# A Guide to Cookies and Compliance

Responsible Marketing

DMA
Data & Marketing Association

# Contents



Copyright / DMA (2020)

# Background

In the UK, the Information Commissioner's Office (ICO) issued guidance on the use of cookies in July 2019[1]. The guidance was produced to clarify existing legislation in view of the requirement to apply a GDPR level of consent.

The DMA Cookie Guidance Group has prepared this guidance, which we hope complements the ICO's document while being user friendly for all types of organisations.

The guidance includes information about different types of cookies, best practice and use cases. It focuses on helping marketer use cookies in a compliant and innovative way while putting consumers' needs first.

Ultimately, our aim is to improve awareness of, and compliance relating to, cookies - increasing the overall size of the market and revenues as a result. We hope you find the guidance useful.

[1] https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar technologies-1-0.pdf

Copyright / DMA (2020)

# Introduction

Cookies are covered by the Privacy and Electronic Communication Regulation (PECR). However, PECR does not include a definition of consent, deferring to the latest data protection legislation - in this case, the GDPR or Data Protection Act 2018 (DPA2018). Therefore, to place cookies, or use similar technologies, organisations require a GDPR level of consent: freely given, specific, informed and unambiguous.

Cookies can be personal data - because they contain enough information to identify or indirectly identify someone - so obligations under the GDPR and PECR apply. This includes ensuring that an individual has consented to the use of their personal data within a specified scope.

Before placing cookies on a user's device or using the data in cookies, the individual must be given enough information about the use of their personal data, and advice on how they can agree or object to such processing.

Questions organisations often ask as they bid to help consumers understand cookies include:

- Why do we need cookies?
- How do they relate to privacy by design and PECR?
- Where do they sit in relation to the GDPR; the ICO's guidance; PECR; and legislation in other European markets?
- What about competition law and using perceived misuse of fundamental privacy rights to enforce competition?
- Are relevance, control, and compliance equally important?
- How useful are cookies to customers?
- Are there opportunities to improve user experience though innovation and creativity?

Copyright / DMA (2020)

# Cookies, GDPR and PECR

Cookies and similar technologies are governed by PECR, which sits alongside DPA2018 and the GDPR.

If your organisation uses cookies, you must comply with both PECR and the GDPR. It's important to remember that PECR applies to all data, not just personal data.

PECR gives people privacy rights in relation to electronic communications, specifically covering the placement of cookies or similar technologies that track information about people accessing a website or other electronic service on a device.

PECR requires that users or subscribers consent to cookies being placed or used on their device.

## Informed and Unambiguous Consent

If your website tracking is not essential for it to operate - for example, transferring data from one page to another as the user browses - it is likely to require consent. Analytics cookies are not considered to be essential.

Marketing cookies require consent because the intended use of an individual's data is often unclear. Cookie tracking has historically been widely used for online marketing without much oversight or regulation. While it has become the norm, it is a tracking method that is invisible to the individual. This lack of visibility and transparency has been deemed intrusive to the user by legislators and regulators.

Application of the GDPR means the way people are tracked on websites must change. If you're using tracking for marketing purposes you must tell people, giving them enough information - easily available at the time of the consent decision - for them to say they have been adequately informed, and have consented to the form of tracking described.

## Recording the Consent

Access to the information described above is only part of the process. The individual must then be given the opportunity to consent to the tracking. The consent process must not be pre-ticked or designed in such a way that makes it harder for someone not to consent.

Information about the tracking that is recording personal data can be categorised by the type of cookies being used, such as analytics, marketing or third party. This information should be obvious to the user and presented to them before they are tracked.

The default tracking position must be 'off' and the individual should be able to close the consent management process, without changing any preference to 'on'. However, you should also allow options to switch on each type of tracking.

Copyright / DMA (2020)

## Openness, Transparency, and Proportionality

It's vital the description of your choice of tracking is open and transparent. You should never exclude information because you don't think people will understand or approve of it. Nor should you over-complicate the explanation, making it difficult to read.

Initial information provided could contain links to further detail about the cookies, who they are set by and for what purpose.

Consider the number of cookies you are using to track people's personal data: is the amount of data that you are sharing with third parties proportionate? Are you getting value from the amount of data which you are sharing with third parties? Have you considered trying to minimise the use of personal data? Or considered alternatives, such as anonymisation and pseudonymization?

There are several other pertinent questions you should be asking:

- Can you explain to a user why you need to track them, gather and share this information with third parties and do you believe consumers will find these uses reasonable?
- If you are using retargeting, do you understand how an individual's personal data will be used or transferred elsewhere?
- To what extent is user data being shared within the network and could you explain what is happening to the data without confusing the user?

Copyright / DMA (2020)

# How Cookies Work

## What Cookies Do

Cookies are an efficient way for website owners to store an individual's personal information without having to keep and process all their activity data.

Cookies capture information about a user's online behaviour, browsing history and buying habits. They might record on-page dwell time, links clicked and even preferences for page layouts, colour schemes and so on.

Without cookies, online shopping would be much harder. The benefits include smoother interaction for the user with sites they visit frequently. Cookies can also be used to store shopping cart data as items are added to an online basket.

Marketers can use browsing history to infer a user's preferences. They can develop a profile of the individual to serve targeted advertising relevant to the user's interests.

## How Cookies are Created

Cookies are created when a user's browser loads a particular website or accesses online content. The website sends information to the browser, which then creates a text file - placed on the user's device - reflecting certain personal information associated with the user.

This allows the website to recognise them on subsequent visits. Each time the user visits the website using the same device or subscriber identity, the browser retrieves and sends the text file to the website's server, so it knows the user has returned.

Besides the website being viewed, cookies are created by external websites that run ads, widgets or other elements on the page being loaded. These cookies affect the ads displayed, or how widgets and other elements function on the page. They create a log file recording decisions made by the user. For example, a user may wish all information to be displayed in English.

By analysing the log file sent with the cookie, it is possible to track which pages the user has visited, in what sequence and for how long.

Copyright / DMA (2020)

## Types of Cookie

**First-party cookies:** Created by the website the user is visiting.

**Third-party cookies:** Created by organisations other than the website operator. Along with other types of cookie, they help with analytics as well as online advertising.

**Persistent cookies:** Can be used to recall user preferences, settings, and information for future visits. Persistent cookies provide convenient access to information, enhancing the user experience. Once set, they expire on a specified date.

**Secure cookies:** Also known as an HTTPS cookie, they are only transmitted over encrypted HTTPS connections.

**Session cookies:** Used to remember a person's actions as they navigate a website. Typically, the cookie 'remembers' information, or the contents of a shopping basket. A session cookie is deleted when the user closes their browser.

