

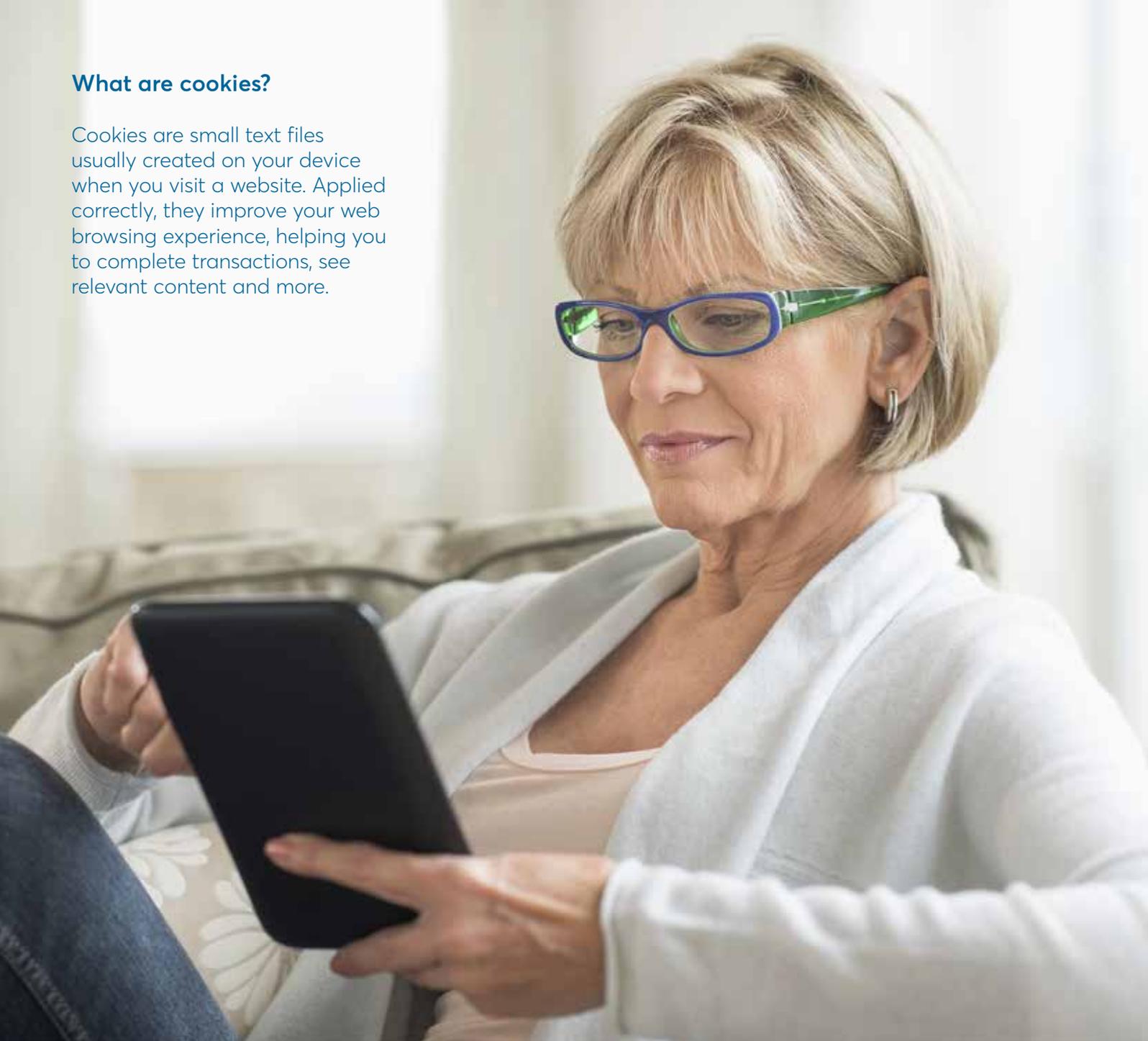
Prior placement of cookies

Do cookie management tools work?



What are cookies?

Cookies are small text files usually created on your device when you visit a website. Applied correctly, they improve your web browsing experience, helping you to complete transactions, see relevant content and more.



