



Wolf Software Limited

JPECR Plugin – Technical Documentation & Legal Information

Issue: 1.0

Date: Sunday 18th December 2011



Contents

1 Overview.....	4
1.1 The Legislation.....	4
1.2 What does this mean?.....	4
1.3 How to comply with the UK's current law on cookies.....	6
2 Impact – What it means to you.....	7
2.1 Immediate Impact.....	7
2.2 Long Term Impact.....	7
2.2.1 Penalty for non-compliance.....	7
3 Our Solution.....	8
3.1 Demonstration.....	8
3.2 The Workflow.....	8
3.3 Implementation.....	9
3.3.1 No Javascript ?.....	9
3.4 Installation.....	9
3.4.1 Getting Consent.....	9
3.4.2 Using Consent.....	10
3.5 Customisation.....	10
3.5.1 Look and Feel.....	10
3.5.2 Defining you own cookies.....	10
3.5.3 What can't I change?	10
3.5.4 Additional Settings.....	11
3.6 What the solution does not do.....	11
4 Support.....	12
4.1 What if I have problems or questions?.....	12
4.2 Commercial Support.....	12
5 Version History.....	13





1 Overview

May 26th 2011 was a significant date for website owners as it delivered an unwelcome and unexpected surprise in the form of a new European Union law that requires website owners to make significant changes to their websites.

This new Cookie Law as it has become known is an amendment to existing privacy legislation that requires websites to obtain informed consent from visitors before they can store or retrieve any information on a computer or any other web connected device.

Cookies are simply small files that the majority of websites use to remember visitors to it and are typically stored in the visitor's web browser in order that the site remembers them should they re-visit at a later date or should they move through the site page by page.

They are designed to make the users visit easier such as storing your profile information, remembering text size or automatically logging in your username and password if you choose to do so on your next visit.

It is the use of 'tracking' cookies in particular that the EU wants to focus its attentions on, by raising awareness to the new law. By requiring websites to inform and obtain explicit consent for cookies it aims to give web users more control over their online privacy.

1.1 The Legislation

The Privacy and Electronic Communications (Amendment) Regulations 2011 came into force on 26 May 2011, amending the original 2003 Regulations. If cookies are used by a website, the UK Regulations provide that certain information must be given to that website's visitors and the visitor must give his or her consent to the placing of the cookies, unless a limited exception applies.

The relevant rules are found in amended Regulation 6, which reads as follows:

6. - (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
- (2) The requirements are that the subscriber or user of that terminal equipment -
- (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
 - (b) has given his or her consent.
- (3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.
- (3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.
- (4) Paragraph (1) shall not apply to the technical storage of, or access to, information -
- (a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
 - (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

1.2 What does this mean?

The UK Regulations mean that a website operator must not store information or gain access to information stored in the computer (or other web-enabled device) of a user unless the user "is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information" and "has given his or her consent". The consent requirement in the UK Regulations replaces the previous position which provided that visitors should be given the ability to refuse cookies.

The only cookies that do not need users' consent are those that are strictly necessary to fulfil the user's request for services. That will cover, for example, the use of cookies to remember the contents of a user's shopping cart as the user moves through several pages on a website. Other cookies, including those used to count visitors to a website and those used to serve advertising, will require consent.



The term "consent" is not defined in the UK Regulations or the Data Protection Act 1998. It is, however, defined in the Data Protection Directive of 1995, as "any freely given specific and informed indication of his wishes". This Directive was implemented in the UK by the Data Protection Act 1998.

The consent requirement has been the subject of much discussion since the publication of the EU Directive amending the cookies law. Various authorities, including the Article 29 Working Party (a coalition of data protection regulators from across the EU), the UK Government and the Information Commissioner's Office have voiced conflicting opinions on how the consent requirement will operate in practice. The authorities have differing views on whether consent should be obtained prior to the placing of cookies. It is difficult to see how anything other than prior consent will comply with the wording of the UK Regulations.