**Super cookies:** Designed to be permanently stored on a user's computer.

**Zombie cookies:** Recreated after deletion from back-ups stored outside the web browser's dedicated cookie storage.

## Cookie Usage

**Analytics:** Analysing a user's activity on a website.

**Personalisation:** For user preferences e.g. language, font settings, themes, etc.

**Session management:** Log-ins, shopping carts, game scores and other factors the server must remember on behalf of the user.

**Tracking:** Recording and analysing user behaviour.

## Cookies and Similar Technologies

Functions usually performed by a cookie can be achieved by other means e.g. using certain characteristics to identify devices and analyse website visits.

PECR applies to any technology that stores or accesses information on the user's device. This could include, for example, HTML5 local storage, local shared objects, and digital fingerprinting techniques.

Copyright / DMA (2020)

# Using Cookies Compliantly

## Cookie Audits

Your organisation may have taken an organic approach to adding cookies from various teams: insight, marketing, technology and so on.

Ask firstly 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 find and log all the site's cookies, 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.

A clear explanation to users of the cookies in use, minimising complexity, is vital. For instance, if your site carries no advertising, there is no point talking about advertising cookies.

Areas to cover in an audit include:

- Identify which cookies are already on your site, using a combination of browser-based tools and server-side code review
- Confirm the purpose of each cookie and name the department or individual responsible for it
- Decide whether cookies are linked to any information held about users, such as their name
- Identifying what each cookie holds or processes
- Confirm the type of cookie: persistent or session
- Determine the lifespan of any persistent cookies and whether the duration is justifiable
- Categorise cookies to distinguish between those which are strictly necessary and non-essential
- Review your consent mechanism to ensure users can control the setting of non-essential cookies
- Define which are third-party or first-party cookies; if third-party, understand who is setting them up and the legal basis of processing
- Ensure your privacy notice provides accurate information about each cookie
- Confirm what information is captured by third parties and what users are told in relation to this
- Document the findings and agree an appropriate review period

Copyright / DMA (2020)

## Categorisation of Cookies

Following collection, cookies must be grouped into clear and easily defined categories.

You could use your organisation's Data Protection Impact Assessment process to help do this, based on how intrusive cookies are to the user. The more unexpected and intrusive a cookie is, the more information you need to make available.

It's possible to set essential cookies without consent. For all other categories, you need to secure GDPR-level consent.

## Essential Cookies

Cookies solely used to facilitate communication on the site. They are deemed strictly necessary to provide the service required by a user. This might include:

- Items in a shopping basket on an e-commerce site
- Cookies regarding compliance with the GDPR security principles e.g. online banking. These can cover activities necessary to fulfil the service, such as repeated failed logins
- Cookies that ensure page content loads quickly and effectively
- First-party session cookies used for authentication purposes; persistent cookies sit on a device so require consent
- Streaming media, which forms part of the service but not for personalisation or usage monitoring (which would require consent)
- Load-balancing purposes, where cookies are only used for this purpose on sites and apps
- Session cookies that store a user's preferences (but not persistent cookies that save preferences, which require consent)
- When users are logged into a social media platform, and the service includes plug-ins and other tools provided by that platform

If strictly necessary cookies are used for additional, non-essential reasons, these purposes must be communicated separately and would require consent. If consent is not given, the user must be able to switch them off.

Copyright / DMA (2020)

# Non-essential Cookies

These cookies require consent:

**Analytics**

- Any cookies that help the website to understand the patterns of traffic and site usage e.g. Google Analytics, Adobe Analytics
- Analytics tools that don't directly rely on cookies for identification but may use an IP address, beacons, etc
- Demand Management Platforms (DMPs) - or other customer data platforms - which employ AI to automate the creation of customer segments

**Advertising**

- First-party cookies dropped by the host website (usually but not always a media site), allowing the host to understand site usage and serve relevant ads
- Third-party cookies e.g. ad tech companies, direct advertisers or other organisations interested in understanding usage of the host website. This might cover frequency capping, ad affiliation, click fraud detection, market research, debugging and so on. The host must seek consent on behalf of the third party

**Personalisation**

- Used to understand the patterns of an individual's behaviour on a website, so you can determine the next content to be served to that individual
- Cookies that identify a user, so on their return to a website they can be presented with a tailored greeting
- Cross-device tracking, where cookies are placed on a user's device to link it to their personal account as part of a browsing record

**Social media**

- Non-logged in users of a social media platform who are using social media plug-ins; users who have logged out or who are not members
- Any social media tracking via device cookies, whether for social media members or non-members

**Marketing**

- Any cookies dropped onto a device as part of a retargeting campaign, after someone has visited a site at least once

Copyright / DMA (2020)

## Your Cookies Policy

Once you have a clear idea of what cookies have been dropped and which categories they fall into, you must update your cookies policy to provide an open and transparent explanation of how they will be used. This policy should remain under review to reflect new cookies added to the master list.

A simple consent mechanism for non-essential cookies may capture all consent in one place. A more sophisticated system can be used if there are complex cookie requirements coupled with a desire for line-by-line consent. This may apply to media owners who must manage ad-tech supplier consent e.g Adchoices.

Copyright / DMA (2020)

# Advertising Cookies

Advertising cookies are not always third-party cookies. The host website will set its own cookies to help segment its audience base, so it can serve ads to distinct groups.

There will also be instances when ad-tech companies set cookies on a user's device if they are processing user data in advertising auctions. The host site must ensure the user can understand which cookies have been set and what their personal data will be used for.

The organisations collecting third-party cookies should be obvious, as consent is always required to set them. However, frameworks for capturing consent differ between businesses.

The most widely used is the IAB Transparency and Consent Framework, used to underpin a number of widely used Consent Management Platforms, such as OneTrust.

Each host site should have a contractual relationship with third parties. Guarantees should be sought that the partner organisation isn't wholly reliant on the contract for overall revenues and profitability, as this increases the risk of decision making that may not amount to good governance.

There are limited checks and balances in place to control the processing of personal data by third parties. However, the introduction of accreditation/certification schemes such as ISO 27001/27701 will provide some assurance.

## IAB Framework

Launched in April 2018, the framework is designed to help publishers tell users what data is being collected, and how they and their vendors plan to use it.

An updated version of the framework, TCF 2.0, was launched in August 2019. This was released because of further consultation with the ICO and publishers.

## Segmentation and Ad Tech

Ad tech infrastructure is complex. Essentially, it provides a means for ads to be served programmatically to users in real-time. As part of the processing of user data, ad-tech companies use machine learning to develop customer segments based on common browsing behaviour. The ICO has signalled consent is required to conduct this type of processing.