'Setting cookies before users have had the opportunity to look at the information provided about cookies, and make a choice about those cookies, is likely to lead to compliance problems.'

What were we looking at?

We had a theory that the majority of websites were allowing the 'prior placement' of non-essential cookies. This report shows our findings, but first...

What is 'prior placement' of cookies?

Prior placement is the term used to describe when a website places cookies onto your device before asking for your permission to do so.

Is prior placement of cookies allowed?

As shown by the adjacent quote, prior placement of cookies has been questionable ground in the United Kingdom under PECR since 2012. The exception is for what are known as 'essential' cookies (more on these overleaf).

GDPR and cookies



There has been renewed scrutiny of cookie compliance within the European Economic Area (EEA) following the introduction of GDPR.

This is because, under GDPR, the geographic location of the site user is now the determining factor of whether or not consent is required (rather than the location of the site owner).

What does GDPR say about cookies?

'Natural persons may be associated with online identifiers [...] such as internet protocol addresses, cookie identifiers or other identifiers [...]. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

-- Recital 30

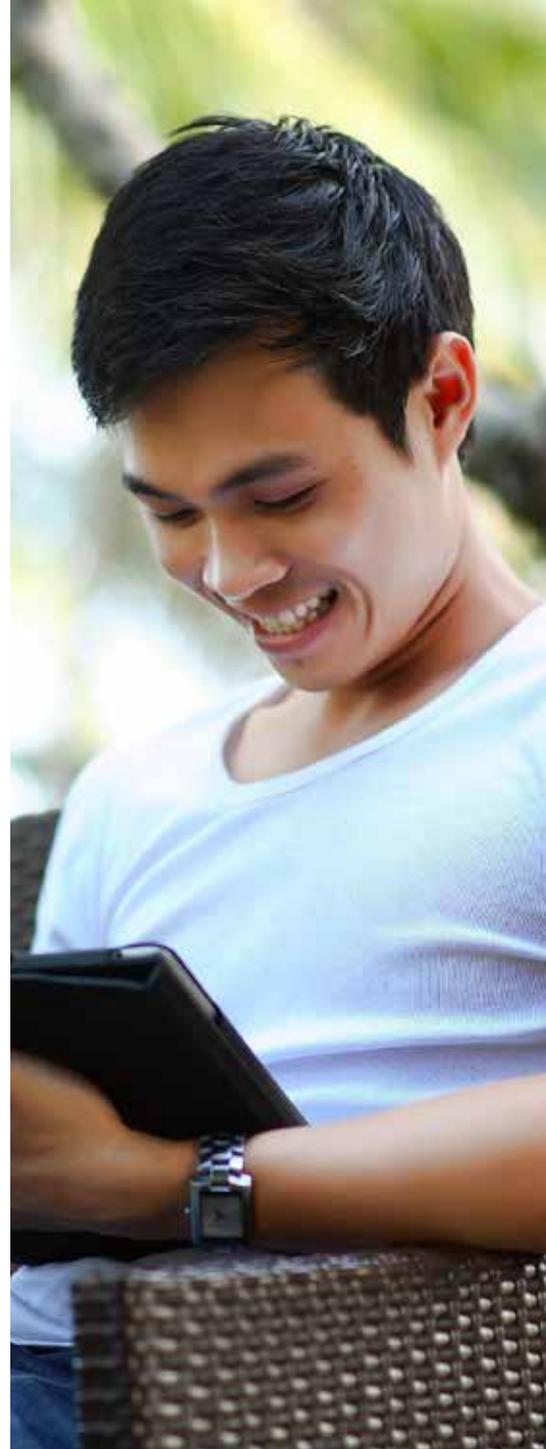
Since IP addresses can be connected to individuals, explicit consent should be given when placing cookies under GDPR.

That's okay, you say, I have a cookie pop-up on my site that allows people to decline or give their consent.

We'll talk about that shortly...

Cookie classifications

There are categories of cookie classification to make it easier for web users to understand the exact purposes of the cookies being placed on their devices.



Strictly necessary (sometimes known as **essential**) cookies, which may be used for security purposes or remembering critical previous actions (whilst online shopping, for instance). These are the only cookies which do not require explicit consent.