The Article 29 Working Party warned that consent cannot be implied from browser settings.

"Consent must be obtained before the cookie is placed and/or information stored in the user's terminal equipment is collected, which is usually referred to as prior consent," said the Working Party's Opinion. "Informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user."

"Average data subjects are not aware of the tracking of their online behaviour, the purposes of the tracking, etc. They are not always aware of how to use browser settings to reject cookies, even if this is included in privacy policies," said the Working Party. "It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes."

The Working Party did not go as far as to say that every website needs to ask every visitor to accept every cookie, though. Many cookies are used by advertising networks across multiple websites. For these cookies, consent can be given once to a network and cover all the websites that network serves, according to the Working Party.

Shortly before the publication of the UK Regulations the Information Commissioner published guidance that offers advice on when and how the consent may be given.

Although the guidance suggests a number of methods to obtain consent it stops short of proving definitive guidance on how to achieve compliance, leaving it to businesses and organisations to review their use of cookies and consider how they might be able to obtain the necessary consent.

Both the ICO and the Government have not ruled out the use of browser settings to achieve compliance in the future. The Government has set up a working group comprising Mozilla, Apple, Microsoft, Google, Yahoo, the Internet Advertising Bureau and Adobe to work on a technical solution. In the meantime the ICO advises businesses to obtain consent some other way.

The guidance states:

"At present, most browser settings are not sophisticated enough to allow you to assume that the user has given consent to allow your website to set a cookie. Also, not everyone who visits your site will do so using a browser. They may, for example, have used an application on their mobile device. So, for now we are advising organisations which use cookies or other means of storing information on a user's equipment that they have to gain consent some other way".

The guidance continues:

"You need to provide information about cookies and obtain consent before a cookie is set for the first time. Provided you get consent at that point you do not need to do so again for the same person each time you use the same cookie (for the same purpose) in future".



The ICO will consider issuing more detailed advice if they deem it appropriate. They have stated in their guidance that this may include further examples of how to gain consent for particular types of cookies as methods develop.

Fortunately for operators of web sites, the ICO has indicated that during the next twelve months it will not be taking any enforcement action against companies that can show that they are considering their use of cookies and working on solutions to the problem of obtaining consent. The key message from the ICO is that inaction is not acceptable.

1.3 How to comply with the UK's current law on cookies

Under the UK Regulations you still need to provide information on how you use cookies on your website. Therefore we still recommend that if your website uses cookies, you should:

- include a link to your privacy policy on all pages;
- explain in that policy how and why you use cookies; and
- include a link in your policy to www.aboutcookies.org so that your visitors can access instructions on deleting and controlling cookies.

Your privacy policy should explain, for example, that you use cookies to count visitors to your website. If you facilitate the delivery and reading of third party cookies on your website, that should also be addressed. The third parties should be identified. If you use Flash cookies, address that too.

The ICO guidance states that it is a starting point for businesses to achieve compliance, In the absence of definitive methods of compliance it is difficult say for certain what steps need to be taken to comply with the UK Regulations. We suggest that businesses should at least:

- audit how their sites operate and receive data from online partners and providers and what they receive to obtain a clear understanding of where cookies are used and for what purpose;
- assess how intrusive their use of cookies is; and
- whenever a new site is developed or an existing one upgraded, or a website-related commercial relationship started, ensure that there are clear details about the operation of cookies and tracking to be used.

The ICO guidance suggests a number of different methods that can be used for obtaining user consent but encourages businesses to find the solution that works best for them.

