# EU Cookie Law: Be Compliant, Not Complacent

New guidance has left businesses with a sense of security about the recently introduced regulations. But is it false?

canddi
who, what, when, now.

## Table of Contents



## Executive Summary

The EU Privacy and Communications Regulations became enforceable in the UK on the 26th May after a one-year grace period. On the day before, the Information Commissioner's Office (ICO) released new guidance for businesses on how they could comply and the potential threats from non-compliance.

This guidance appeared to significantly lower the bar for compliance, and diminish the threats of sanctions for non-compliance. The result has been an almost audible sigh of relief from the UK online business community. But taking a lead from the headlines in the new guidance may be misleading: significant threats remain for those companies who fail to comply, and the burden of compliance may be higher than it first appears.

This document outlines some of the key considerations for businesses looking at compliance in the light of the new guidance and describes how CANDDi's solution, CANDDi Cookie, can help businesses to remain on the right side of both the spirit and the letter of the law.

## Introduction to the Cookie Law

Since 26th May 2012 your business has been obliged to comply with the EU Privacy and Electronic Communications regulations, better known as the Cookie Law.

In short these regulations demand that you inform visitors to your website before you use any mechanism to collect data about them. They also state that you must give visitors a choice about whether they accept these mechanisms – typically a cookie.

Here's the exact wording:

> *"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."*
>
> *Regulation 6 of the Privacy and Electronic Communications Regulations 2003 (PECR)*

Cookies are tiny pieces of code downloaded by your website to the Visitor's machine. They are used by almost all websites for many different purposes. The only exception to the law is when a cookie is *essential* to the purpose of the website. This applies in very few cases.

## The Changing Guidance

Until the day before the regulations were enforced the Information Commissioner's Office or ICO, the UK regulator for all matters of data privacy, had been quite clear that visitors to your website must *explicitly* opt in to receiving cookies. i.e. They would have to click a button at some point that said in essence: "Yes, I am happy to receive cookies on my machine for the purposes you have specified."

At the very last minute – just one day before the legislation was due to be enforced - this guidance changed. The ICO announced that implied consent would now be considered a valid approach to compliance, allowing companies to simply tell visitors that they were collecting data and assume their assent if they didn't explicitly opt out. They ICO also played down the threat of fines for non-compliant businesses.

## Compliance Not Complacency

This was all welcome news, if a little belated. But the sense of security with which it has left businesses may well be false.

Here are six things to consider for your business in the light of the new guidance.

- **The ICO's guidance may not stand up to European scrutiny**
  The new guidance issued by the ICO the day before the regulations were enforced explicitly contradicts its previous notes, yet the regulations themselves have not changed. The new guidance is also inconsistent with the EU's own working party on the subject, which concluded that: "...only in very specific, individual cases, could implied consent be argued."

  The debate about what constitutes compliance may not be over.

- **Compliance depends on the data you collect**
  The burden of compliance is a sliding scale. If you are merely counting people you may be able to get away with 'implicit acceptance' i.e. informing people about the cookies you use and assuming they have no problem if they don't explicitly opt out.

  But the more data you collect about people – even for example, anonymous but detailed data about their browsing behaviour – the greater the expectations on you to gain their consent. Using implied consent for anything beyond the simplest analytics could be open to a challenge.

- **Big corporations may be test-cases, not best practice**
  Some large corporates have taken a very light-touch approach to compliance, assuming the visitor's assent even if they do nothing for just a few seconds. This has encouraged other companies to follow suit, but this may not be wise.

  Firstly the compliance requirement is going to be different for every business, depending on the data they collect and how they use it. Secondly some of these approaches do not appear to be compliant under any interpretation of the rules. You need to consider what you believe to be inside the bounds of the regulations and what is appropriate for your business.

- **A privacy policy is not enough**
  The ICO has been pretty clear that even if you are only collecting the minimum of data, placing information in your privacy policy about your use of cookies is insufficient. You need to make it clear to visitors what data is being collected and how it is to be used, without them having to seek out this information. This means that unless they have previously assented to your use of cookies, you need to be highlighting your policy and practices, wherever and whenever visitors land on your site.

- **You are only compliant if you can prove it**
  Even if you have a compliance solution in place, do you actually know that you are complying with people's wishes? If a specific person, or the regulator, decided to challenge your compliance, could you prove it?

  Imagine the nightmare situation: someone complains to the ICO because they believe you have targeted them based on data collected after they had opted out. The ICO asks you for evidence of compliance. What do you do?

- **Fines were never the biggest threat**
  The ICO has stated that it is unlikely to use financial sanctions against non-compliant companies in the first instance. But what is a fine compared to public suspicion of the way you have used people's data? Honesty and reputation should always have been the biggest drivers for compliance. Nothing in the new guidance diminishes these factors.