Copyright / DMA (2020)

# Social Media Cookies

Anyone using multiple social media platforms may be tracked as they move from website to website.

Cookies could be placed on a user's devices when they visit pages via platforms or websites using platform tracking - such as Facebook Audiences, Twitter, Spotify, Instagram etc - or Google Ads.

A recent judgement from the European Court of Justice made it clear that if an advertiser is present and gathers data on a social media platform, the advertiser and the platform are joint controllers. This places an obligation on advertisers that use social media to ensure users understand that their data will be shared with the social media platform, and partners and users of that platform. This information must be shared with individuals and consent obtained before any cookies are placed.

Copyright / DMA (2020)

# Device Fingerprinting

The mechanisms that place cookies on a user's device are known by many names: beacons, widgets, tags, images, or pixels, to cite just a few.

There are other ways to track users online. Although they don't use cookies, they still fall under the guise of 'other tracking methods.'

One of these methods is device fingerprinting. It uses several data points from a device, such as the information that is shared when it connects to a website or other electronic communications service, to differentiate it from other devices.

Device fingerprinting can be intrusive, especially if it seeks to uncover multiple parameters from the person's browser - but it may be necessary.

As device fingerprinting may not be covered by PECR, because it doesn't use cookies to identify a person, it falls under the GDPR and may be considered invisible processing.

It could therefore be unexpected to the user, especially if they have disabled cookies to prevent tracking. It is highly likely that the use of this type of tracking will require consent.

Copyright / DMA (2020)

# Cookie Tracking in Email

Cookies that track users' behaviour after they click a link in an email are very popular. They can be placed when a link is clicked, or by using web beacons or images.

Many email service providers place cookies when a user interacts with the content of a message. They are dropped onto a user's browser if they open an email in webmail or placed when a user clicks on a link in an email to view a website. Cookies can also identify what action a user takes once they click through to a website.

Open tracking pixels are based on similar technology to cookies. They allow data to be read from the recipient's device, telling the email sender whether the message was opened and what sort of device was used.

## Consent

Electronic marketing messages, such as email and SMS, can only be sent if the user has given consent to receive it. If at the point of recruiting a customer to email communications the marketer gives clear, concise and relevant information about the kind of tracking that will ensue, and how it will be used in email marketing, it's likely the recipient will be well informed, and have some expectation of measurement and tracking of their actions.

## Tracking Consent for New Subscribers

Email opt-in is one of the best times to gain permission for tracking. Users are already familiar with being asked for permission to be sent electronic marketing communications:

*" Please tick this box to register for our newsletter, allowing us to send you relevant offers and information. We use cookies to help ensure we only send you what you want, click here to find out more.*

*Please tick here if you wish us to use your browsing habits on our website and emails to help us better tailor the content you see."*

When the potential subscriber clicks on "find out more" they must be taken to your privacy notice, which sets out what tracking is used, how it will be used and how it impacts the recipient.

Copyright / DMA (2020)

## Consent via Soft Opt-In

Many websites use this to gain email marketing permission. Although this is an effective way to acquire marketable email addresses, positive action is required if gaining consent for tracking. For example:

*"We would like to send you emails from time to time with offers and other relevant information. Please deselect this box if you do not want these emails.*

*We use cookies to help ensure we only send you what you want and to improve your online experience, click here for further details.*

*Please tick this box if you wish us to use your browsing habits on our website and emails to help us better tailor the content you see."*

## Consent via Email

Although you can still email contacts on existing lists, there is an obligation to educate these recipients about what tracking is used. This information need not be confined to tracking used in emails; it can also include tracking used throughout your website.

Clear information should be provided about tracking. One method is to use a statement such as the one below, at the head of an email or in the pre-header. You would include this when contacting people who have chosen not to accept cookies for the time being.

*"We can use cookies to help us send you relevant offers and to improve your online experience, click to find out more."*

Using this method allows you to continue communicating with your customer while simultaneously offering them a more personalised experience. It's also non-intrusive to the recipient. It requires no action on their part to continue reading the email content. Once the link is clicked, the user is presented with a web page with information on cookies and the chance to opt in.

## Real-Time Bidding (RTB)

In RTB, the log file information or profile collected via tracking cookies is shared widely throughout the ad-buying eco-system with multiple organisations (sometimes as many as hundreds). They can decide whether to invest in presenting their ad to an individual who has a profile of browsing habits closely matching the organisation's ideal customer.

Copyright / DMA (2020)

The company that wins the bid, and the right to display the relevant ad, often keeps the profile data and uses it to enhance any log file information already held about these customers.

The diagram below is taken from a presentation by Dr Johnny Ryan of Brave, illustrating the movement of personal data and its transfer to many companies in the ad-tech supplier chain.