Performance cookies used for website improvement, such as analytics, error management or to conduct performance testing on a site.

Functionality cookies may be used to remember users' previous settings and preferences, or to allow website features such as posting comments.

Targeting or advertising cookies collect browsing habits in order to serve more relevant advertisements to the user.

Some notes on the report

Our method

We tested 100 of the most popular websites* to see how many placed cookies automatically onto our devices.

Here's what we did:

- Clear all browsing data
- Visit the site URL directly and allow the page to load
- Note the number of cookies placed automatically
- Opt out as fully as the site allows
- Note any change in the number of cookies
- Repeat with each new site

If there was an increase in the number of cookies after the opt out, we repeated the process in more detail. We took note of the publisher, the name and the purpose of each cookie and whether it was placed before or after opt-out.

How scientific is this?

We wanted to draw attention to the fact that this is fairly unscientific as studies go (and we know it), but we were keen not to over-orchestrate the experiment. We wanted to report on a real world experience.

With that in mind, it's also important that we highlight that the results achieved by following our method would vary based on your location, browser settings and other factors.

If you have already conducted a similar analysis, we'd love to hear from you about your findings. Our contact details can be found at the end of the report.

Anonymisation

We aren't publishing what we found to slam brands for their handling of cookie consent, but to raise awareness of a more concerning trend that we uncovered around cookie placement.

Our goals are:

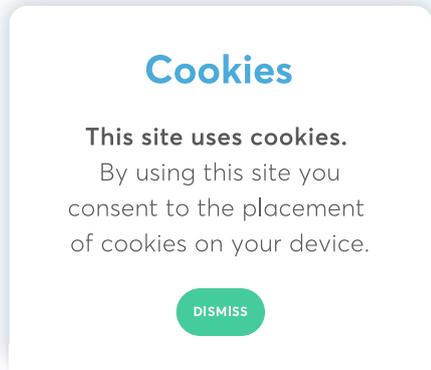
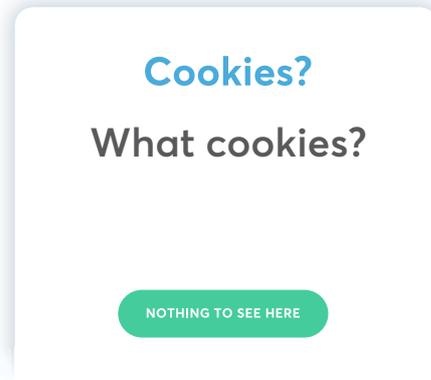
- to help brands achieve genuine compliance with GDPR and PECR for their management of cookie permissions
- to help defend the privacy rights of individuals using the internet within the EEA

To ensure that this message is not lost, we have taken the decision to refrain from naming any brands.

What we found

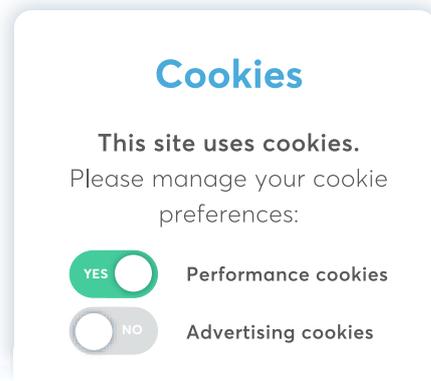
41% of sites made no reference to cookies

These sites placed cookies without making users aware that they were doing so. If your site has non-essential cookies, this approach is not compliant with GDPR legislation.



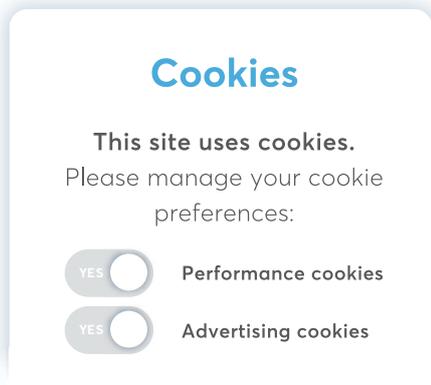
43% of sites displayed a cookie notification

They informed users that cookies were being placed but did not give them a choice to decline. This is known as a force opt-in.



