

Cookie Compliance in the UK

Tags and Cookies Deployed Before User Consent

Learn about the latest developments from the UK's Information Commissioner's Office (ICO) and the risks of non-compliance.

See the results of our scan of over 160 customer-facing websites for major brands operating in the UK to understand the current state of tag and cookie compliance in the UK.

Receive a FREE tailored report (see the *example report* at the end of the article) to understand how your website compares, with a deep-dive into your tag and cookie compliance performance to help you understand your current-state, and give actionable insight into areas for improvement.

If you have not already provided site details for your FREE personalised report and would like to do so, please reach out to us via email and use the email title "Cookie Compliance in the UK – Free Report":

cookies@loophorizon.com

At Loop Horizon...

... we are passionate about cookie & tag compliance. It's one of the many areas where we support clients; helping them adhere to regulatory requirements and to their own data privacy standards, to mitigate brand and regulatory risks.

Developments in late 2023 and early 2024 from the UK's Information Commissioner's Office (ICO) – [writing to 53 of the UK's top 100 websites to warn of enforcement action if they did not make changes to their cookies to comply with data protection law](#) – make this all-the-more relevant.

Prompted by ICO activity, we established an independent service to monitor tag and cookie compliance in the UK. We scan an ever growing list (currently over 160) of homepages of the largest brands operating in the UK, including the majority of the FTSE 100, across industry sectors, but focused on those with large customer bases.

We've all known for years about potential fines under GDPR of up-to 4% of global revenue. And while on paper this can be huge for some brands, the reality is that fines to date have largely been focused on the big advertising platforms (Meta 2021, €225m; Meta Jan 2023, €390m; Meta May 2023, €1.2b; Amazon 2021, €746m; TikTok 2023, €345m; Google 2021, €90m – [and so on](#)).

Enforcement under PECR is different – [fines up to £500k and potential criminal prosecution](#) – and the [ICO prefers to work with organisations to find a resolution](#).

The recent activity by the ICO – along with their intention to “[not stop with the top 100 websites. We are already preparing to write to the next 100 – and the 100 after that](#)”, “[Our bots are coming for your bots](#)” and “[make the changes now, or face the consequences](#)” – might make the risk feel a bit more real for UK companies.

So while huge fines might not be the immediate outcome, the ICO are driving home the point that companies need to “[recognise and take ownership of the correction of any data protection shortcomings](#)” to avoid enforcement action.

The biggest risk is likely the reputational damage from being named as non-compliant. Most companies we scanned have large customer-facing websites. A public compliance breach is an easy story to write and can rapidly erode customer trust, damage reputation and impact revenue.

We’ve worked with lots of companies over the years, and we believe that few brands are deliberately breaching the rules – they are customer centric and want to do the right thing for their customers. But mistakes can creep in overtime and occasionally things may be deployed too quickly in the chase for trading performance.

Often the biggest challenge for brands is simply knowing if they are over the line, before the ICO makes that assessment for them.

So brands need to ask themselves: how do I make sure I know if I’m compliant?

Summary

Our scan focuses on whether companies are tracking users before they've had the chance to reject. It's a simple count of the number of cookies and third-party vendor tags loaded on each homepage before consent has been granted by the end user; that is to say, before the user has interacted with the cookie consent banner such as the one shown below.

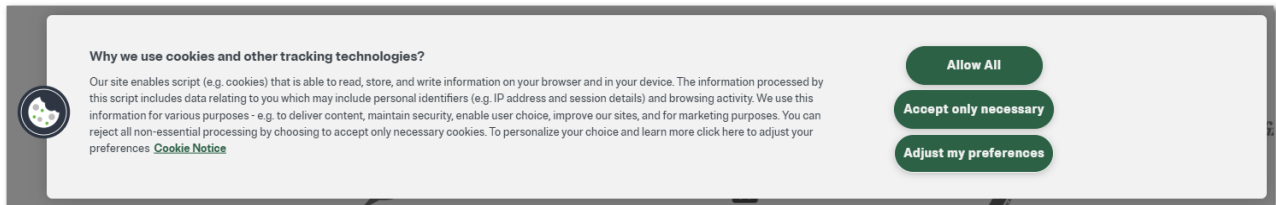


Figure 1: How many cookies and third-party vendor tags are set when the homepage first loads, before the user has interacted with the cookie consent banner?

Top-level findings

We categorised Brands into 4 buckets, based on the count of tags and cookies that fired pre-consent:

	Great	Ok	Uncertain	Problematic
Cookies	33%	40%	14%	13%
Tags	14%	58%	21%	7%
	1-2 cookies and tags	3-8 cookies and tags	9-15 cookies and tags	16+ cookies and tags

Some cookies and tags set pre-consent are likely legitimate; often core site functionality requires this, and this is compliant.

However where we see *large* numbers of cookies and tags before consent, it can be an indicator of compliance issues. The statements from the ICO suggest that this is what they will be looking for, and opens the door to deeper investigation

The minimum value for both tags and cookies is 1 (23% of companies for cookies, but only 8% for tags, fall into this camp). The maximum value for tags set before consent is 21, and for cookies it is 44! This is a single company; the same for both.

When we deep-dive into the outliers from our chart, these numbers start to reveal poor compliance performance. It's impossible to confirm if this is intentional, or simply due to a lack of awareness, and of proper monitoring, process and controls.

However, what is clear is that it represents a breach of trust with the end user and places companies in considerable risk of brand damage and action from the ICO.

What's in the detail

1. [Scan Methodology](#)
2. [Overview charts](#)
3. [Two specific deep-dives on Problematic examples](#)
4. [Industry sector specific charts](#)
5. [Example tailored report \(based on loophorizon.com\)](#)

What did we measure?

We decided to keep it simple:

1. The number of third-party vendor tags loaded on each homepage
2. The number of first-party cookies set
3. Page-load speed
4. Global revenue

Why those measures?

The count of third-party vendor tags and cookies alone doesn't mean that a website is not compliant with GDPR and PECR, but it is a strong lead indicator of compliance, and is a very consistent measure across all sites, thus ironing out any nuances in approach from site-to-site.

It has the added advantage of being extremely simple and easy to understand benchmark, measuring what is set when a user first lands on a website, and before they have been able to grant or deny consent to advertising, analytics, personalisation and more.

PECR ([and the ICO](#)) is very clear on this point – only essential tags and cookies should be set before consent is granted. So the higher the volume, the greater the likelihood that something isn't right.

We also know that the number of scripts set on a site can have a direct impact on page performance (albeit there are many other factors at play). So adding page-load speed as our bubble-size measure brings customer experience and revenue impact in to the results.

Lastly, given the potential impact to brand & reputation, we've including global revenue for the brand, also indicated by bubble-size, as an alternative metric.

