Guidance on Auditing Third-Party Cookies

April 2021

Responsible Marketing

Data & Marketing Association

Contents

Introduction

Since the Information Commissioner's Office issued their Guidance to Cookies in July 2019, many of the templates, processes and procedures that used to be common practice are now unlawful.

Why the change?

- The ICO has expressed some concern about profiling, not only on social media, but algorithmic and electronic profiling in advertising. This is following on from the Cambridge Analytica scandal
- Existing laws, such as PECR have been updated and brought into line with GDPR
- The ICO has expressed concern about websites that offer services to the public, who also collect website visitors details for marketing; especially if these services relate to children or collect special category data for health services

What has the ICO done to address this?

- The ICO has issued guidance on cookies, marketing, artificial intelligence and machine learning and data ethicsThe ICO has opened a public portal for data subjects to report websites which break the rules
- The ICO has issued guidance to the public about their data rights, so the public are more informed about the use of cookies.

What are the changes?

It is important to remember that these are not changes, more like clarifications on the use of cookies to align with GDPR and PECR. The clarifications are outlined in the new guidance and associated cookies best practice. The main points are:

- Cookies that are used for marketing, require consent, before they are placed. This includes tracking cookies within emails. The consent will need to be renewed periodically
- As per the Privacy in Electronic Communications Regulations (PECR), continuing to browse a website does not constitute consent to cookies being placed on a browser. This is also contrary to the GDPR principle "Privacy by default and by design"
- "Essential cookies" are cookies that are essential to the function of the website (such as shopping basket and payment functionality)
- Analytics cookies are not essential to the function of the website for the user; therefore, consent is needed for you to place them on a browser
- "Paywall consent" is also no longer lawful, as this means that consent is not meeting the GDPR definition of "freely-given" as consent is conditional to being able to access the website and associated services
- Consent must meet the GDPR definition, in that it is "freely-given, clear affirmative action"; obviously, this means "opt-in". Legitimate interests are not applicable, as per PECR

Case Study

A healthcare charity offers healthcare services, advice and guidance; but also, a retail shop, and fundraising (marketing) on their website. For further clarification on the differences between service and marketing messages please see the DMA Service Message Guidance, here.

Accessing the website and continuing to browse means that first and third-party cookies are placed on the browser.

The daughter of a gravely ill patient looks on the website for advice and guidance and to apply for support services.

The same day, her social media pages are filled with advertisements which talk about death and dying, and which ask her to fundraise. When she clicks on the advert to find out more about "why am I seeing this advert/" the social media page informs her that she is being shown this advert as the charity wants to target people who have visited their website recently.

The daughter finds this extremely insensitive and intrusive and complains to the charity and asks why cookies were placed on her browser and given to Facebook without consent.

Risk:

- The daughter could complain to the ICO and report the charity
- The daughter could stop supporting the charity
- The daughter could tell her friends and family or go to the media about this, meaning reputational risk.
- The ICO could investigate, audit and there could be financial and non-financial penalties imposed.

Approach to Auditing your Cookies

If you operate a website, that places cookies used for marketing, either first party cookies, or third-party cookies, you are responsible for the data collected at that point. You are responsible for how you use that data and responsible for how that data is processed by third parties. You must understand what is happening to all the data collected.

To do this, you will need to have an up-to-date record of all websites that are associated with your brand; including those built and hosted by third party processors; as long as you are the controller for the purposes of the processing, or a joint controller of the data. It is recommended to audit affiliates even if you are not the data controller as they could still be hurting your brand with unauthorised cookies.

As per GDPR, even if those websites are hosted outside of the EEA, if those websites "solicit" or "process" the data of EEA citizens, they fall under the territorial scope of GDPR. "Soliciting" could be offering the website in European languages, offering payment in European currencies, or offering shipping to European destinations.

For each website you will need the purpose of the processing, such as a lottery, services, information and support, chatrooms, gaming.

You will need to go into each website and look at the default landing page cookies. This is particularly important for websites that are built and hosted by third parties.

If you are collecting personal data (such as on web-forms) you will need to make sure that the website is secure by having an up-to-date SSL certificate and/or other security features.

You will need to understand all current and planned campaigns which rely on passing cookies that you have collected on your website to advertisers, particularly Social Media Pages.

You will need to understand what third party controllers do with data that you pass to them; whether they use them for their own purposes and who they sell data to. For example, Facebook will use personal data to sell on to as many different advertisers as possible. You need to be able to explain this on your website cookie policy.

Approach to the Change

It is good to take an iterative approach to cookie notices. Try different wording that explains the purposes of the processing and test what affect that has on consent opt-ins.

You can try different placement of the cookie banner, or of the opt-in mechanisms. For examples, please see the DMA Cookie Guidance, here.

Look at research into what other organisations have done and see what has worked and what has not worked.

You must plan for the likely outcome that you will not be able to pass as many third-party cookies to marketing agencies as you used to, as people may not give consent. Look at research which investigates the effect of asking for consent on cookie volumes. The DMA Cookie Guidance here has more information about types of cookies that may be used.

