BANNER®

Here comes the Cookie Monster

Making sense of the EU Data Protection Legal Framework

Introduction

Today, nobody should need telling that privacy is a big deal. No matter that thousands of people regularly share the deepest secrets of their souls (and the accompanying pictures) with 'friends' on Facebook, the merest sniff that a company is abusing users' privacy and all hell breaks loose. **(We saw this not so long ago with Facebook itself.)**

For those of us involved in direct digital marketing, the rules around double opt-in and personally identifiable information (PII) are now pretty clear and commonplace. There are some exceptions at a country level – Germany being a prime example of where the rules on informed consent are more stringent. But overall we understand that in order to market to an individual, they must give their permission to be marketed to. They might do this directly or via an agreement with a third party such as a publisher. But as long as they do and we give them the opportunity to unsubscribe, everything is fine.

Of course, even from a purely business viewpoint, this makes perfect sense. As the UK's information commissioner, Christopher Graham puts it, "Get privacy right and you retain the trust and confidence of your customers and users; mislead consumers or collect information you don't need and you are likely to diminish customer trust and face enforcement action."

It's all a matter of trust.

That was then this is now?

While things are relatively simple for outbound email-based communications, they're about to get a lot more complicated for everything else.

The issue, in a word, is cookies. Specifically, the use of cookies to track people as they move from site to site. This is becoming even more of an issue with the growth in retargeting technologies that allow us to serve buyers with relevant messages based upon their previous behaviour.

The view of the regulators is that, in terms of privacy, using a cookie on a customer's PC to track them is no different than using their email address to market to them. As such, they should know that this is happening and, crucially, give their explicit consent. Importantly, it is no longer enough to bury information about your use of cookies in your site's privacy policy.

This has profound implications for today's marketers.

In this Insight article, we'll take a look at what the new regulations say and what they might mean for your marketing.

Just before we start, one thing we should make clear – **we are not lawyers**. This is our understanding of the situation (informed by our partners at Eloqua, advice from the **Information Commissioner's Office** and our association with the Internet Advertising Bureau). You should, as a matter of course, take legal counsel before acting on anything you read here. We cannot take responsibility for the legality of your campaigns.

Right, now that we've got our own lawyers off our back, on with the show...

The EU Data Protection Legal Framework

The snappily titled 'Directive 95/46/EC' is focused on protecting individuals when it comes to the processing of personal data. The equally memorable 'Directive 2002/58/EC' concerns itself with the protection of privacy in electronic communications. Together they make up the bulk of the new EU data protection regulations and came into effect on 25th May 2011.

Essentially these directives deal with two areas:

1. **Personal data** – ie information that can be used to identify an individual. This includes name, age, gender, address (business or private) or email. Critically, *it also includes the behaviour connected to that individual*.
2. **How personal data is processed** – including its collection, recording, storage, use and disclosure.

While these laws are a European requirement, they apply to any business collecting or processing data through any establishment or equipment located in the EU (ie servers). There is also some debate whether for cookies this means a user's individual PC. Ultimately, it probably pays to be paranoid.

Setting the ground rules

Many of the core principles will be familiar to anyone who runs outbound email campaigns. Data must be processed fairly and lawfully, and used only for the purposes for which it was collected. It must be accurate and kept up to date. You must allow people to change or erase incorrect information about themselves. And you mustn't keep the data longer than necessary.

The differences come more in what you need to tell individuals about the data you hold on them – and remember, we're talking cookies here.

While individual countries are enacting the new regulations in sometimes slightly different ways, the principles are the same. The UK version sums it up well (with not too much legalese):

> *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 Version 1 2 09/05/11 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.*

What this (and the wider directive) means is that users need to know who you are and why you're setting a cookie. They need to know what data you're capturing and who you will be transferring it to. And they need to know the possible consequences if they do not disclose their data. All this is in addition to the right to correct and/or remove data you hold on them.

It’s all about consent

As with the existing rules around email communications, compliance is about the people you are tracking giving their informed consent.

The key word here is ‘informed’. This means they know specifically what they’re agreeing to and that you only collect data to fulfil on their requests. You are allowed to process the data you collect for legitimate business purposes – but the individuals’ rights always come first. This means you should assume that specific consent is always required.