The Results

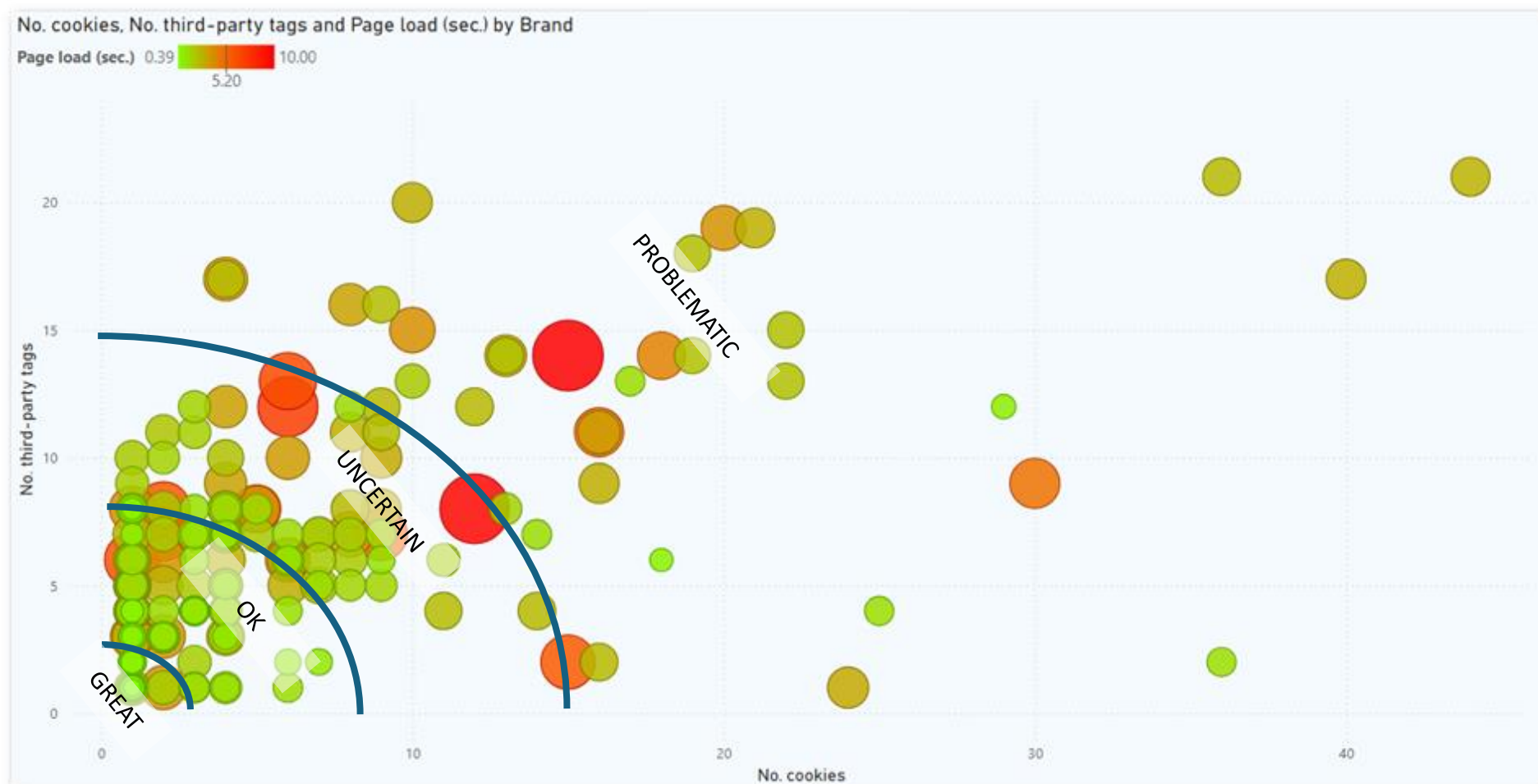


Figure 2: This chart displays all homepages scanned. The majority of brands set a relatively small number of tags and cookies pre-consent, but there are some clear outliers.

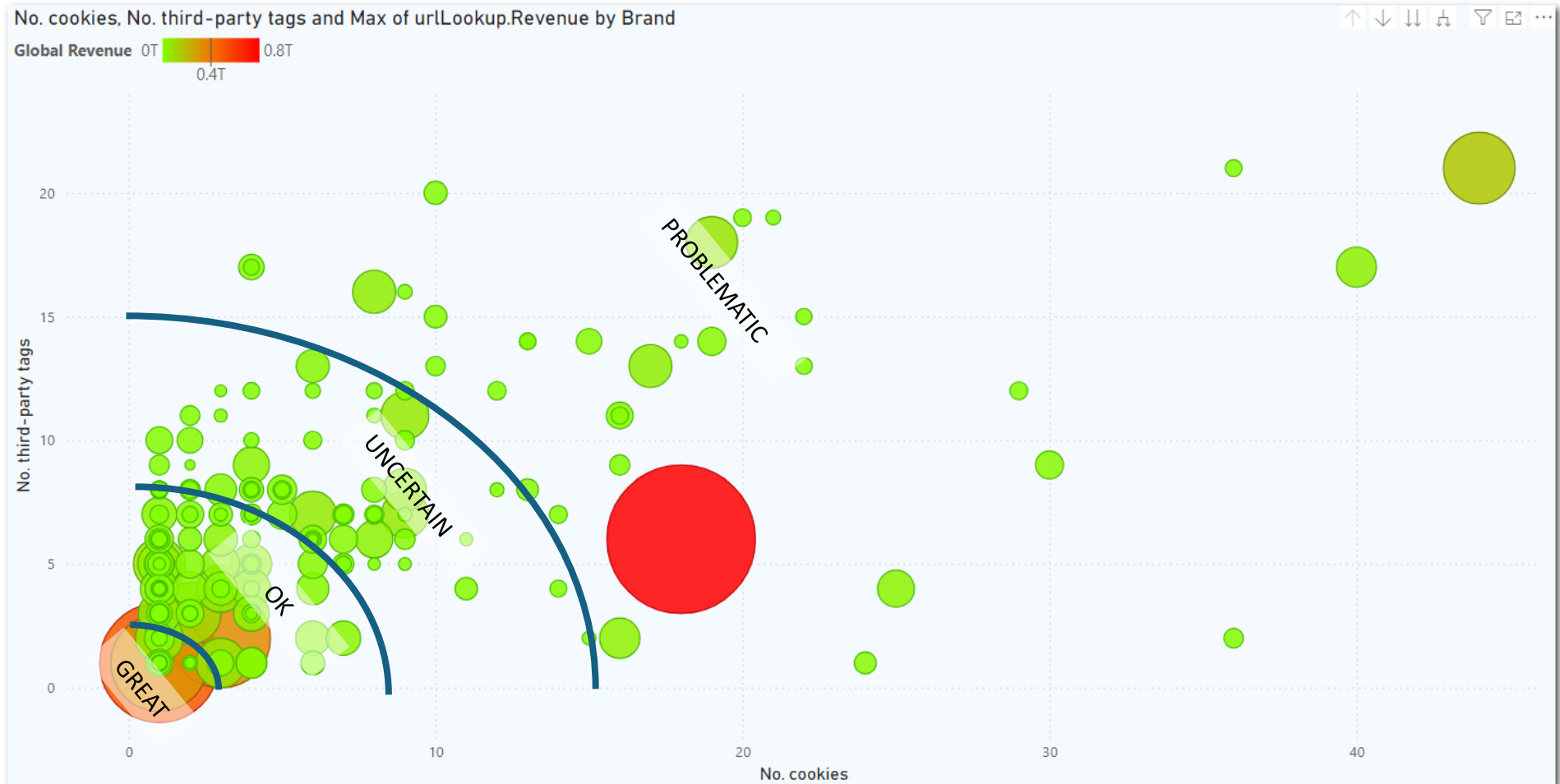


Figure 3: The large red bubble in the lower centre of the graph is a global revenue of over £800 billion. The relatively small bubble at the top right represents almost £160 billion in global revenue – it is only green due to the absolutely huge revenue figures for some of the brands we scanned.

What are you seeing here?

This graph shows all c160 homepages scanned. You can see that there's a wide spread of cookies (X axis) and tags (Y axis) set before users have granted consent. This demonstrates that – although there's a range of levels of adherence to GDPR and PECR (with some clear outliers) – at a high-level view, a large number of brands scanned are setting a wide range of tags and cookies before a user has granted consent.

The following four pages show the same dashboard, broken down by industry sector for:

1. Retail
2. Media
3. Banking
4. Consulting

This is then followed by deep-dives into two specific outliers from the graph using a tool called [ObservePoint Debugger](#) (a Google Chrome extension), which can be used manually when loading a website to give an in-depth view as to exactly what tags are being set pre-consent. ObservePoint Debugger also categorises these tags, which helps give a feel for how many of these tags are likely to be essential.