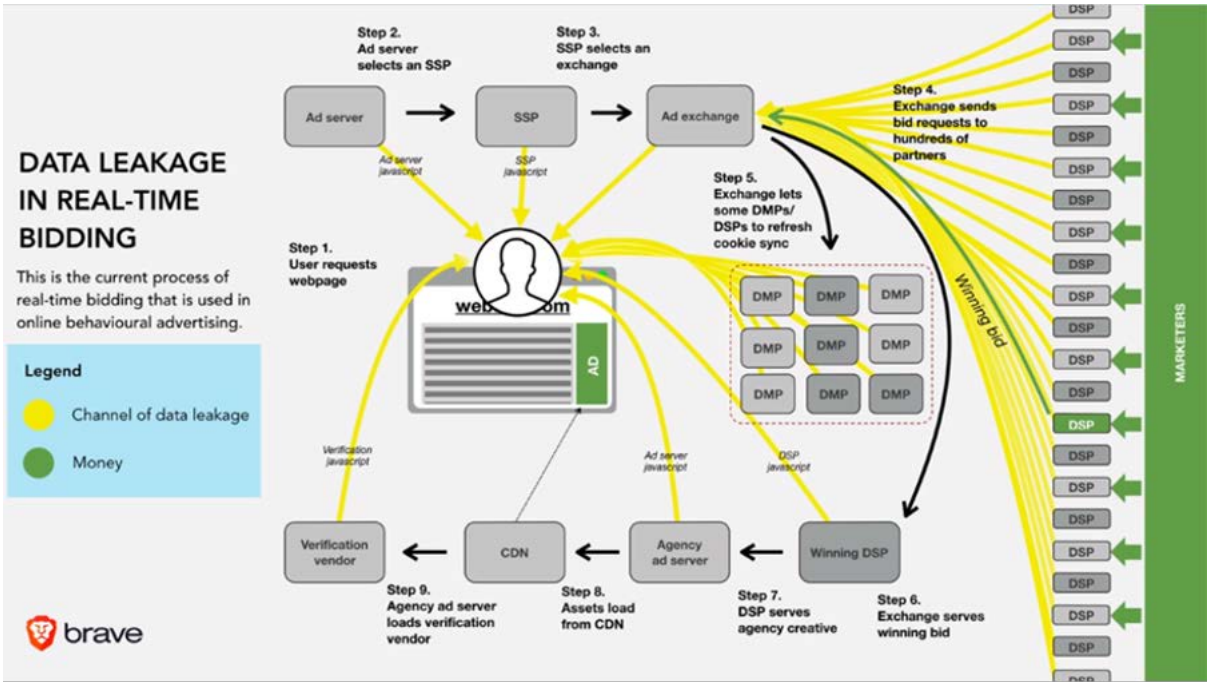
## Data Leakage

The number of technology partners in the RTB chain can be vast, and this presents a challenge. It is very difficult, if not impossible, to anticipate the final recipient of data collected via cookies used by or placed by your website.

This makes it unlikely that you will be able to adequately inform and consequently obtain valid consent for the RTB cookies you have on your website. It also means that if you are merely advertising using RTB, you are very unlikely to be able to identify the legal basis for processing the data you use.

The diagram below illustrates the complexity of the RTB infrastructure and demonstrates the lack of control and security for personal data within the RTB environment.

This is one of the reasons that a detailed cookie audit must be carried out on any third parties that are collecting data via cookies on your website.



## Ad Tech

Based on guidance from the ICO, ad-tech vendors are joint controllers and have responsibility to properly respond to consent signals. For this reason, many choose to follow a common protocol like IAB Transparency & Consent Framework. This gives additional assurances in the ad tech / publisher partnership.

The use of consent in ad tech remains complex. Once a website allows third-party access, there isn't much accountability from the domain owner's perspective.

## Data Minimisation when Collecting Consent

This refers to the data that organisations collect to log consent. Data minimisation best practice uses anonymous identifiers, stored by the client to maintain user consent settings on a website over time. Whenever consent is updated, a new transaction is created against that ID. If a user clears their cookies, they will be given a new, anonymous ID.

## Disable Default Execution

This can be achieved through both tag management configuration settings and methods within the HTML source of a web page. These controls can be leveraged to disable default scripts and only activate them once consent has been captured.

within the market, such as the introduction of pro-privacy browsers, has altered some of the basics around how existing blocking technologies operate. Certain browsers are - by default - configured to block specific types of cookies. While this is a popular approach, friction remains; the approach eliminates websites' ability to differentiate content, and how they use and respect consumer data.

Copyright / DMA (2020)

# Alternatives to Cookies

## Contextual Marketing

This is a major industry concern. Websites will frequently leverage behaviours such as the user journey to attempt inferences about them e.g. “Is this person a serious buyer?” The information can be valuable for organisations because it provides a more holistic picture of how people interact with sites.

## Audiences

Creating audiences has always been an issue for marketers trying to consolidate their understanding of user behaviour across various devices. Restrictions on the possible legal basis of processing for web-tracking purposes has exacerbated the problem.

However, this also creates a new opportunity for companies to re-engage with consumers, by showing them the ways they use customer information and encouraging them to proactively manage it.

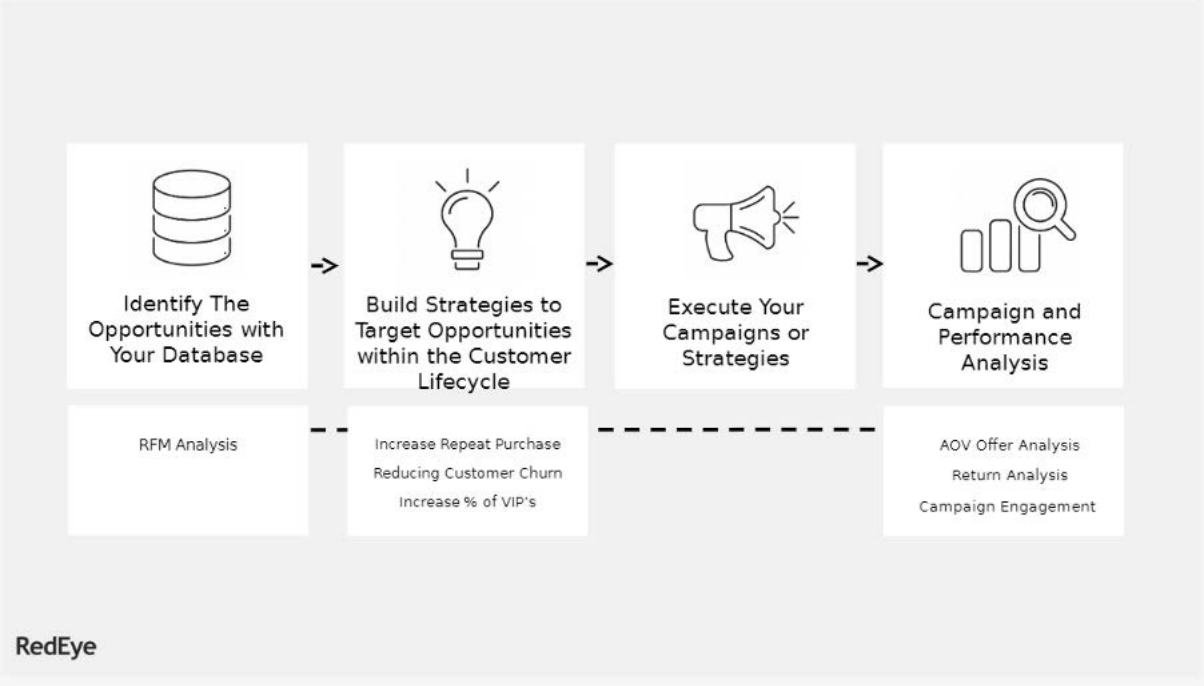
Copyright / DMA (2020)

# Targeting Using Customer Insight

## Segmentation Methods

Several cookie-free methods can help organisations target customers with relevant and effective marketing. Many are based on using the predictive nature of transactional tracking to identify products likely to be purchased, and when a user is likely to buy them.

These types of segmentation rely on the use of customer knowledge, typically obtained through analysis of customer behaviour and insight gained by examining purchase history.