- pop ups or similar techniques asking for consent can be used. Pop ups are discouraged by Web Content Accessibility Guidelines. They may also spoil the experience of using a website Users can also block pop ups by default, making this impractical;
- consent can be obtained by using terms of use or terms and conditions. In using this option consent is given by the user when they first register or sign-up. If this method is used it is essential that a user is made aware of any changes made to the terms to include consent for cookies and specifically that the changes relate to the use of cookies. It would then be necessary to obtain a positive indication that the user understands and agrees to the changes;
- preferences that users choose when visiting a website can also be used as a means of obtaining consent. Consent could be gained as part of the process by which the user confirms what they want to do or how they want the website to work, provided sufficient information about the use of the cookies is provided. This would apply to any feature where a user is told that a website can remember certain settings they have chosen;
- website features, such as videos, that remember how users personalise their interaction can also determine user consent. In this case, where the user is taking some action to tell the webpage what they want to happen – opening a link, clicking a button or agreeing to the functionality being 'switched on' – then their consent to set a cookie can be asked at this point;
- for use of analytic cookies to gather information about how people access and use a website it may be possible to add a footer or header to a webpage containing text. This text is highlighted or turned into a scrolling piece of text when a site wants to set a cookie



on a user's device. In turn this could direct the user to read additional information, possibly contained in a privacy policy, and make an appropriate choice;

- where a website allows a third party to set cookies the process of getting consent is more difficult. Initiatives that seek to ensure that users are given more and better information about the use of information, for example the use of the "i" symbol, referred to below, should be used. Anyone whose website uses or allows third party cookies must ensure that the right information is delivered to users so they can make informed choices.

2 Impact – What it means to you

2.1 Immediate Impact

Companies are being encouraged to prepare by examining their cookies to see what purpose they fulfil and reach a decision about whether they require "informed consent" from visitors to keep using them.

This review process is important to undertake, because from 26 May the ICO is obliged to investigate any complaints it gets about the use of non-compliant cookies.

"We will look into those complaints and see what that company is doing to work towards compliance," said the ICO. Only by showing the results of this work will web firms be able to convince the ICO they are intent on complying.

2.2 Long Term Impact

2.2.1 Penalty for non-compliance

New powers have been introduced so that a serious breach of the UK Regulations can result in an ICO fine of up to £500,000. Before this the fine was £5,000 and companies may have been willing to run the risk but with these increased powers the result of enforcement action is potentially more severe.



3 Our Solution

At Wolf Software we have spent a considerable amount of time attempting to find a legally compliant solution to the cookie law problem.