Retail

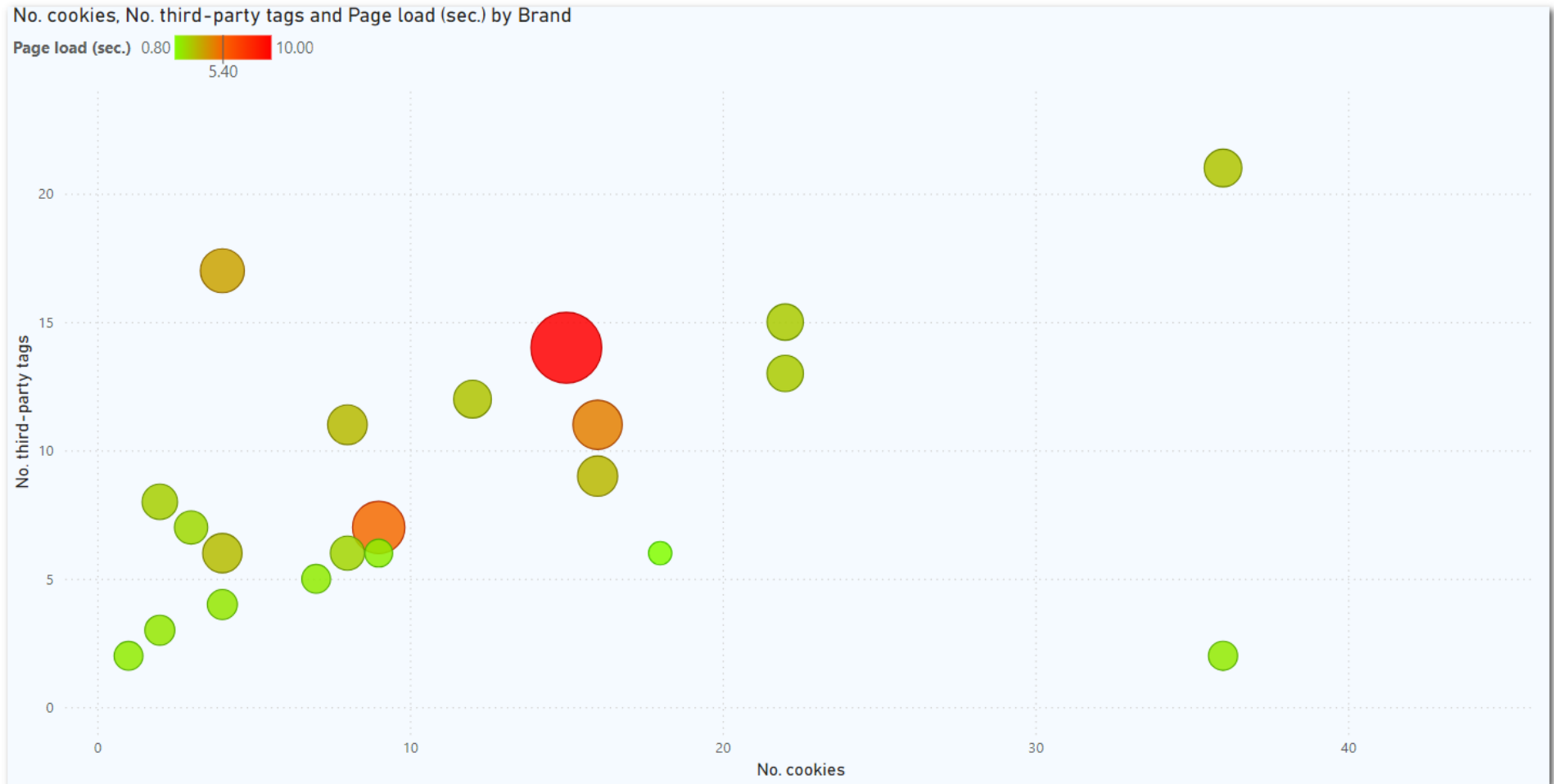
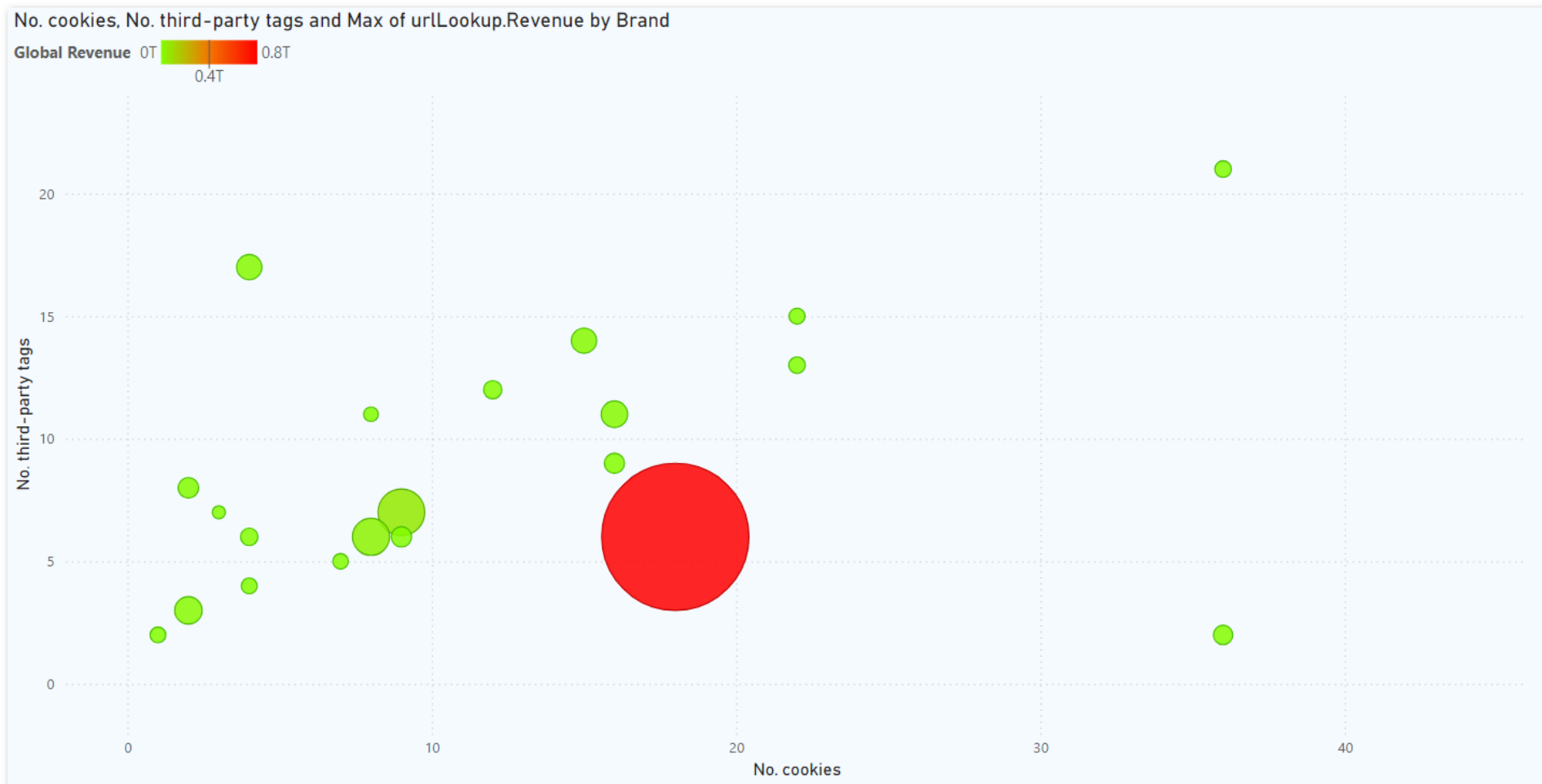


Figure 4: The retail sector has brands all-across the range, and also shows some interesting variance in load speed.



The B2C retail sector has a high incentive to keep tagging in place – marketing / advertising tags enable efficient and targeted marketing activity, while analytics and personalisation tags help optimise the on-site experience, driving revenue.

