is that the user who gives his consent does so with a free and specific expression of will, based on information, as referred to in Section 1, under i, Dutch Data Protection Act. Such an expression of will requires users taking a conscious step giving such consent. If users are offered a choice to give their consent or not, but do not make one, it cannot be automatically concluded that they have thus given their consent. Various plugins for websites have become available by now that notify users of current regulations, and that allow users to give consent properly. Once the user's consent has been obtained, it is saved in a cookie, rendering it unnecessary to obtain his consent again for every subsequent visit.

Can I obtain a user's consent for multiple domains?
If the user is informed about the cookies to be used and about the different domains, his consent may be valid for multiple domains. It must be completely clear to the user that his consent is obtained for multiple websites. In addition, the user must have the opportunity to

browse through a comprehensive list of domains, so that there has been a free and specific expression of will, based on information.

When obtaining a bundled consent for multiple domains, it must be ensured, at least, that the consent remains sufficiently specific:

1. The user must be reasonably able to expect that a bundled consent is given for those domains. In order to be able to consider consent to be 'specific,' the main relevant point is that these websites offer the same *type of service*.
2. In addition, these websites must use the same technology or technologies. Consent cannot be obtained in one go for a list with different technologies that could be used on different domains. In such a case, the information that is given cannot be sufficiently specific.

Attention: the user's consent is only valid for the domains and cookies about which the user was informed. If you add a domain or a cookie to the list at a later point in time, you will have to obtain his consent again.

Does a user have to give his consent with every visit?
No. Users are not required to give their consent again with every repeat visit to a website if they have already given their consent once. The consent remains valid for the lifespan of the cookie unless the user revokes his consent, for example by deleting the cookie. In addition, the user's consent will no longer be valid if the website owner changes the nature of the consent obtained, for example by changing his privacy and/or cookie policy.

How do I know if a user has revoked his consent?
If a user deletes a cookie or has it deleted by, for example, the browser or a virus scanner, the website that stored the cookie in question must assume that the user revoked his consent. If the same user revisits the website, he needs to be informed again and his consent obtained again, just like with any other new user. If at all possible, the website owner could point out to the user that he had given his consent before, and ask him whether he would like to extend that consent. Repeat visits by the same user could obviously also be made on other devices. In addition, if multiple users use the same device (and visit the same website), it can be considered a repeat visit. In all cases, the party that stores a cookie must assume that, if the device does not have or no longer has any cookies, the user has not given any consent.

Does a user's consent apply to all users of the device?
The consent applies to the user that has given it. In the case of multiple users using the same device, it depends on the usage of the device. If the website owner can access a previously stored cookie, he may assume that consent was given for it. After all, it is quite possible that different users use the same profile and/or browser for which the consent was given. If the website owner can see in his registration that consent has been given, but no cookie can be found anymore, the website owner must assume that consent has not been given, and must be

reobtained. This may be the case if multiple, different profiles and/or different browsers are used on the same device, as a result of which cookies are stored in different locations.

And what about browser settings? Can a user indicate with a setting in his browser that he has or has not given consent?
ACM welcomes any user-friendly solution in which giving consent in the browser settings can be realized. Discussions about such solutions are held at a European level. Parties that store or access cookies cannot automatically assume that, if a browser accepts cookies, the user must have given his consent to do so. Many browsers, by default, are currently set to accept all cookies. It cannot be concluded from the fact that the user has not changed this yet, that he thus accepts cookies. The Do Not Track systems of the current generation of browsers are not sufficient at this point. It is not allowed to wait with the implementation of the cookie provisions in anticipation of the developments in this field. ACM will be keeping a close watch on any possible developments in this field.

I often read about a 'reverse burden of proof' in the case of tracking cookies. What is that?
Tracking cookies may involve processing of personal data, in which case the party that stores and/or accesses the tracking cookies must comply with the Dutch Data Protection Act. The Dutch Data Protection Authority (CBP) enforces this part of the provision. The *presumption of law with regard to tracking cookies,* which comes after Section 11.7a, paragraph 1, under b, Tw, is also part of the cookie provision. Based on this presumption of law, the CBP may assume that, with regard to the use of tracking cookies, personal data is processed, and that parties are required to comply with the Dutch Data Protection Act, unless the party that stores and/or accesses, is able to demonstrate that he does *not* process any personal data.

How can I prove that I have obtained consent?
It is your responsibility to demonstrate you have properly obtained the user's consent to store cookies. The law does not dictate in what way this has to be demonstrated. One way to prove that consent was obtained from the user is to register the way in which his consent was obtained, in what way the user was informed, and the time that his consent was given. The proof of consent alone is not enough. You must be able to prove that the user was properly informed.

In many cases, it is difficult to prove that a specific user has given consent for storing a cookie. Therefore, it is also sufficient if the website owner demonstrates he had a watertight procedure with which he correctly informed the user, and with which he correctly obtained the user's consent. A watertight procedure means that the procedure will always lead to a lawful consent. In this context, it is important that it can be demonstrated that, at any point in the past, the procedure functioned as described. This means that some sort of version management must be performed. This way, it can thus be proven that the website owner has obtained the user's consent.