Copyright / DMA (2020)

Methods include:

**RFM (Recency Frequency, Monetary value)**

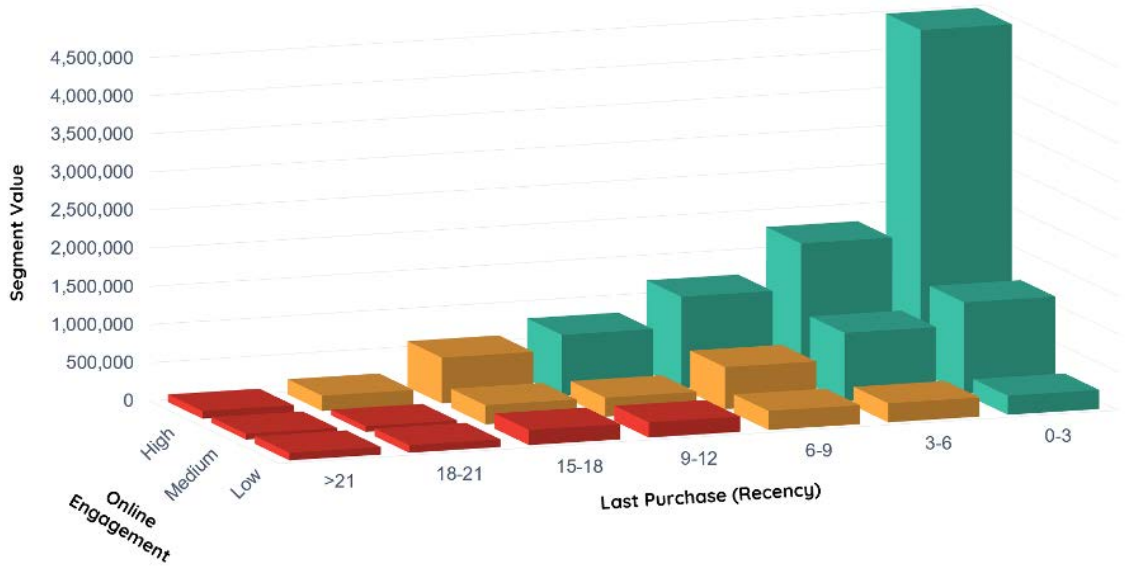
Based on the premise that the more recently someone has been purchased a product, the more frequently they have purchased and the more money they have spent, the more likely they are to purchase again. RFM analysis and segmentation can be used effectively in online marketing, in the same way it's successful offline. RFM is closely related to FRAC.

**FRAC (Frequency, Recency, Amount and Category)**

FRAC uses frequency as the first driver, with the other elements cross-matched against it. You would need to analyse your transactional data to determine which of these methods is the most predictive of future sales of specific items.

**e-RFM (engagement RFM)**

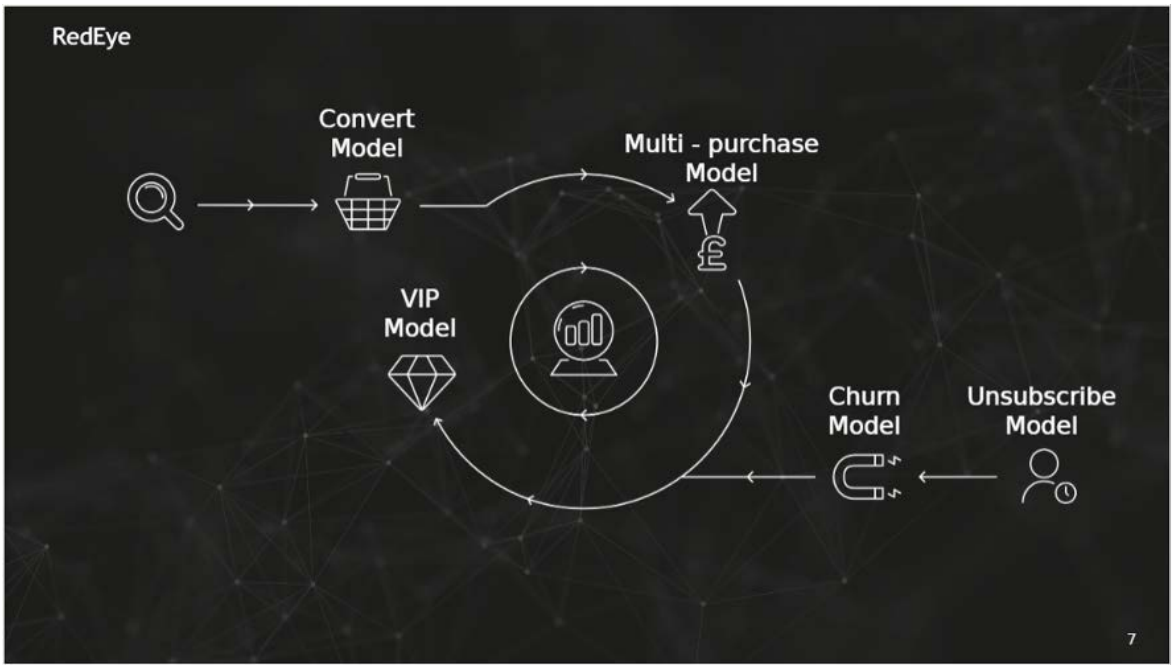
This is a combination of the transactional segmentation (RFM) with recency of online engagement. It determines online engagement by using the recency of an email open or click, or a website log-in or social media comment or other action. You can also apply this type of segmentation to specific products or services




Copyright / DMA (2020)

# Customer lifecycle marketing

Customer lifecycle marketing can be used to target the message to customers based on which stage they have reached. Modelling can be undertaken using transactional data and does not require the use of data obtained via cookies.