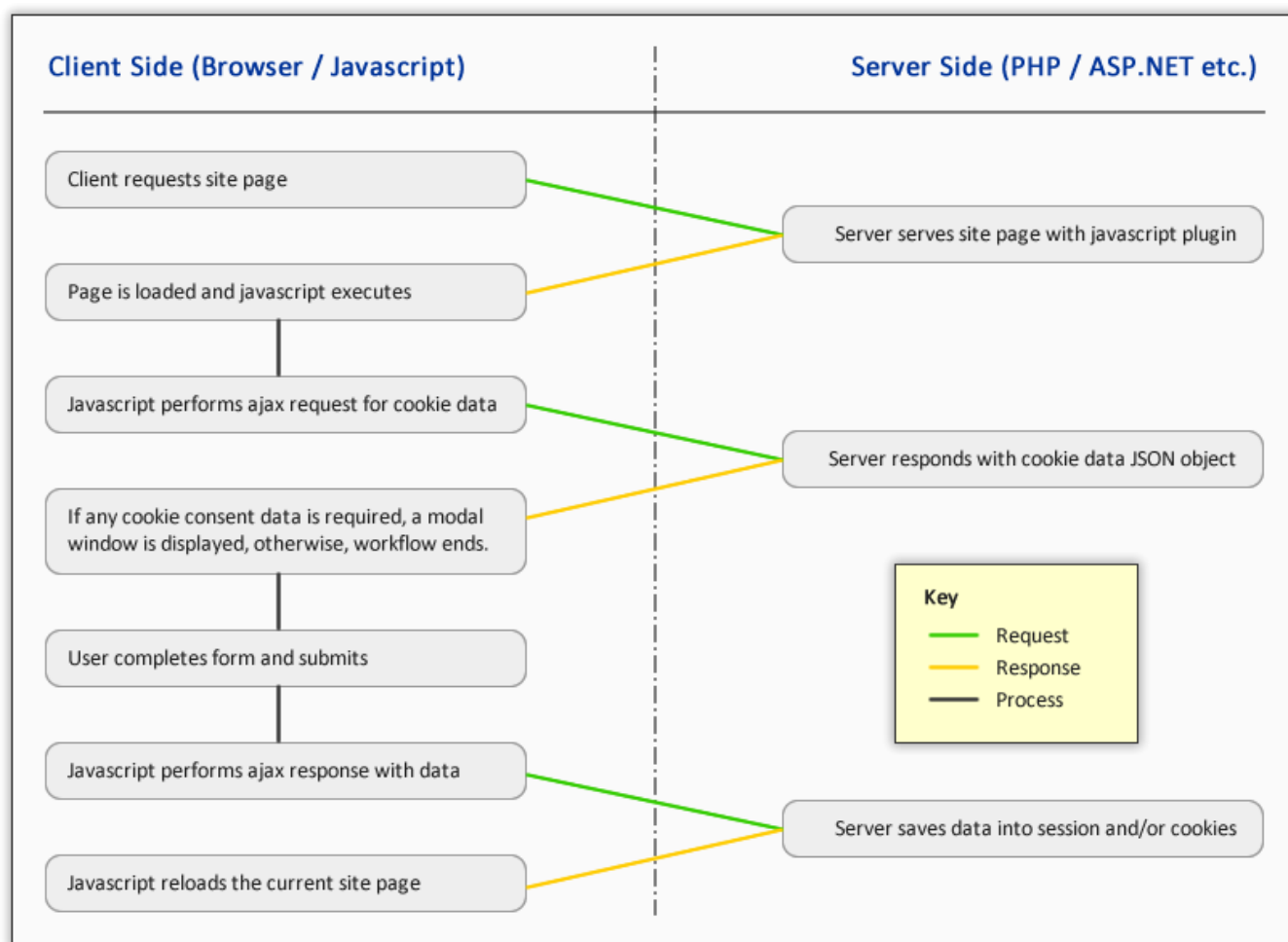
We started off with [jpegrga](#) which is a legally compliant plugin for Google Analytics. This allows you to use GA on your website in a legally compliant way and handles all the prompting of the user and setting of cookies. It is now in use in many sites across the UK and also other European countries. The next step was to write a plugin that could handle any type of cookies and deal with the consent gathering aspect in order to gain legal compliance for any site using it.

3.1 Demonstration

There is a live demonstration of this solution [here](#). It has been tested on as many PC based browsers as possible, and also iPads and mobile phones to ensure it works on as many internet enabled devices as possible.

3.2 The Workflow

In the default setup on a standard website this is the workflow for the plugin.





3.3 Implementation

The 'free' implementation that is available is written in PHP and jQuery (javascript), however the server side part of the solution could be written in any language required and we will be releasing a commercial .NET implementation at the beginning of 2012.

3.3.1 No Javascript ?

If the user visiting the site does not have javascript enabled this is not a problem, they will be presented with a link (which is hidden by javascript so only visible to non javascript users), which will take them to a fallback page, that requires NO javascript to function and allows the user to set and unset there preferences exactly the same as if they had javascript. The fallback page can be renamed as desired and styled to fit the rest of your existing website.

3.4 Installation

Installation is very simple simply download the jpecr package from our website and unpack it. The following items from the archive need to be copied or moved into your website directory.

- assets (directory) – This includes all the key workings of the package.
- fallback.php – This is the fallback page for people without javascript [Note: This can be renamed if you wish]

Once this is done, you have all the workings of the plugin available to you. The final thing that is required is the following code to be placed in the <head> of your website pages.

```
<link href="/assets/css/jquery.jpecr-default.css" rel="stylesheet" type="text/css" />
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js" type="text/javascript"></script>
<script src="/assets/js/jquery.jpecr-0.1.js" type="text/javascript"></script>
<?php
    include_once 'assets/pecr/cookies.inc.php';
    include_once 'assets/pecr/functions.inc.php';
    always_include_plugin(false);
?>
```

The above code is used to do the following:

- Include the style sheets for the plugin – You can change any of the settings in style sheets
- Include the jQuery code – This is loaded from google, but you can load it from any source including locally
- It loads the main jpecr plugin code
- The allow to always_include_plugin decides if the plugin needs to be called on every page load or only when new cookies or unconsented cookies are located. Changing this to true will cause the plugin run on every page, however it will still only show the modal when needed.