Media

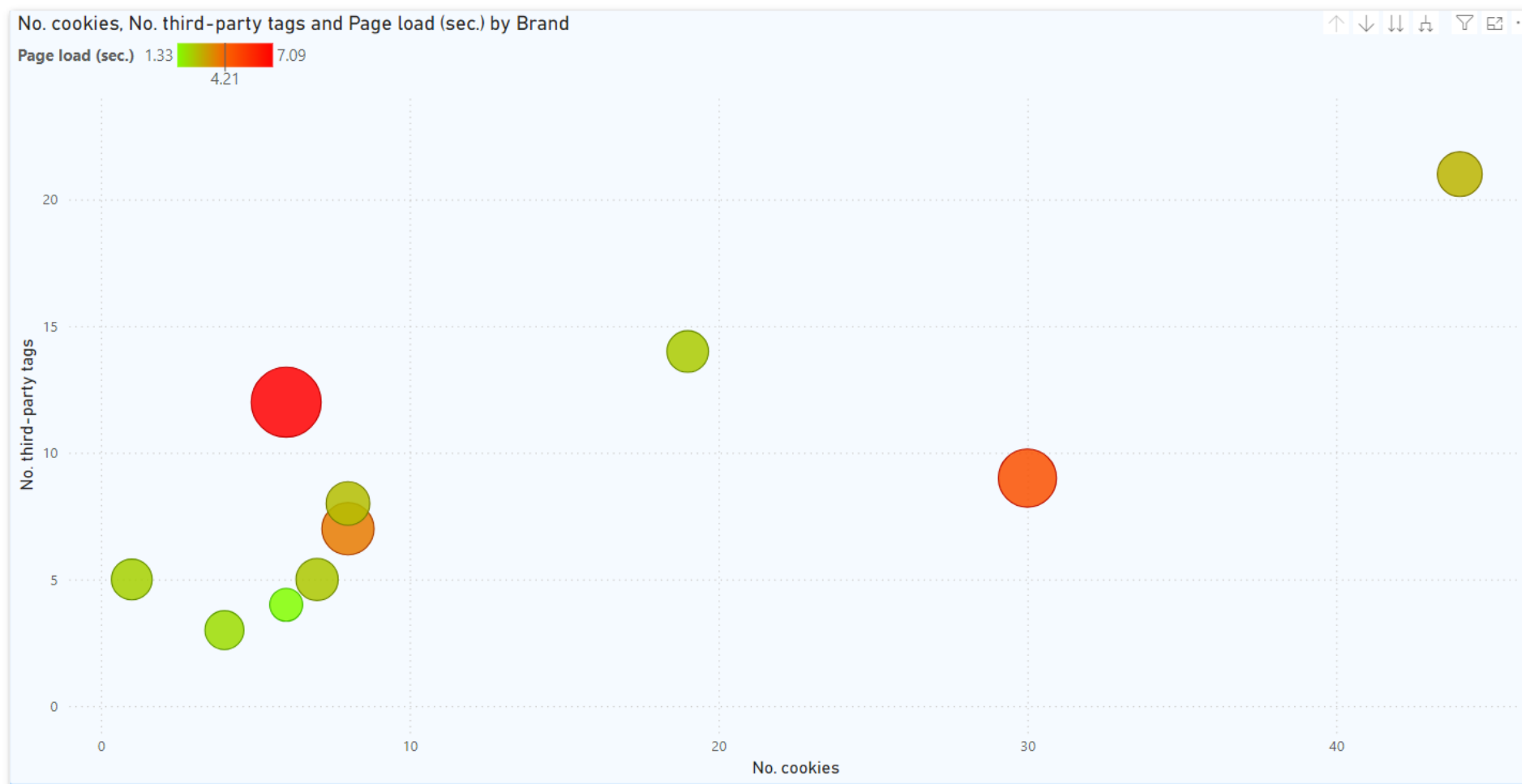
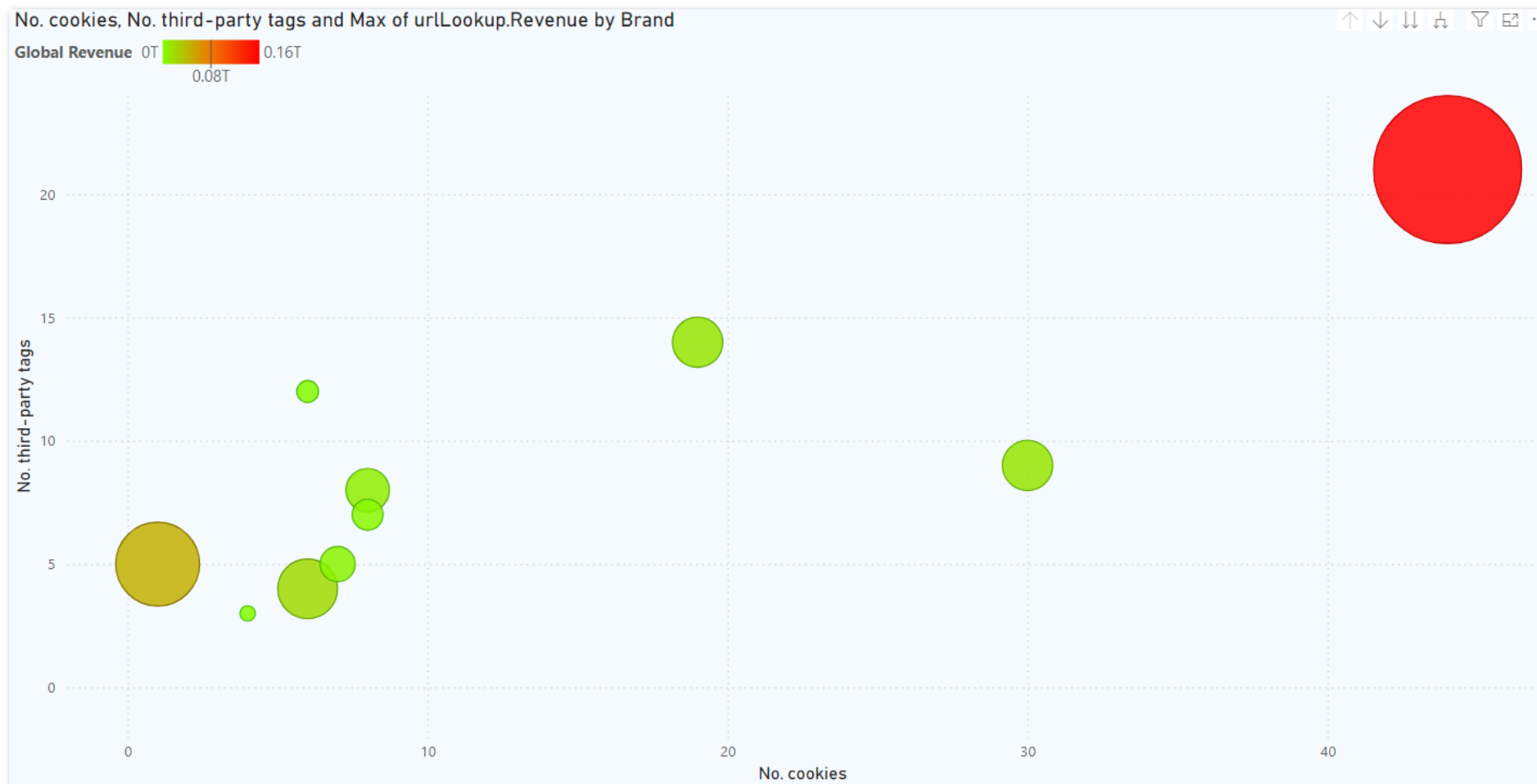


Figure 6: Media looks to be a little more compliant but with some clear outliers.



The Media sector has some clear outliers, setting a lot of tags and cookies before consent.

Banking

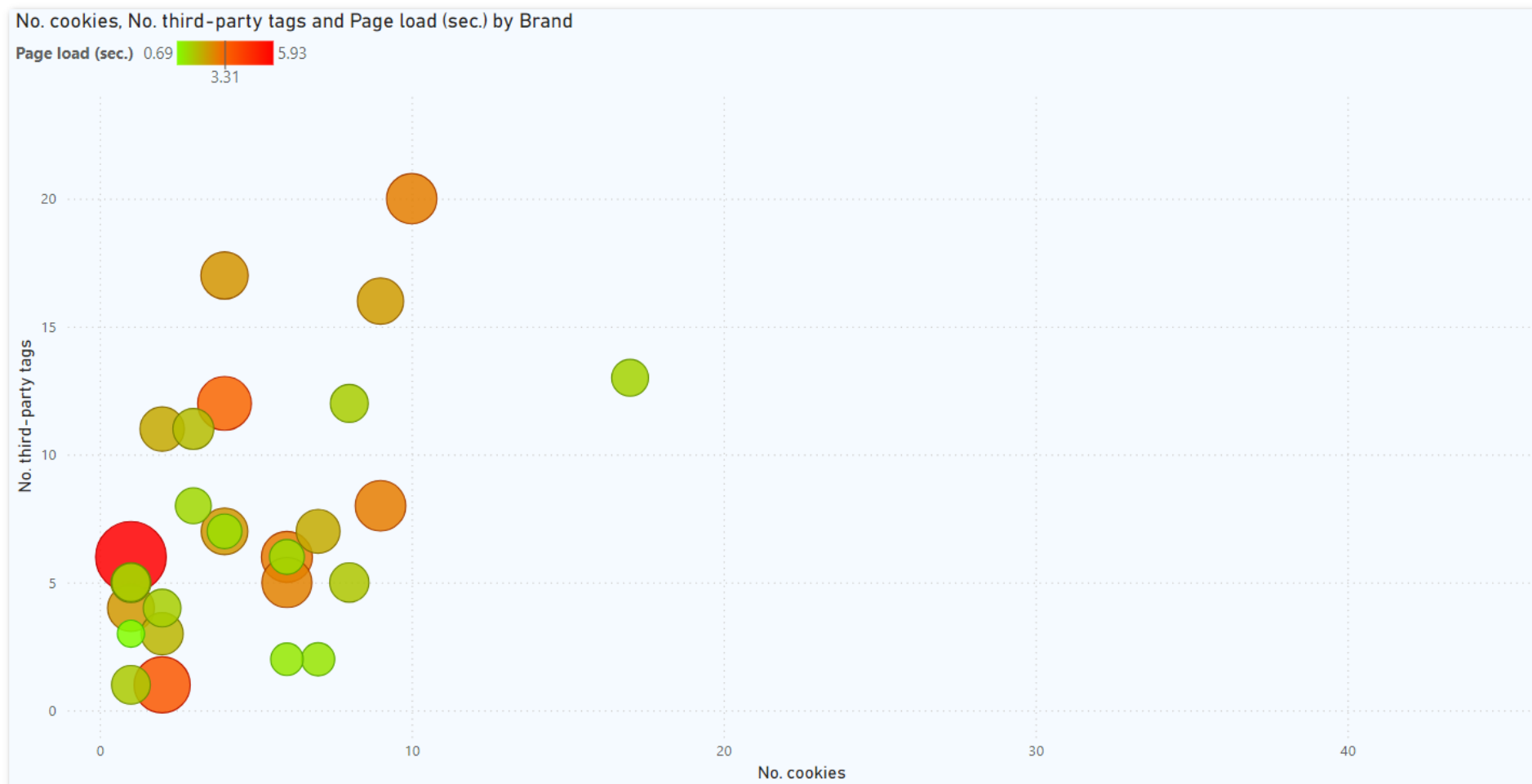
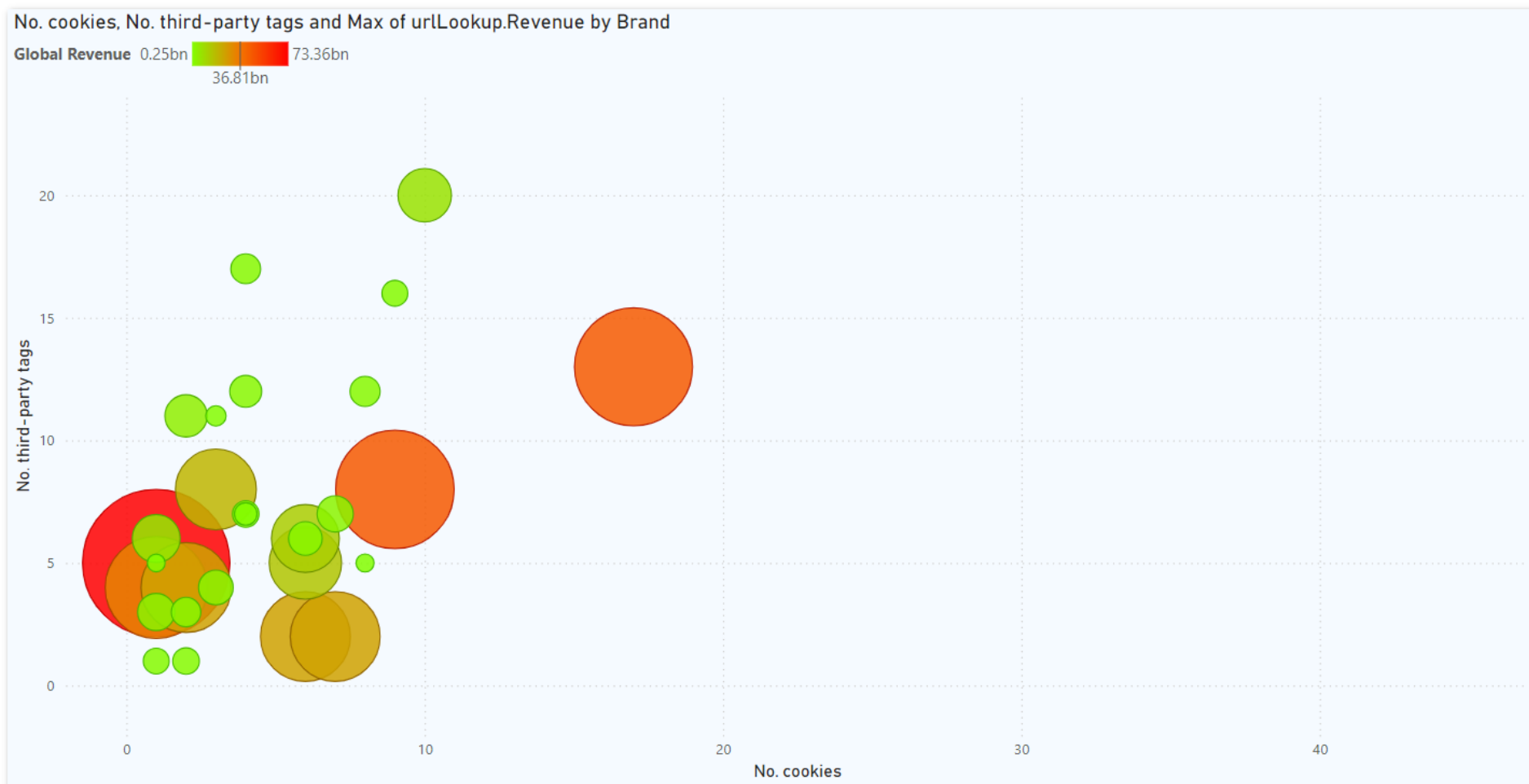