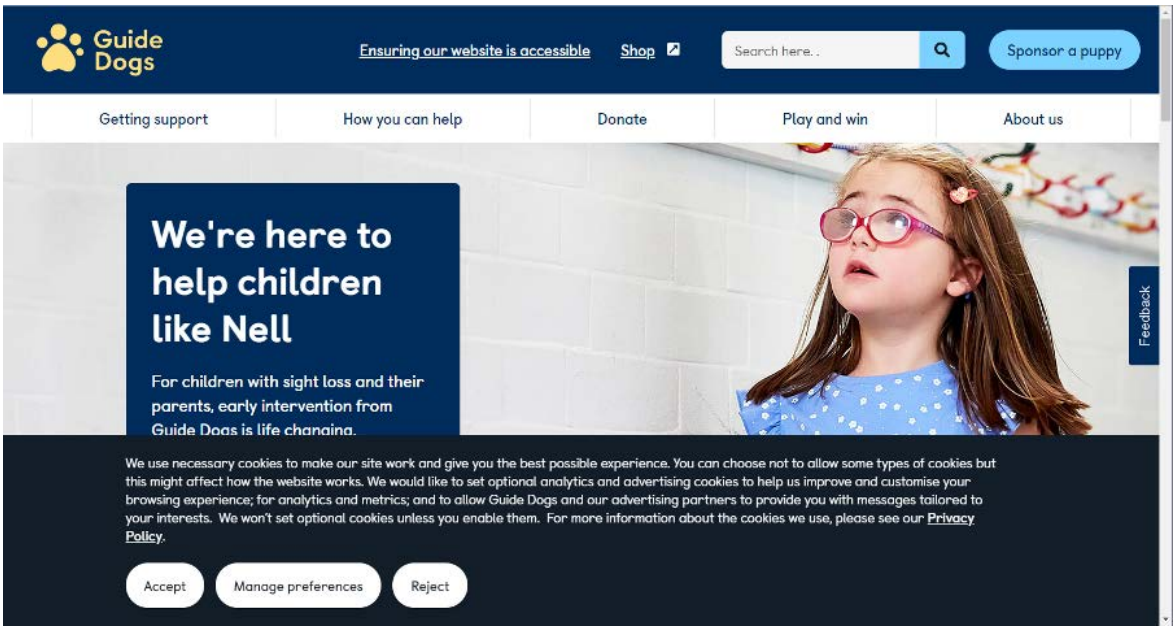

Copyright / DMA (2020)

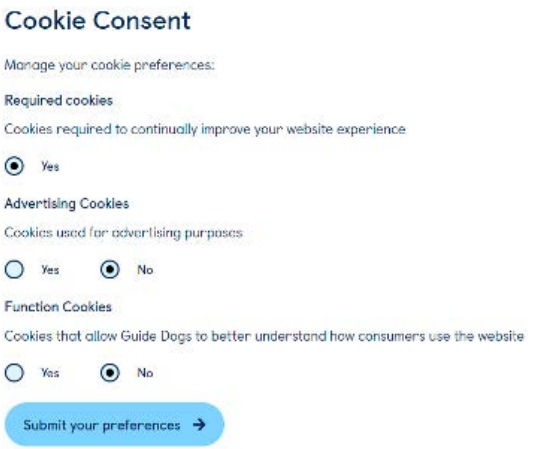
# / Case Studies

It is important to note cookie banner compliance varies from country to country. Featured below are some examples of compliance and non-compliance from Uk websites.

**Compliant example:**

The cookie banner lends equal weight to 'accept' and 'reject' buttons. The preference centre uses an opt-in model; all cookie categories are set to off by default.

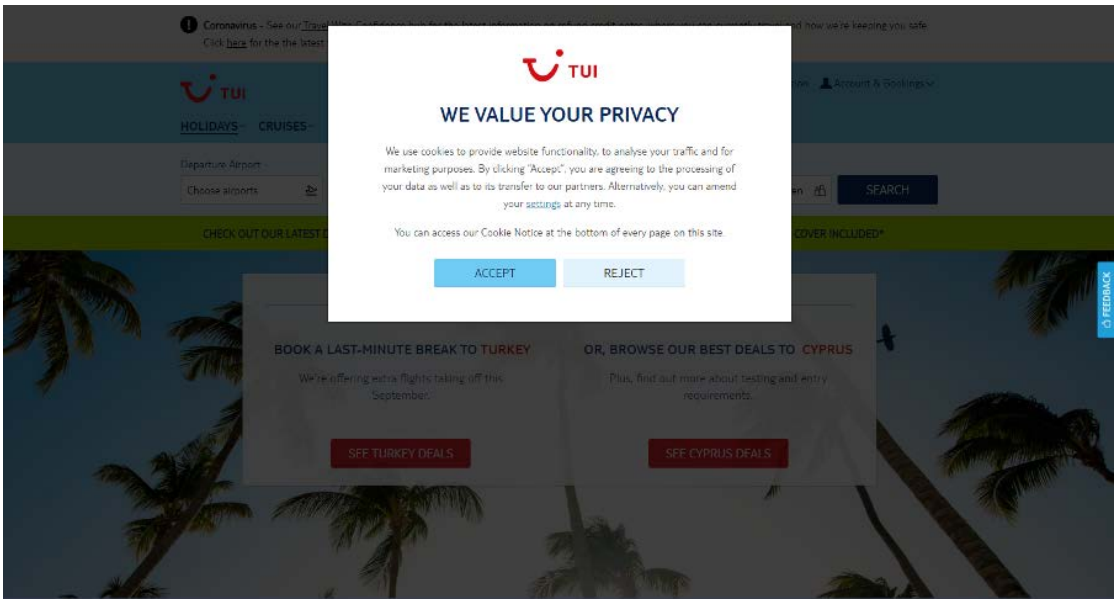



Copyright / DMA (2020)

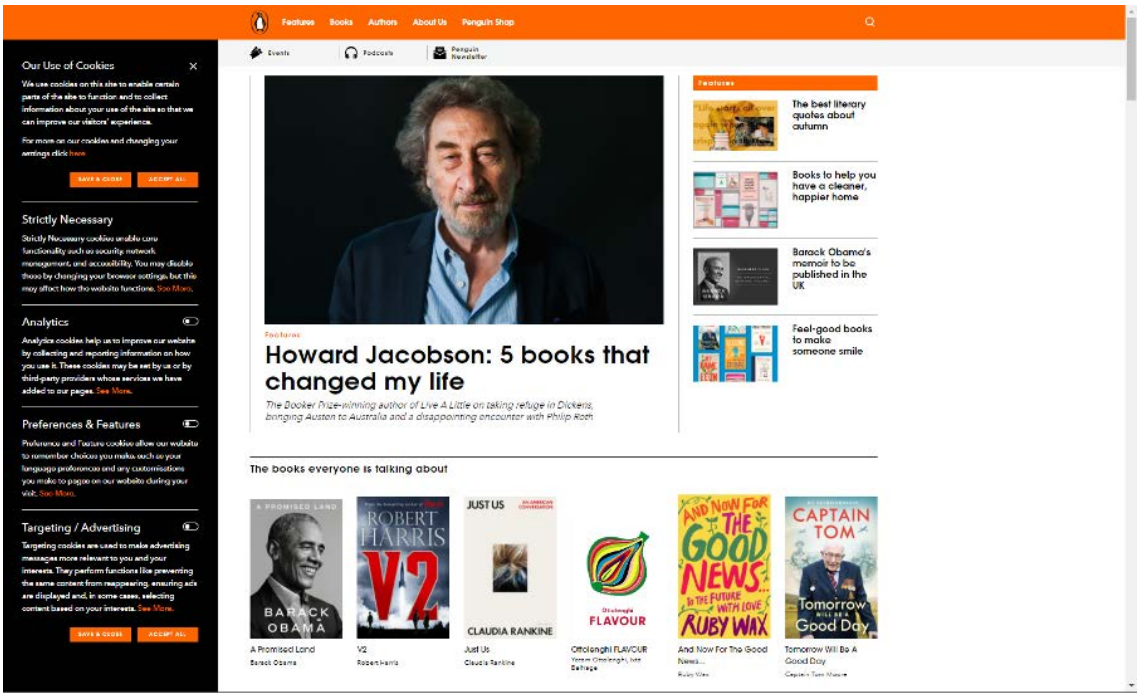
**Compliant example:**

The cookie banner lends equal weight to 'accept' and 'reject' buttons.