Once you have this code in your page and you reload, you should see if pop up and ask for your consent to test cookies shipped with the package, Google, Facebook, Twitter and Newcookie. These of course can be changed to anything you require and should reflect the results of your internal cookie audit.

3.4.1 Getting Consent

Once the plugin has been installed the user will be presented with a pop up modal when they first enter the site, or any time when there are cookies in the list they have not been replied to. They can also click a link (or button) to allow them to change their settings at any time to alter there consent, or to make the consent permanent or not.



3.4.2 Using Consent

Before delivering any cookies you need to check to see if the user has given consent to such content, we have provided a simple function which will do this for you.

Lets use the example of Google Analytics, we ask the user for consent to use this and its associated cookies, and call the cookie 'google_analytics'.

```
<?php

if (have_consent('google_analytics'))
{
    include your GA code here
}
else
{
    The else is optional, but you can use it to offer a link to give consent
}
?>
```

As you can see, this does require a small amount of additional code adding to your site, but the locations should be identified during the cookie audit and the changes are VERY small and simple and allows for complete compliance with the law.

3.5 Customisation

3.5.1 Look and Feel

This solution can be customised in a number of ways. You are free to edit the styles defined in the included style sheet as much as you like so that it fits the look and feel of your website, anyone familiar with CSS should be able to do this. You are also free to change the logo to your own logo (simply replace logo.jpg in the assets directory).

3.5.2 Defining your own cookies

You define your own site cookies by editing it the assets/pecr/cookies.php This is the key file as it defines the name of all the types of cookies that you are using on your site. The following needs to be defined for each cookie

- name – The name of the cookie, this is used for checking consent
- title – The title of the cookie (short description)
- description – A description of the cookie for the user
- more_info – A link (or text) for more information about the cookies, this could be to your own privacy policy
- link – true or false (if the more_info is a link set this to true, else set it to false)
- consent – This is the default and should not be changed, it is set later by reading the users settings
- permanent - This is the default and should not be changed, it is set later by reading the users settings

It is perfectly ok to define cookies in groups, you do not need to specify every single cookie that is used (We checked this with the ICO), so for Google Analytics you can simply ask for consent to Google Analytics once even though it actually sets at least 4 individual cookies. Your cookie audit should allow you to define these groups.

3.5.3 What can't I change?

The only thing that you cannot do is remove the link back to Wolf Software.



3.5.4 Additional Settings

We have added a 'keep alive' feature for people who want to use this, PHP sessions do time out (default is one hour), so if someone visits your site and does not do anything for an hour, and has no permanent settings then they will be prompted again once the session times out. The keep alive if turned on will stop this as it invisibility checks in with the site at a time specified by you, e.g. every 15 minutes.

3.6 What the solution does not do

The solution does not remove the need for a cookie audit, this is something that you must do in order to ascertain what cookies you need to gain consent for. As a minimum you should review all of your cookies and decide which ones require consent and add all of these into the cookie list.



4 Support

4.1 What if I have problems or questions?

If you have any problems using this solution or you have any questions about it or how to use or modify it, then do not hesitate to contact us, we can be reached via email at support@wolf-software.com and one of our developers will assist you.

4.2 Commercial Support

We do not offer commercial support for the free solution, however as above if you email us then we do our very best to assist you, we are however releasing a commercial version with support early in the New Year.



5 Version History

Issue	Change	Date	Author
1.0	Initial Release	18 th Dec 2011	Wolf Software.