Figure 8: Banking brands are more to the left of the chart, suggesting a greater degree of compliance.



In a heavily regulated industry like Banking, brands look to be taking a stricter approach to GDPR and PECR.

Consulting

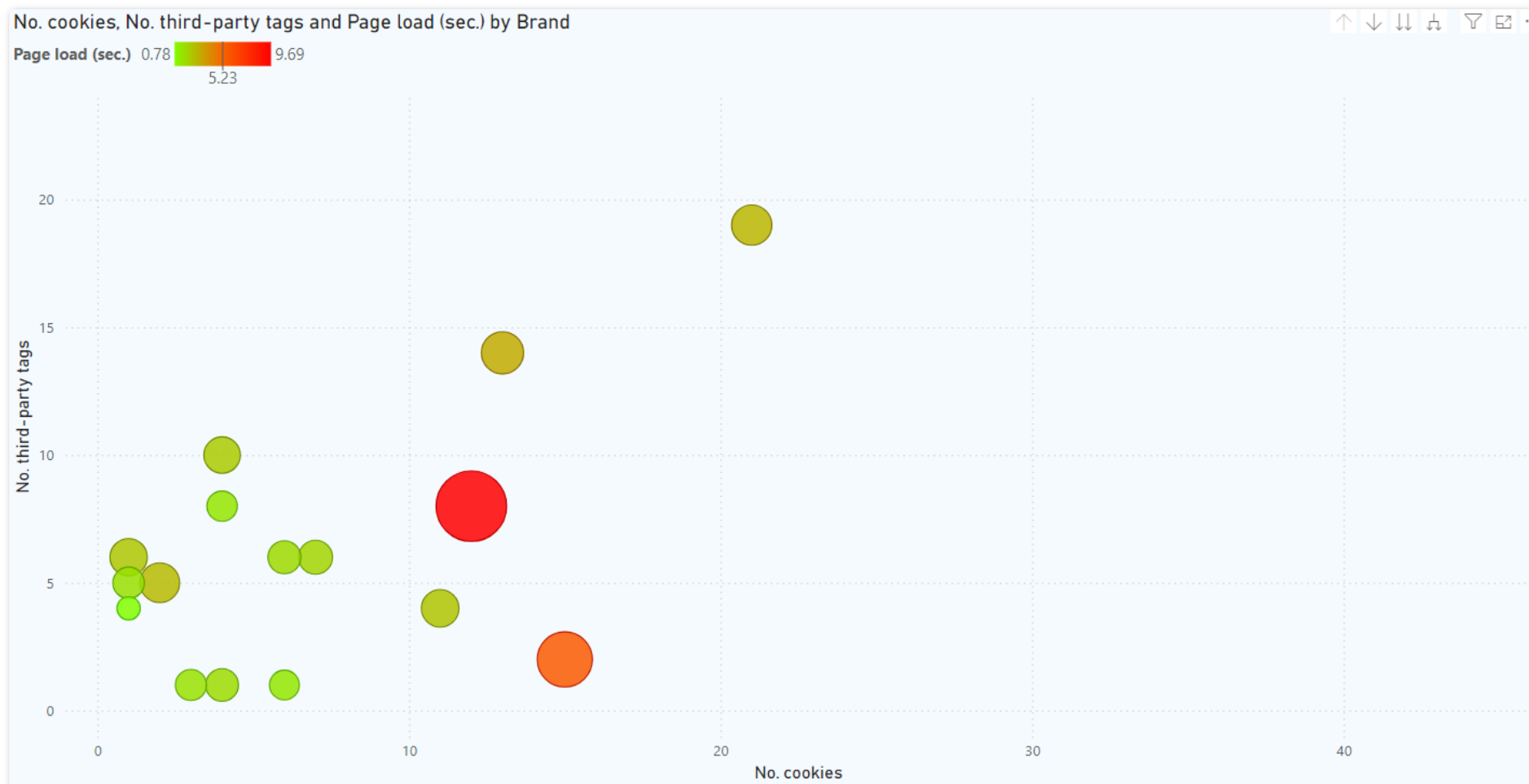
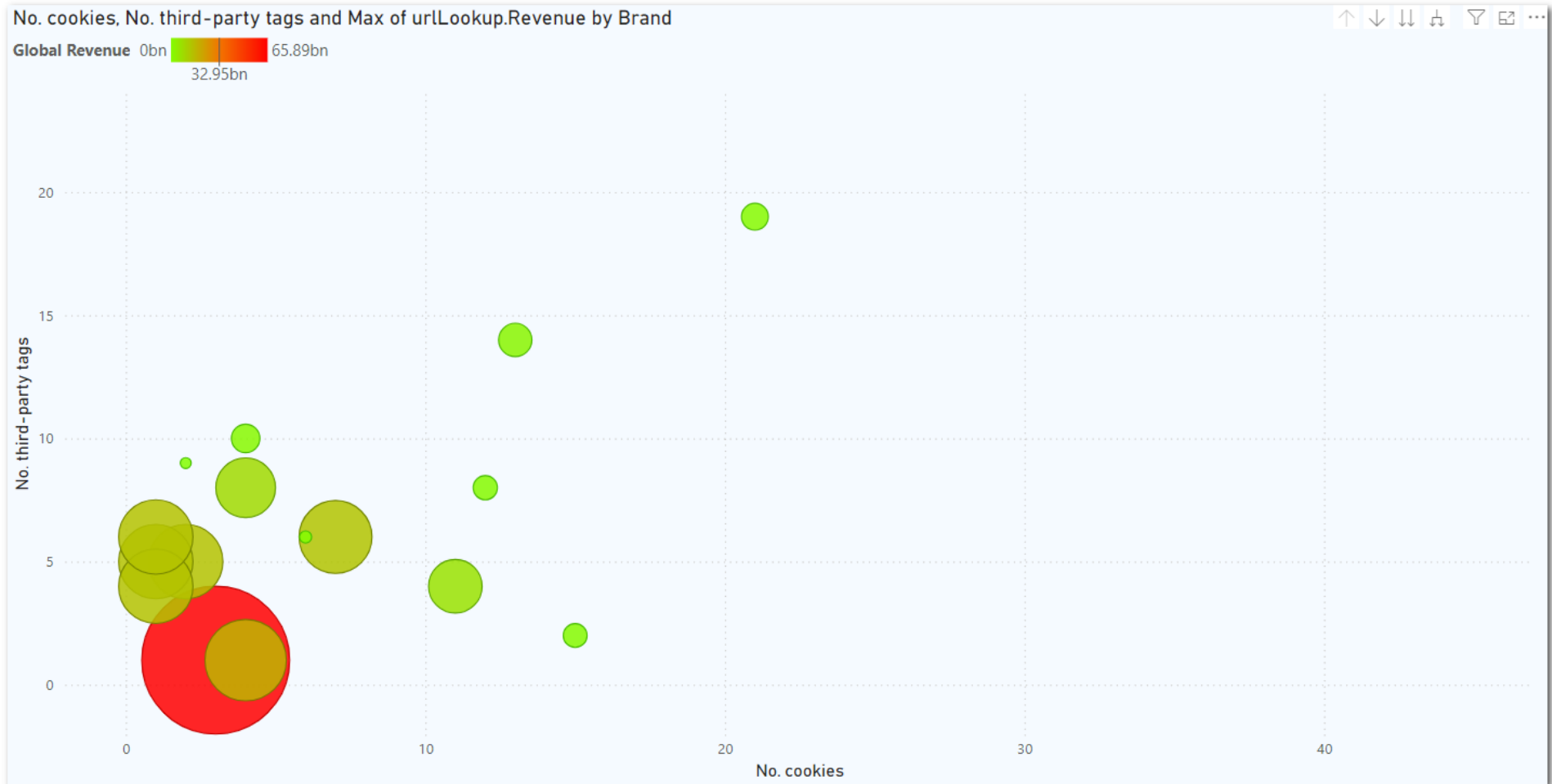