## How Can I Ensure Compliance?

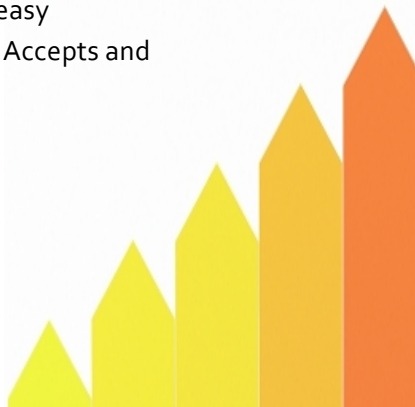
CANDDi Cookie is a full-featured solution for companies seeking provable compliance with the EU regulations. Features include:

- **Decision Interface:** CANDDi Cookie presents first time visitors to your website with a dialogue box in pop-up, banner or modal format (centred with rest of screen greyed out), explaining that the site uses Cookies and why, linking to your Privacy Policy and giving the user the option to accept or reject cookies, via both explicit and implied methods. The dialogue boxes are completely styled to match your site.

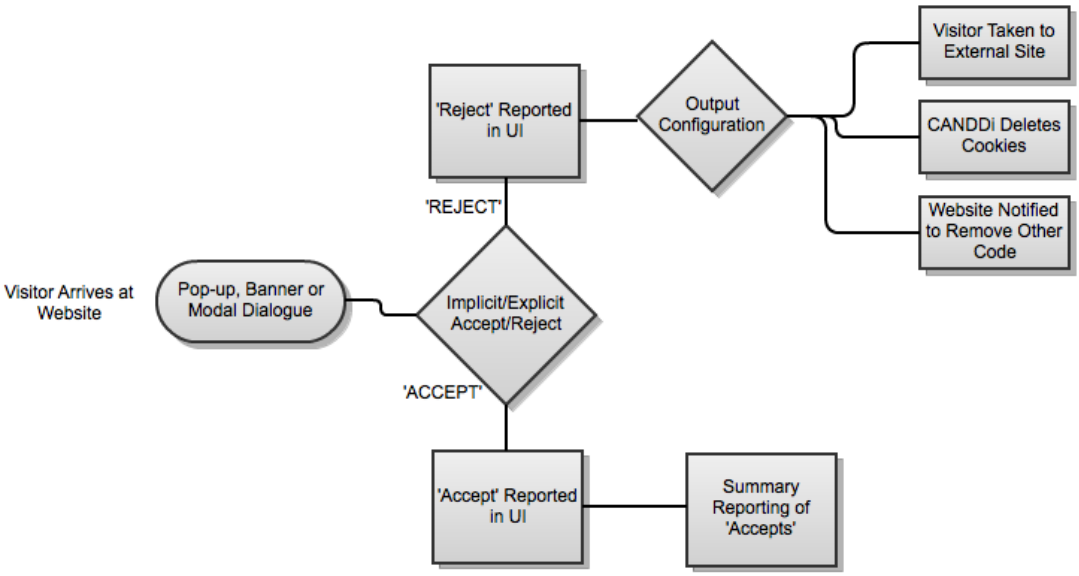
  CANDDi Cookie allows you to experiment with different dialogue options so that you can choose the best option for your business. For example you could try a popup on one day and a modal box on the next, and CANDDi's summary reporting will show which one achieved the greater acceptance rates.

- **Response Management:** CANDDi Cookie allows you to choose how you respond when someone rejects Cookies. Visitors can either be redirected to an alternative page (for example, providing basic information and contact details but explaining that they can't browse the main site without accepting cookies), or allowed to continue browsing but with tracking disabled.

- **Audit Trail:** CANDDi Cookie provides a full record of all Visitors who accept cookies for future reference. The decision is available to view in each Visitor's individual profile via the CANDDi user interface, or as a summary Stream of all people who have accepted and when that can be exported into a spreadsheet for easy reference. CANDDi also provides a summary report on the number of Accepts and Rejects in each period.



- **Tracker Blocking:** CANDDi Cookie allows you to choose how to implement compliance for your site (see flowchart below). You define which cookies are essential to the operation of your site (and so allowed under the EU Directive) and which should be removed. When a Visitor chooses to reject cookies, CANDDi Cookie can delete all of the specified first party tracking cookies from their machine. CANDDi can also notify your site not to render certain elements – e.g. third party tracking code – if required.




## Get CANDDi Cookie

CANDDi Cookie is a simple, cost-effective way to achieve compliance without changing the fundamentals of your website.

Want to get compliant with CANDDi Cookie? **Talk to us today**.

Tom Cheesewright
tom@canddi.com
+44(0)161 242 7234