

# The EU ePrivacy Directive - What it means to our clients

## Introduction

The EU ePrivacy Directive came into affect on 25<sup>th</sup> May 2011 which focused on website cookie ruling. The key substance of the change will be a move to an 'explicit opt-in' from a 'right to opt out'. This note has been put together to give our clients practical advice on how it affects web analytics, and draws from statements already made by key influencers such as Adobe.

## Background & Summary

The EU ePrivacy Directive has been revised and came into effect on 25<sup>th</sup> May 2011. Whilst most of the directive is aimed at ISPs, the section of concern to site operators covers any information that is read from or written to a user's device from across the Internet. What has become known as the "cookie directive" is clear in that it states explicit consent must be given before a cookie is set on a user's device. The Information Commissioner's Office (ICO) has issued guidelines indicating that the only exceptions would be where a cookie is used to provide an invaluable service on a site (such as maintaining a shopping basket). Analytics cookies are not deemed essential and the guideline explicitly states "the exception would not apply....if you decide to use a cookie to collect statistical information about the use of your website."

The law is actually being managed and introduced by The Department for Culture, Media & Sport which the ICO will then regulate. The ICO is likely to issue more detail and examples in the future. In the meantime companies are (extremely) unlikely to face any sanctions in the short term as the situation is so unclear. In fact Communications Minister Ed Vaizey has said "Therefore we do not expect the ICO to take enforcement action in the short term against businesses and organisations as they work out how to address their use of cookies." Failure though, to take any action before 26 May 2012, could result in a significant fine.

No web analytics vendor (to our knowledge) has a solution, or issued anything other than a holding statement.

Companies however should NOT ignore these regulations and the ICO states that in the event of a complaint, it will look more leniently on those who have started to make changes and have a realistic plan.

## What site owners should do now:

1. Make sure your privacy policy is up to date. This should accurately describe how you use your customers' data as well as the data practices on your site, including your use of analytics software and your advertising practices.
2. Make sure your privacy policy includes a link to the page to opt-out of the analytics services offered by your analytics' provider (or other services that have opt outs). Ideally, the link to the opt-out page should also be included somewhere more obvious on your website in addition to your privacy policy.

## 3. Create a plan

- a. Audit your site to determine what cookies and local stored objects you use on which pages, & why
- b. List the data each cookie enables
- c. Score these cookies based on their privacy issues, e.g.0 for essential usage of site, 3 for behavioural targeting
- d. Any 3<sup>rd</sup> party cookies in particular should be identified, as any consent for these must be very clear
- e. For each cookie, determine what the possible solutions to obtaining consent might be
- f. Speak to each of the suppliers responsible for the cookie
- g. Detail the actions you plan to take
- h. If you cannot think of an alternative, justify why it is critical to you

Logan Tod & Co would be happy to work on specific projects to help clients assess their situation, create this action plan and possible consent routes. The current solutions to be considered include:-

- **Browser settings** - Implied consent from current browser settings is **not** deemed sufficient by the ICO. It does appear to be a favoured future route but requires that browser software is enhanced to support clearer consent. It might be an option in the future, but could be flawed in that it will only be suitable for the segment of users upgrading to a new browser
- **Pop-up screens** requesting consent to set cookies when a user visits the page, with clear explanation as to how they will be used, is the obvious but intrusive option
- **Terms and Conditions acceptance** - capturing cookie consent in the way T&Cs are frequently obtained
- **Settings, functional and feature led consent**; as long as it is explicitly stated, consent can be gained when users sign up to features on a website (such as remembering preferences)

## Disclaimer:

This article is for guidance only and has not been reviewed by a lawyer and the author takes no responsibility for the advice given. Organisations should seek guidance from their own legal advisors as each situation is different and companies will have their own attitude to risk and approach to privacy considerations.

## Further Reading

[http://www.ico.gov.uk/~/media/documents/library/Privacy\\_and\\_electronic/Practical\\_application/advice\\_on\\_the\\_new\\_cookies\\_regulations.ashx](http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx)

[http://www.culture.gov.uk/news/media\\_releases/8051.aspx](http://www.culture.gov.uk/news/media_releases/8051.aspx)