Figure 10: No major issues here, bar the outlier toward to top right.



Loop Horizon's industry sector – by and large – is relatively compliant. However, this may simply be a reflection that this industry is largely B2B, so there is less incentive to drive leads through semi-anonymous website activity.

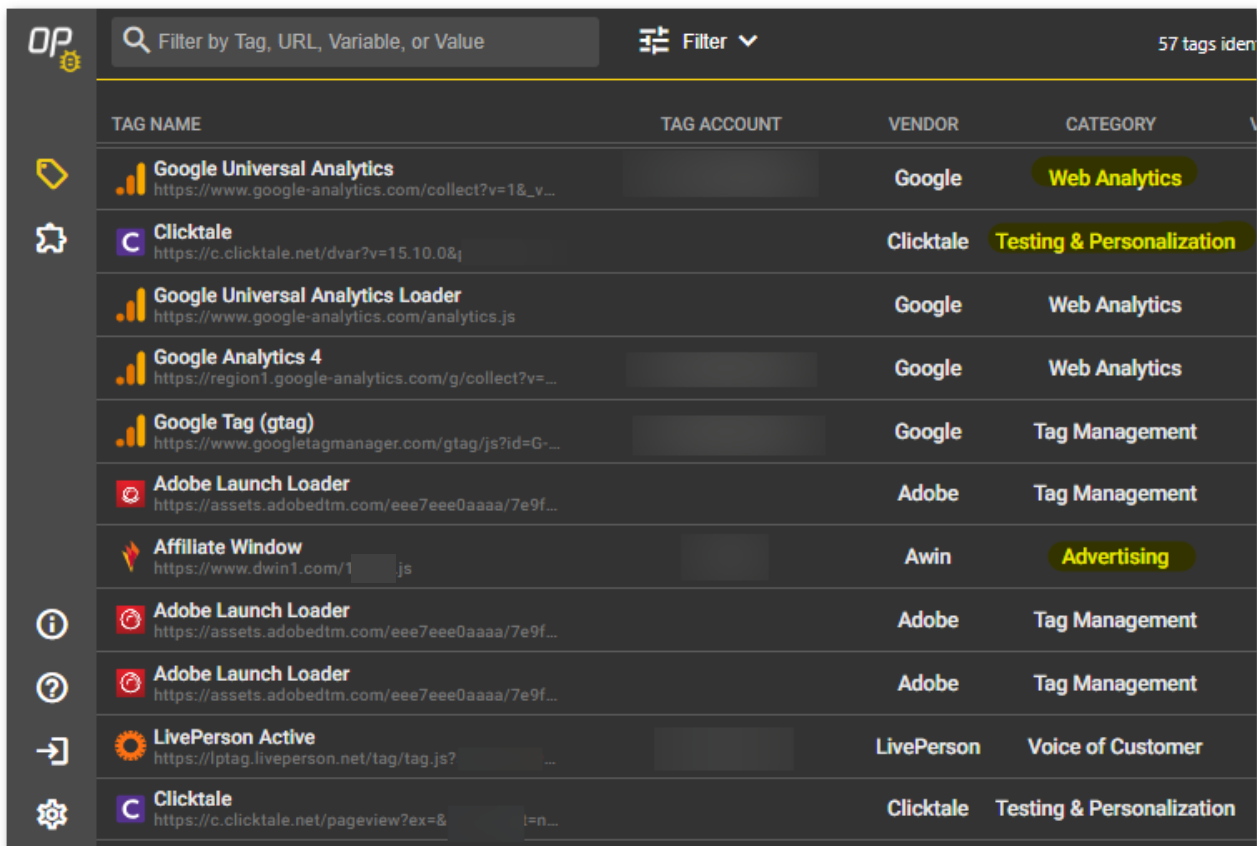
Outlier deep-dives

Reviewing two outliers from our scan in more detail, we found that a wide range of third-party vendor tags are set before user consent. These tags cover multiple usage categories, including advertising, analytics and personalisation.

These outliers mislead their end-users through their consent management platforms, by telling them that specific third-party vendor tags, or entire tag usage categories, are turned off, even though this is not the case.

They continue to track their end-users, even after the user expressly declines consent. This disregards the user's consent decision and misleads the end-user into believing they have a choice around whether they are tracked, where no choice actually exists.

Outlier one



TAG NAME	TAG ACCOUNT	VENDOR	CATEGORY
 Google Universal Analytics https://www.google-analytics.com/collect?v=1&v...		Google	Web Analytics
 Clicktale https://c.clicktale.net/dvar?v=15.10.0&l		Clicktale	Testing & Personalization
 Google Universal Analytics Loader https://www.google-analytics.com/analytics.js		Google	Web Analytics
 Google Analytics 4 https://region1.google-analytics.com/g/collect?v=...		Google	Web Analytics
 Google Tag (gtag) https://www.googletagmanager.com/gtag/js?id=G-...		Google	Tag Management
 Adobe Launch Loader https://assets.adobedtm.com/eee7eee0aaaa/7e9f...		Adobe	Tag Management
 Affiliate Window https://www.dwin1.com/1...js		Awin	Advertising
 Adobe Launch Loader https://assets.adobedtm.com/eee7eee0aaaa/7e9f...		Adobe	Tag Management
 Adobe Launch Loader https://assets.adobedtm.com/eee7eee0aaaa/7e9f...		Adobe	Tag Management
 LivePerson Active https://lptag.liveperson.net/tag/tag.js?...		LivePerson	Voice of Customer
 Clicktale https://c.clicktale.net/pageview?ex=&...&n...		Clicktale	Testing & Personalization

Figure 12: A range of tags are set before consent is given, including those for analytics, personalisation and advertising categories.

Having cleared cookies and refreshed the homepage (so acting as a new user), we see a wide range of third-party vendor tags set before consent is granted, covering advertising, analytics, personalisation and more. Here's a list of the vendors / tools found:

- Adobe Audience Manager
- Adobe Experience Platform (AEP) Interact (for Adobe Analytics and Adobe Target)

- Adobe Launch
- Affiliate Window
- Clicktale
- DynaTrace
- Floodlight Counter
- Google AdService
- Google Analytics 4 (note: advanced consent mode)
- Google Tag (gtag)
- Google Universal Analytics (note: defunct)
- LiveEngage
- Optimizely

Moreover, if you look at the Consent Management Platform for this company, you can see that specific vendor tags from the list of those set above, are meant to be switched-off by default.