Of course, while this is a relatively straightforward exercise when someone opts in to receiving communications from you, it is intrinsically more complex when you are using real-time tracking via cookies to target and retarget people across the web.

There is currently some discussion about whether a user's browser settings could be used. In this proposal, if a user has amended their settings to allow certain types of cookie, that could be taken as consent to drop specific types of cookie on their machine. However, right now this is just a proposal and cannot be relied upon as a workable solution (though in our eyes it has many merits).

Ultimately, it is likely that you will need to obtain specific consent (in the same way you currently do for opt-in communications) to use cookies.

Gaining consent - the options

There are multiple ways you can seek and obtain people's permission to set a cookie. The easiest is to ask as part of an opt-in registration. However, this is not the only way and does not cater for existing customers who have already opted in for one type of communication (eg email) but not for others.

For this group, you could look at building a consent request into new, high value gated content. In the same vein, you could also open up new features of your site that require cookies - eg personalisation, wishlists, content monitoring and notification, personal libraries etc.

You could consider using pop-ups and splash pages. However, many users have pop-ups disabled and a splash page may make too much of the issue, deterring users in the process. We wouldn't recommend it as an approach.

Of course, you could proactively reach out to users, explaining the benefits to them personally of allowing a cookie to be set on their PC and incentivising a response (eg with a competition or offer). This is a more transparent way of approaching the issue for existing users and could help negate suspicion over the issue.

Ultimately, the key is that the user should get something in return. Carrots not sticks.

Being open

While cookies are the main focus for the new regulations, there is also concern over the retargeting of customers with banner ads based on their behaviour.

There is, of course, little scope for full disclosure within the limited screen real estate available. That's why the Internet Advertising Bureau (IAB) is creating an industry-standard symbol (shown) to help viewers spot a retargeted ad. They have also created a set of best practice guidelines which focuses on three principles:

1. **Notice.** Companies must give clear and unambiguous notice that they are collecting data for behavioural advertising purposes (whether on a third party site or on their own domain).

2. **User choice.** Users should have the opportunity to decline behavioural ads and be given information on how to do so. They should also give consent for their data to be processed.

3. **Education.** Companies should make information about behavioural advertising (and their use of it) easily available in a readily understandable format.

The IAB have also launched a pan-European consumer website for individual privacy preferences management: **www.youronlinechoices.eu**

What you should be doing right now

The new directives came into force on 25th May 2011. For many clients across many campaigns, there will be little to worry about. In addition, in the UK, the Information Commissioner's Office has indicated that compliance will be phased in gradually and that marketers will be given time to address issues as they arise.

However, for those using retargeting there are a number of actions to consider right now:

- For ads retargeting anonymous customers in online advertising – the main action lies in adding a way for people to know they are being tracked and to opt out if they so wish (eg by using the IAB's enhanced icon)

- For tracking anonymous visitors across your site – our understanding is that no action is required at present if you are using 1st party cookies (which are not covered by the directives). We should point out, however, that there is some debate over this. If you are using 3rd party cookies (eg such as those from Eloqua) you will need to gain consent

- For beginning to track new visitors who register personal information – amend your opt in declarations to include the use of their personal data for tracking purposes

- And for extending the use of previously registered users' data to include tracking – you will need to gain their explicit consent to do so

In addition, we would also recommend:

- Apportioning responsibility for data privacy within the context of behavioural advertising with publishers and ad networks

- Ensuring the privacy policy on your website sufficiently discloses the use of cookies and how they will be used

- Providing a simple means for users to provide explicit consent or opt out

- And consider making "do not track" functionality compatible with the latest incarnations of browsers from Microsoft, Google and Mozilla

Tracking and retargeting technology is a powerful way of increasing responses and improving user experience. We have used it and seen it work across a wide range of our clients. While the new directives do place an additional burden on today's marketers, the results to be gained are, in our opinion, more than worth it.

Want to know more?

If you would like to discuss how you could use this technology to improve results for your brand (all while staying within the new directives) we'd love to talk.

Email **Michael Wrigley** at **michael@b1.com** or call him on **020 7349 2266.**

Follow us on: **Twitter: @bannercorp**

And keep up to date at: **www.b1.com/blog**