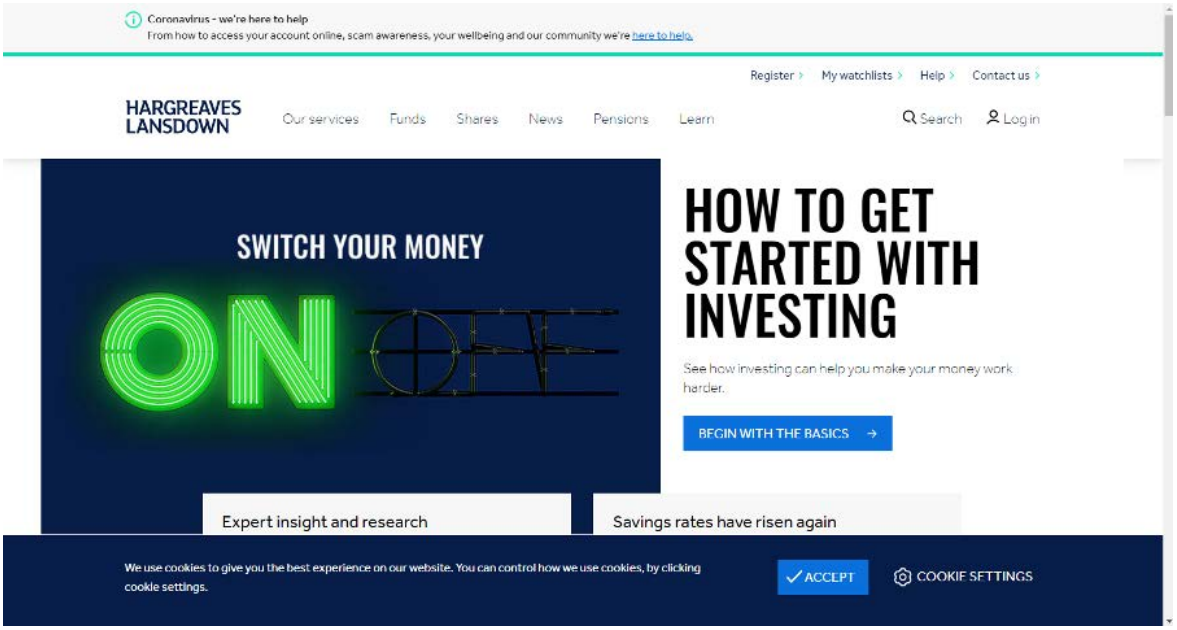

**Compliant example:**

The cookie banner is combined with the preference centre making choices clear and easy to adjust.

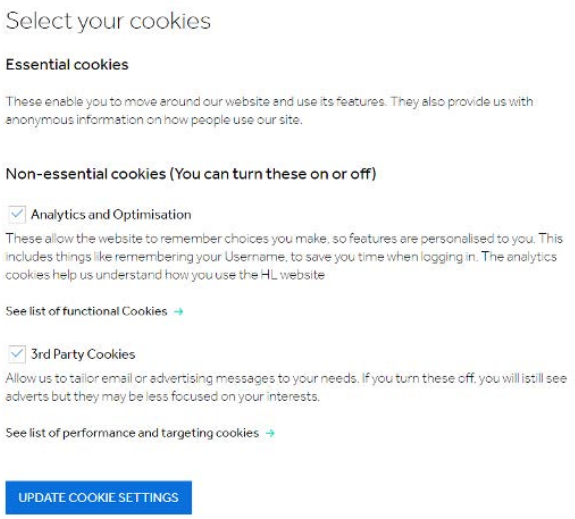


**Non-compliant example:**

A cookie banner that doesn't provide the visitor with a mechanism to reject cookies without taking the additional step of visiting the Cookie Settings page.



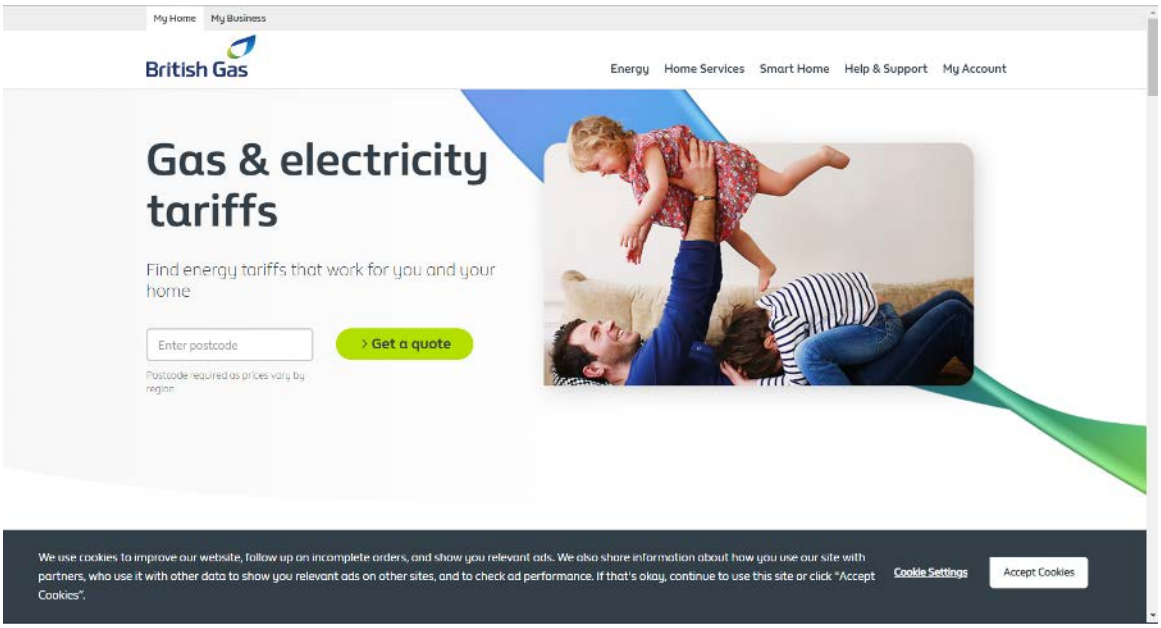

The cookie setting page has pre-ticked consent boxes requiring a visitor to opt out of all cookie categories instead of opting into cookie categories.