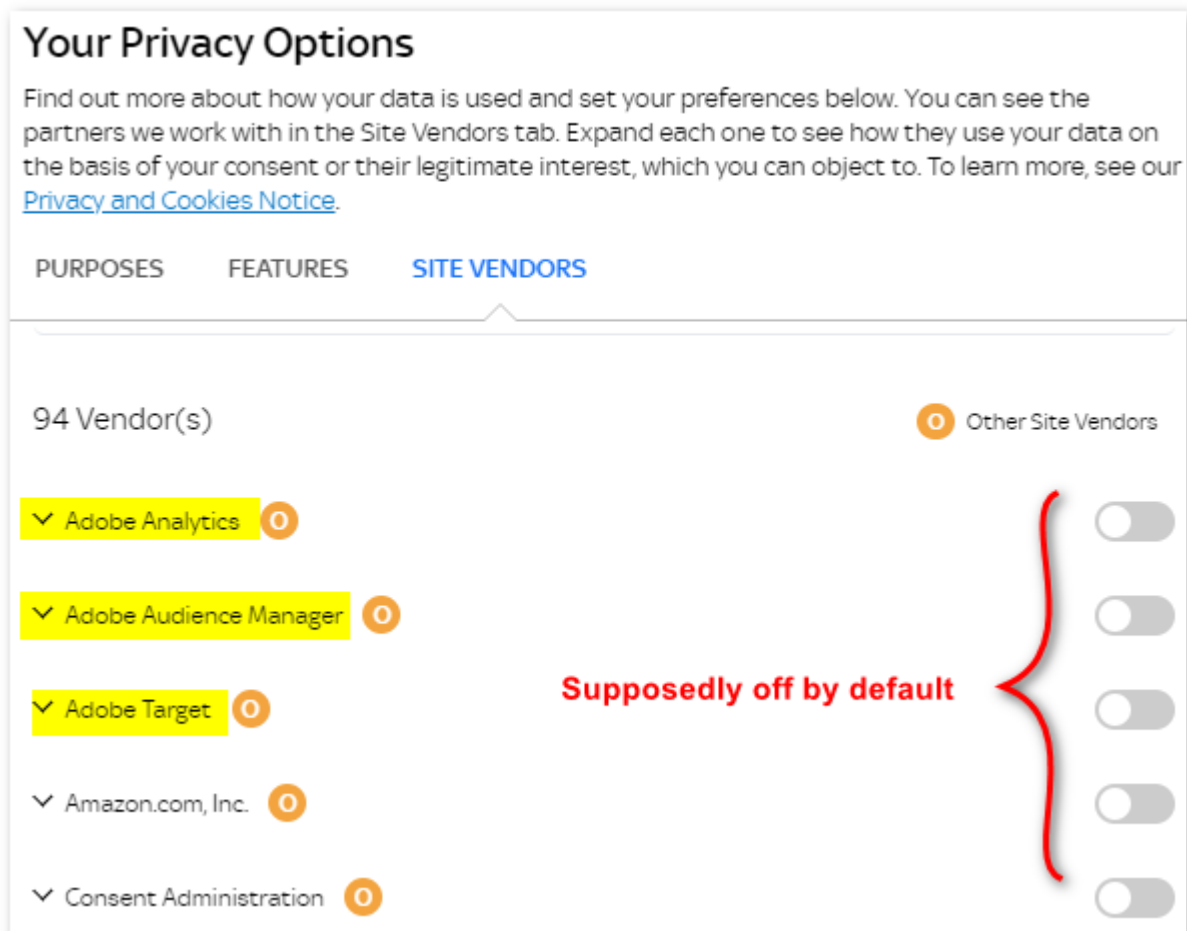


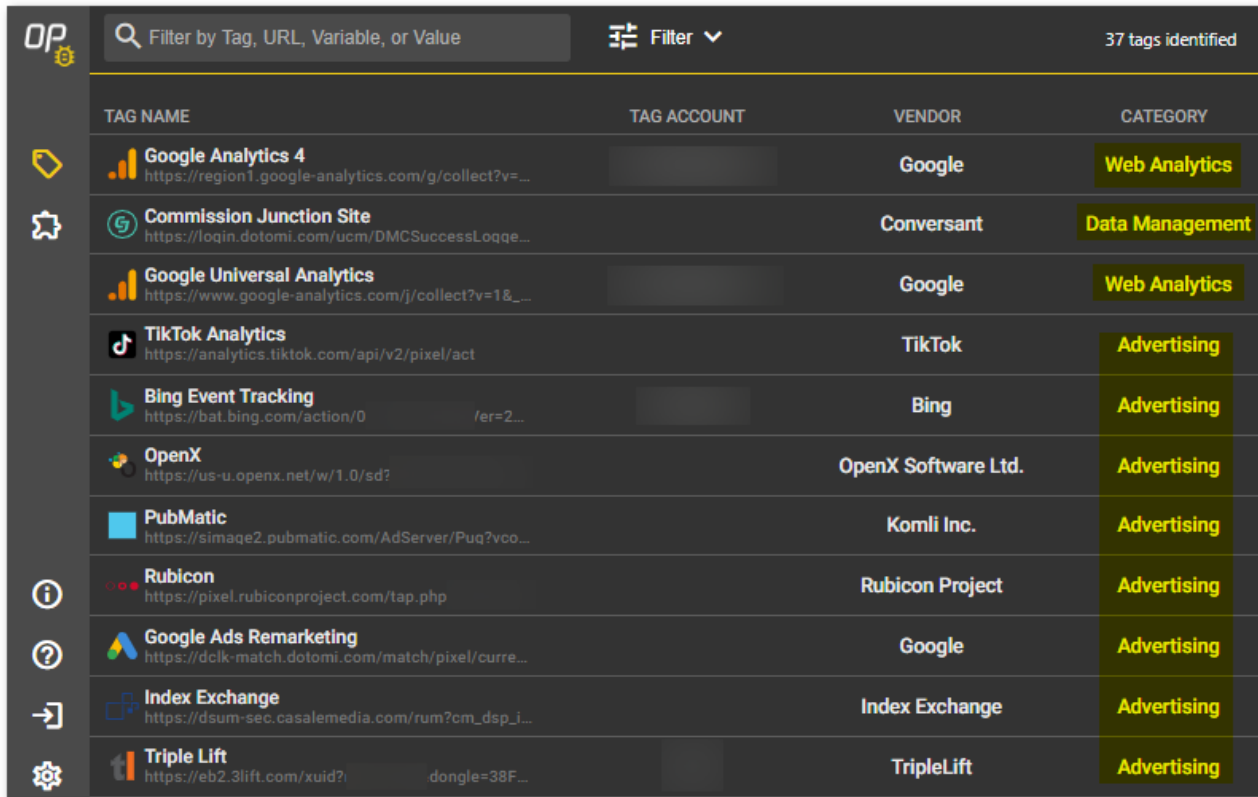
Figure 13: There are more as you scroll down the list - GA4, AWIN, LiveRamp and many more, are all meant to be off by default before consent.

If you then click to "reject all" via the Consent Management Platform, and reload the page, you still receive all of the vendors that were set pre-consent (as in, the list is identical). In other words

– declining consent with this company makes no difference at all to the level of tracking a user is subjected to.

Whether intentional or not, this company is misleading its users – tracking users while telling them that they are not being tracked, and giving users the appearance of control while disregarding their choices.

Outlier two



TAG NAME	TAG ACCOUNT	VENDOR	CATEGORY
 Google Analytics 4 https://region1.google-analytics.com/g/collect?v=...		Google	Web Analytics
 Commission Junction Site https://login.dotomi.com/ucm/DMCSuccessLoqqe...		Conversant	Data Management
 Google Universal Analytics https://www.google-analytics.com/j/collect?v=1&_...		Google	Web Analytics
 TikTok Analytics https://analytics.tiktok.com/api/v2/pixel/act		TikTok	Advertising
 Bing Event Tracking https://bat.bing.com/action/0 /er=2...		Bing	Advertising
 OpenX https://us-u.openx.net/w/1.0/sd?		OpenX Software Ltd.	Advertising
 PubMatic https://simage2.pubmatic.com/AdServer/Puq?vco...		Komli Inc.	Advertising
 Rubicon https://pixel.rubiconproject.com/tap.php		Rubicon Project	Advertising
 Google Ads Remarketing https://dclk-match.dotomi.com/match/pixel/curre...		Google	Advertising
 Index Exchange https://dsum-sec.casalemedia.com/rum?cm_dsp_i...		Index Exchange	Advertising
 Triple Lift https://eb2.3lift.com/xuid? dongle=38F...		TripleLift	Advertising