16% of sites offered granular opt-out

On these sites, users appeared to be given the option to decline or accept cookies as they saw fit. This approach complies with both PECR and GDPR best practice.



The granular opt-outs aren't working properly

68% of the sites who seemed to give us a legitimate option to decline cookies placed additional cookies even after we had said no.



'80% of the cookies placed after opt-out were classified as targeting or advertising cookies.'

A worrying discovery...

We thought it strange that the sites which were actively trying to comply by offering cookie opt-outs were still placing cookies more than two thirds of the time (68%) after we declined.

So why is it happening?

Since 32% of the time, these tools worked perfectly, our best guess for the reason that these sites are still placing non-essential cookies after we declined is because implementing them correctly is too complex.

Many rely on tag management software which requires specialist knowledge to set up accurately.

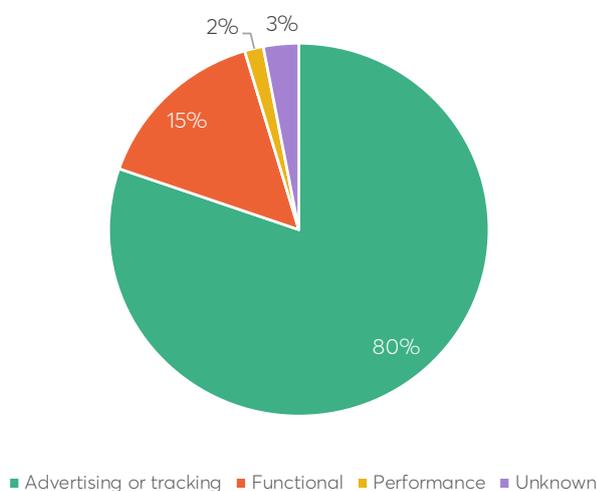
The scale of the problem

On average, 26 extra cookies were placed after we declined.

One site placed a staggering 138 additional cookies after we declined everything but "essential" cookies.

The post-decline cookies came from over 200 different publishers.

Who was still tracking us?



In our tests, 80% of the cookies placed after opt-out were classified as targeting or advertising cookies.

Some (though not all) contained text such as 'dnt' which we can fairly assume as an instruction of 'do not track'. This means, however, that users are being tracked in order to avoid being tracked, and are subsequently trusting the ad networks to remove personal information from any data sets prior to usage such as analysis or sale.

Also worrying is the 3% of cookies which we could not identify. Existing cookie reference sites had no information about them, and the domains issuing them to users could not provide a category, description or purpose for these cookies.

Bitesize conclusions

- There are differing approaches to cookie compliance.
- The majority of sites (59%) communicate that they publish cookies.
- 16% of sites attempted to offer granular cookie opt-out to their users.
- Since 41% of the sites we visited made no reference to cookies at all, however, there is still a greater need for transparency and clarity.
- In our tests, the tools in place to allow users to opt out of tracking did not prevent the placement of declined cookies more than two thirds of the time, probably due to the difficulty of achieving correct implementation.

What next?

Cookies are the responsibility of the site which places them and the terms and conditions from cookie publishers often place the onus directly onto the issuing site to obtain and record permission from users.

Since cookies were still so frequently being placed after opt-out, there's a clear need for site owners to take back control of cookie management with a tool that can be set up quickly and simply, with no scripting or specialist knowledge of tag management required.

If you're looking for a reliable solution for cookie management, we've developed one which:

- does not require specialist tag management knowledge to set up,
- prevents the prior placement of cookies,
- truly allows users to decline further tracking, and
- keeps a record of the consent given.

Find out more at www.syrenis.com or join in the conversation on Twitter using [#CookieCompliance](https://twitter.com/CookieCompliance).

Got questions about this report? Email us: info@syrenis.com





Vanguard House
Sci-Tech Daresbury
Daresbury
Cheshire
WA4 4AB

+44 (0) 1928 622 302

info@syrenis.com



[syrenis_ltd](#)

www.syrenis.com



[/company/syrenis-ltd](#)