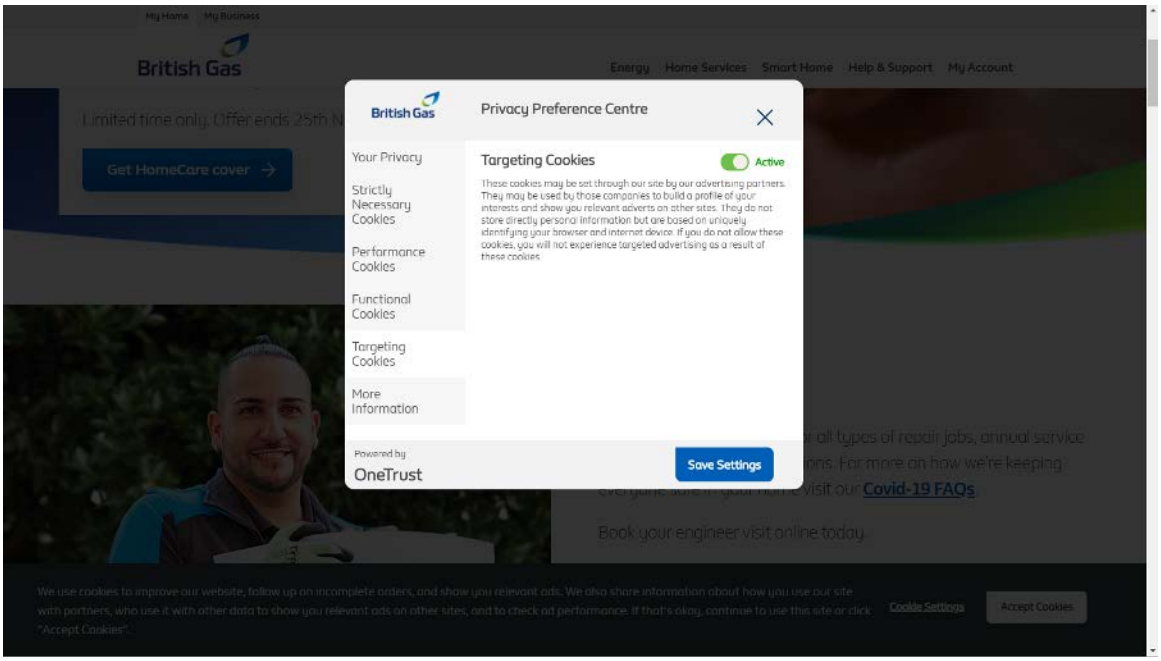



Copyright / DMA (2020)

**Non-compliant example:**

This example is similar in that the visitor must go to a second page where all the cookies default to the 'Allow' setting.




An organisation using this approach has opted to use cookies for personalising ads, failing to give visitors the choice to reject those cookies. Personal data is likely processed regardless of the user's wishes.

Copyright / DMA (2020)

# Innovation and Creativity

Standard options for cookie consent are becoming the norm.

However, organisations can still innovate their approach:

## Cookie Consent Copy Differentiation

Standard cookie consent copy can be dry, impersonal, and largely ignored by users. Organisations are starting to create more interesting, amusing or personalised copy, particularly in consent buttons, to increase user engagement.

## Cookie Banner and Preference Centre Customisation

Cookie banners can be created and customised to match your organisation's branding and tone of voice, making them more engaging, in line with your overall risk appetite. This includes geo-targeting, leveraging multiple languages and changing the banner's placement on the website.

For example, setting up a cookie banner using OneTrust PreferenceChoice enables your organisation to:

- Scan your websites for cookies
- Auto-categorise your cookies based on a database of more than 5 million pre-categorised cookies
- Rescan websites at a specific interval
- Adjust banner / button copy and on-site placement

Google Tag Manager is a common approach to adding cookie consent to websites. It allows organisations to set up consent, so scripts are controlled by preferences chosen by visitors. This can be easier than using standard methods for implementing cookie banners and preference centres. It's important to keep in mind that GTM and other tag management systems have unique structures, so differences in behaviour exist.

Cookie script tags can also be used to integrate the cookie banner within your organisation's websites if they do not use a tag manager. Using the cookie script tag, you can adjust the domains and language you want to publish.

Copyright / DMA (2020)

## Just-in-time Consent

Why ask for consent all at once? Consent can be spread across devices, platforms and experiences via a website or app to gain consent at the most convenient and/or valuable time for the user.

## Creating Proactive Preference Centres

Capturing real-time consent can help a user understand what aspects of data management and use may be affected by their consent for certain elements of web browsing. It's a way to proactively gain consent through just-in-time preference centres.

For example, if a user is on a news site and reading an article, and sees related articles they may want to read, it could be a good time to present a preference centre explaining how certain types of cookies help keep track of what the user likes to read; ensuring they always see content that is interesting and relevant.

Copyright / DMA (2020)

# 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.

Copyright / DMA (2020)

# 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 be 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.

Published by The Direct Marketing Association (UK) Ltd Copyright © Direct Marketing Association.

All rights reserved.

www.dma.org.uk

# Copyright and Disclaimer

'DMA Guide: Cookies and Compliance' is published by the Data & Marketing Association (UK) Ltd Copyright © Data & Marketing Association (DMA). All rights reserved. No part of this publication may be reproduced, copied or transmitted in any form or by any means, or stored in a retrieval system of any nature, without the prior permission of the DMA (UK) Ltd, except as permitted by the provisions of the Copyright, Designs and Patents Act 1988 and related legislation.

Application for permission to reproduce all or part of the Copyright material shall be made to the DMA (UK) Ltd, DMA House, 70 Margaret Street, London, W1W 8SS.

Although the greatest care has been taken in the preparation and compilation of this report, no liability or responsibility of any kind (to extent permitted by law), including responsibility for negligence is accepted by the DMA, its servants or agents. All information gathered is believed correct at November 2020. All corrections should be sent to the DMA for future editions.