Autoriteit
Consument & Markt

Pursuant to the law, ACM has the power to launch an investigation and to take enforcement actions up to five years after a possible violation was committed. During this period, you are required to be able to demonstrate that you properly obtained consent from the user or to save the abovementioned information in order to be able to present them to ACM, if asked to do so.

Version: November 2016

Autoriteit
Consument & Markt

6 Questions about ACM

What is ACM?
On April 1, 2013, the Establishment Act on the Netherlands Authority for Consumers and Markets came into effect. On that date, the Netherlands Authority for Consumers and Markets (ACM) became the legal successor to the Netherlands Consumer Authority, the Netherlands Competition Authority, and the Netherlands Independent Post and Telecommunications Authority. ACM has taken over the powers of each of its legal predecessors. More information about the organization, mission, strategy, market outlook and key priorities for 2013 can be found on its website www.acm.nl.

In what way does ACM enforce?
ACM enforces both the information obligation and the consent requirement of Section 11.7a Tw. ACM takes enforcement actions based on investigations of its own, and on indications it receives from market participants. To this end, ACM has digital investigators. Users can submit tip-offs about possible abuses to ConsuWijzer. If the violator (or alleged violator) has its registered office in a different European Member State, ACM may decide to refer the case in question to the regulator in that Member State. In addition to ACM, the Dutch Data Protection Authority, which enforces the Dutch Data Protection Act, has the power to enforce Section 11.7a Tw (or parts thereof).

What is the maximum fine ACM can impose?
Under its statutory powers, ACM can impose fines up to EUR 450,000 if the Tw is violated. This maximum also applies to violations of the cookie provision, but the actual level of a fine in the case of a violation depends on different factors. The factors that play a role when determining the level of the fine in case of an actual violation have been laid down in the Policy rules of the Minister of Economic Affairs containing guidelines on the imposition of administrative fines by ACM. In addition to fines, ACM may choose to use other instruments such as warnings or imposing orders subject to period penalty payments in order to force a violator to end the violation.

Can ACM take a look at my implementation of the act on my website and approve it?
No. ACM does not give individual recommendations with regard to the correct implementation of Section 11.7a Tw on your website. However, ACM does provide general information about the rules for businesses (visit https://www.acm.nl/nl/onderwerpen/loket for information in Dutch). ACM regularly updates this document with frequently asked questions and answers on its website.

ACM does not grant some sort of final approval (a ‘green seal’) for solutions chosen by website owners, because, on the one hand, websites are often dynamic and are adjusted from time to time, possibly rendering them non-compliant afterwards, and, on the other hand, an ACM seal of approval could stimulate ‘copycat behavior’ among other market participants, since that

Autoriteit
Consument & Markt

particular solution has been given ACM's seal of approval, which could hinder innovation.

Can consumers file a complaint with ACM if cookies are stored on their computers or any other terminal equipment without their consent?
Yes. Consumers can submit these indications to ConsuWijzer: www.consuwijzer.nl.

Disclaimer

ACM drew up and answered these questions about the cookie act with the greatest care. This document offers answers to general questions only, not to individual cases. This document is for informational purposes only.

Should you have any further questions, please send them by email to cookies@acm.nl.

Autoriteit
Consument & Markt

Annex 1: text of Section 11.7a of the Dutch Telecommunication Act

Section 11.7a of the Dutch Telecommunication Act

1. *Without prejudice to the Dutch Personal Data Protection Act, anyone who wishes to gain access to data that has been stored on a user's terminal equipment or who wishes to store data on a user's terminal equipment using electronic communication networks shall be required to:*
    a. *give the user clear and complete information in accordance with the Dutch Data Protection Act, at least about the purposes for which they wish to access or store the relevant data, and*
    b. *have received the user's consent to do so.*

2. *The requirements mentioned in the first paragraph, under a and b, shall also apply when data are stored or when data stored on terminal equipment is accessed in any other way than by means of an electronic communication network.*

3. *The provisions in the first paragraph do not apply insofar storage or access is concerned:*
    a. *with the sole purpose of facilitating communication over an electronic communication network, or*
    b. *that is strictly necessary for providing the information-society service as requested by the subscriber or user or (on the condition that this will have little or no impact on the private life of the subscriber or user in question) for obtaining information about the quality or effectiveness of a provided information-society service.*

4. *Any act as referred to in the first paragraph, the purpose of which is to collect, combine or analyze data about the use of different information-society services by the user or subscriber so that the user or subscriber can be treated differently, shall be considered 'processing of personal data,' as referred to in Section 1, under b of the Dutch Data Protection Act.*

5. *A user's access to an information-society service that is provided by or on behalf of a legal person established under public law shall not be made dependent on the grant of consent as referred to in the first paragraph.*

6. *Under or pursuant to an order in council, more detailed rules with regard to the requirements mentioned in the first paragraph under a and b may be issued as agreed upon with the Dutch Minister of Security and Justice. An advisory opinion regarding any draft version of such an order in council shall be sought from the Dutch Data Protection Authority (CBP).'*