Communicating Privacy

Cookie Policy:

You must have an up-to-date Cookie Policy which explains:

- What cookies are and what they do. This should be in plain English and accessible
- First Party Cookies: the cookies that you use and why you use them, including analytics trackers and pixels
- Third Party cookies: If the cookies are passed to a processor (who only uses them for your purposes) or a controller (who may use them for their own purposes)
- The purposes of those cookies, and whether they are essential or non-essential and what this means
- How to withdraw consent (it must be as easy to withdraw consent as it is to give it)

It is easier to do this in a table format. You can find more information about privacy notice standards here.

Cookie consent and fair processing notice:

On the first visit to your landing page, a user must be able to opt-in to analytics and marketing cookies being placed on their browser. There is no need to ask for consent for essential cookies, these fire automatically.

Therefore, a cookie banner with a fair processing notice should be in a pop-up or other banner, window, or prominent place to allow the user to consent. There is no need to list every cookie and ask for permission for them, you can group analytics cookies into one group and marketing cookies into another group.

They should be allowed to opt-in and opt-out of analytics and marketing cookies, either with a yes/no radio button, or a toggle switch. This allows for the option for them to withdraw consent easily should they wish to at a later stage.

There should also be a link to the cookie policy should the user wish more information.

Template for Communicating the Audit

Your organisation may well have taken an organic approach to adding cookies from various teams within the business: insight, marketing, technology and so on. The more that you engage stakeholders in this process, the better. Actions can be approved faster and there can be more accountability for the technology that is in place.

The first question to ask should be whether a centralised list exists of all the cookies that appear on your site. If the answer is no, your next action should be to log all the cookies you can find on your site. Then ask each team to identify them and their exact purpose.

Although this might be a difficult task, it's essential to know what you're managing before writing a cookies policy or setting up a preference centre. It's vital to minimise complexity to clearly explain the cookies you use. For instance, if you carry no advertising, there is no point talking about advertising cookies.

Areas to cover in your audit include:

1. Identify and engage with all the stakeholders. These may include the marketing, IT, legal and compliance departments. Be aware of the feedback being received from external agencies and how that is affecting stakeholders
2. Identify which cookies are already on your site, using a combination of browser-based tools and server-side code review
3. Identify what your contractual arrangements and validate the customer experience of these.
4. Confirm the purpose of each cookie with an owner of the cookie named as being a department or team
5. Confirm whether the cookies are linked to any other information held about users, such as usernames
6. Identify what each cookie holds or processes
7. Confirm the type of cookie: persistent or session
8. Categorise cookies and distinguish between those which are strictly necessary and non-essential
9. Review the consent mechanism, to ensure users can control the setting of non-essential cookies
10. Determine the lifespan of any persistent cookies and whether the duration is justifiable
11. Define which cookies are third-party or first-party; if third-party, understand who is setting them up and the legal basis of the processing

12. Ensure the privacy notice provides accurate information about each cookie
13. Confirm what information is captured by third parties and what users are told
14. Document the findings and agree an appropriate review period, considering any guidance released by regulators. We recommend a minimum review annually

For more information, you can find a Glossary of Terms for Cookies and Adtech, here.

About the Privacy Working Group

The DMA's Responsible Marketing Committee's Privacy Working Group is a cross council collaborative initiative focused on privacy in data marketing.

The aim of the Privacy Working Group is to support how marketing practitioners should apply the principles of privacy to data and marketing with a particular emphasis on ethics and transparency.

They identify and fulfil any privacy knowledge gaps in the needs of the industry by providing guidance and explore emerging privacy technology.

About the Responsible Marketing Campaign

Working responsibly means putting your customer-first at each and every touchpoint, in each and every interaction.

It is inherent to how the DMA works – and how we encourage the UK's data and marketing community to work.

That means growing an appreciation of, adhering to and ultimately implementing best practice in marketing approaches, especially in light of the arrival GDPR.

These changes to the governance of data have far-reaching consequences for your business, and are still making waves.

At the DMA we aim to demystify this new regulatory environment so you and your customers can benefit. Access our GDPR guidance series - developed in accordance with the ICO - to help you on your journey to GDPR compliance.

Our suite of best practice guides tackles a range of key marketing challenges, and are infused with the real-world knowledge of experts and leaders from around the UK data and marketing industry.

The DMA's events calendar is packed with legal update sessions, morning briefings and webinars that harness the expertise of our Public Affairs, Legal and Compliance teams.

Through our world-renowned Institute (IDM) we offer on and offline learning across responsible marketing themes, at individual and corporate levels. And through learning initiatives run by DMA Talent we ensure the next generation of marketing leaders emerge into the industry fully aware of how to work with a genuine customer-first ethos. Responsible marketing is in everything we do well.

Head to our campaign hub to learn more, and get involved.

About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focused principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

Copyright and Disclaimer