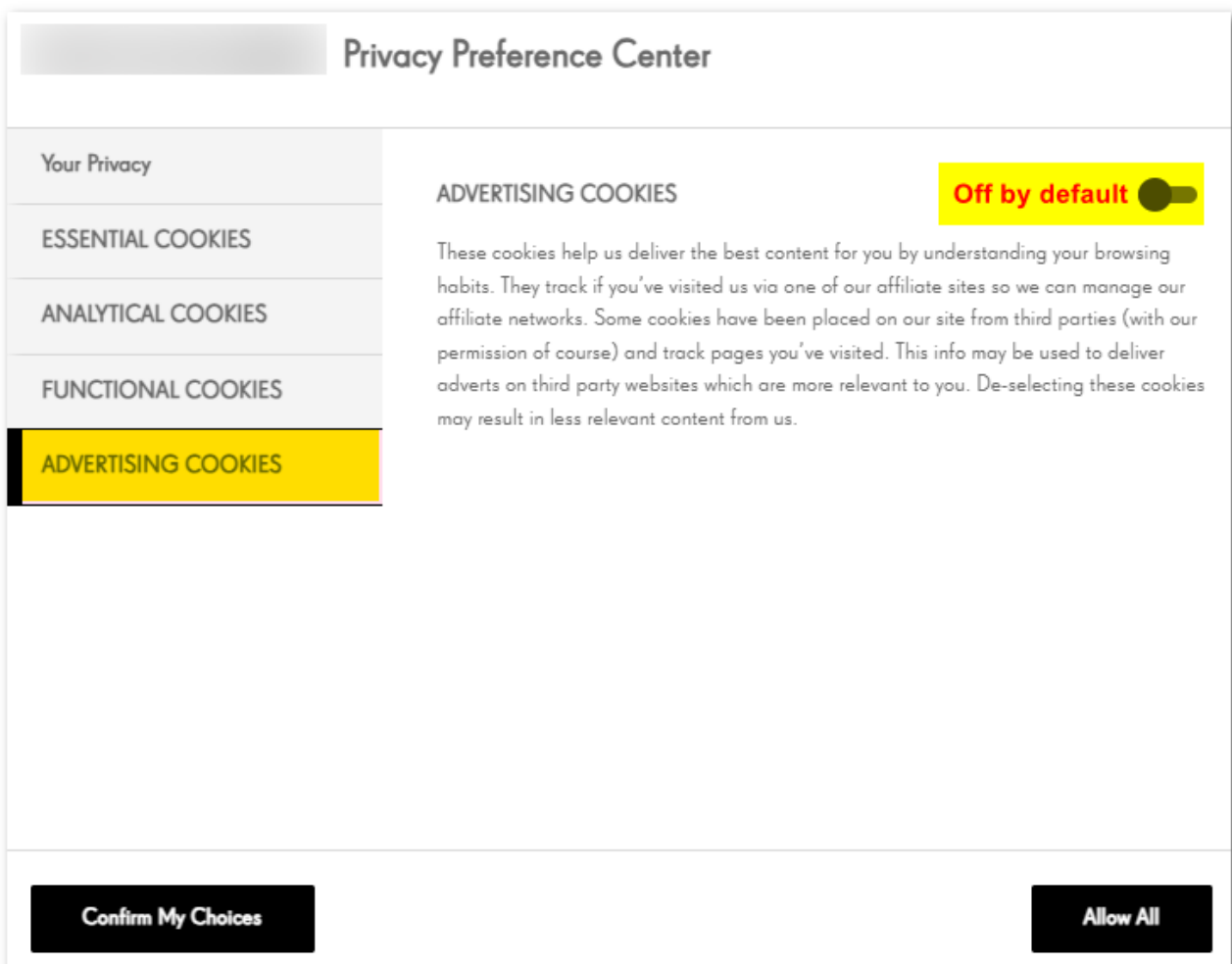
Figure 14: A range of tags are set before consent is given, with by-far the largest group being for advertising, used to track users around the web.

Having cleared cookies and refreshed the homepage (so acting as a new user), we see a wide range of third-party vendor tags set before consent is granted, covering advertising, analytics, personalisation and more. Here's a list of those vendors / tools found:

- Akamai mPulse
- Bing
- BloomReach Loader
- Commission Junction Site
- Conversant
- DAX Audio
- DynaTrace Monitor
- Google Ads Remarketing
- Google Analytics 4
- Google Tag (gtag)

- Google Tag Manager
- Google Universal Analytics
- Index Exchange
- OneTrust
- OpenX
- PubMatic
- Rubicon
- TikTok
- Triple Lift

Again, if you look at the Consent Management Platform for this company, you can see that "Analytics", "Functional" and "Advertising" tags are meant to be switched-off by default.



Privacy Preference Center

Your Privacy

ESSENTIAL COOKIES

ANALYTICAL COOKIES

FUNCTIONAL COOKIES

ADVERTISING COOKIES

ADVERTISING COOKIES **Off by default**

These cookies help us deliver the best content for you by understanding your browsing habits. They track if you've visited us via one of our affiliate sites so we can manage our affiliate networks. Some cookies have been placed on our site from third parties (with our permission of course) and track pages you've visited. This info may be used to deliver adverts on third party websites which are more relevant to you. De-selecting these cookies may result in less relevant content from us.

Confirm My Choices **Allow All**

Figure 15: Here we see "Advertising" switched-off by default. The "Analytics" and "Functional" cookies are also switched-off by default.

If you then click "Confirm My Choices" in order to reject "Analytics", "Functional" and "Advertising" tags and cookies, and refresh the page – interestingly, rather than blocking most third-party vendor tags, *some new ones are set*, only Google Ads Remarketing is turned off.

Here're the new vendors set after rejecting consent (both of which are categorised by ObservePoint Debugger as "Advertising" tags):

- Eyeota
- Freewheel Ads

Whether intentional or not, this brand is also misleading users – tracking users while telling them that they are not being tracked, and giving users the appearance of control while disregarding their choices.

These two examples also demonstrate that the scan we have performed is a reasonable indicator of how much a brand adheres to regulatory requirements.

Example report

What follows on the next page is an example of what you'll receive, using the Loop Horizon website as a guineapig.

If you have not already provided site details for your FREE personalised report and would like to do so, please reach out to us via email and use the email title "Cookie Compliance in the UK – Free Report":

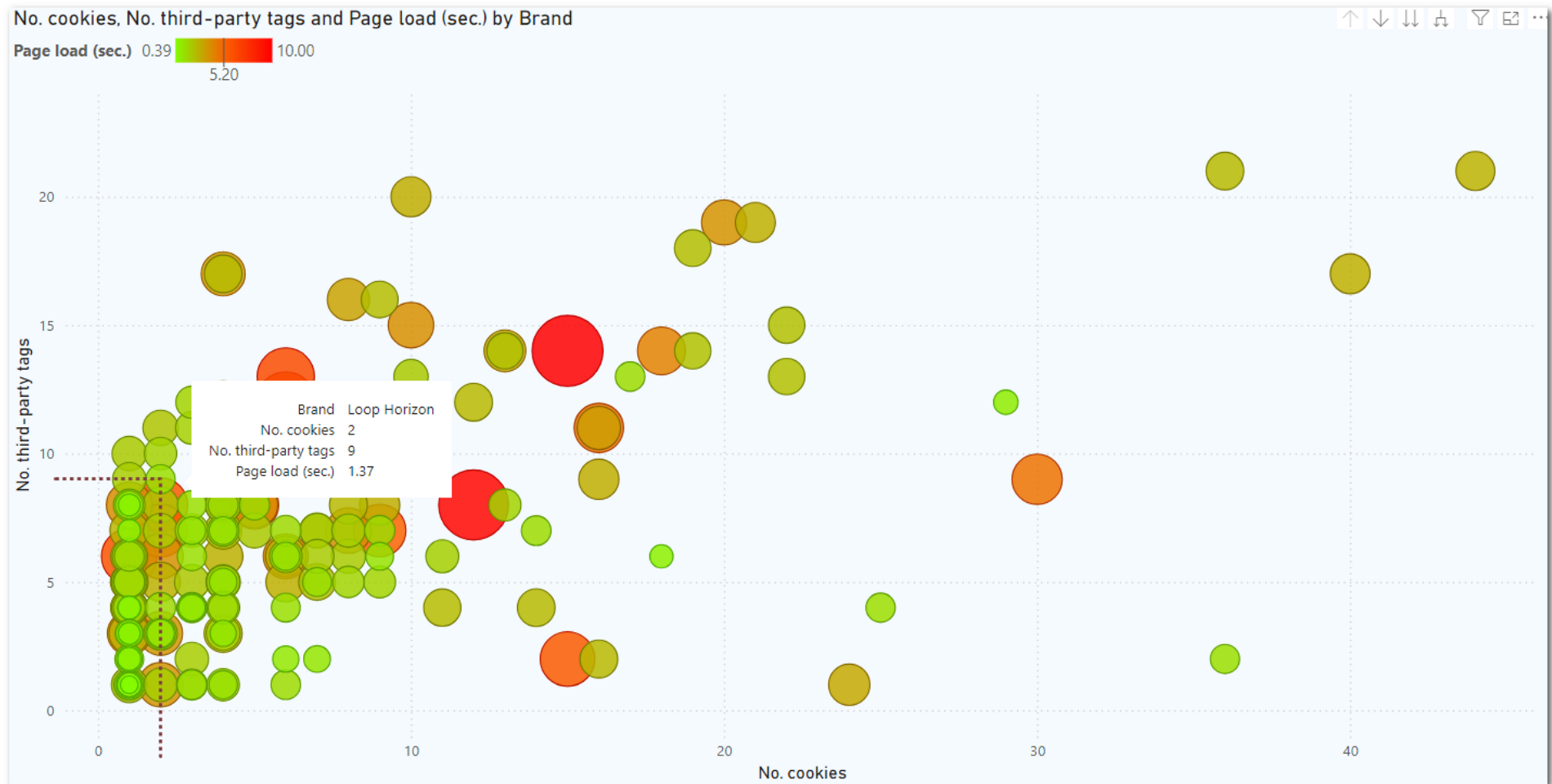
info@loophorizon.com

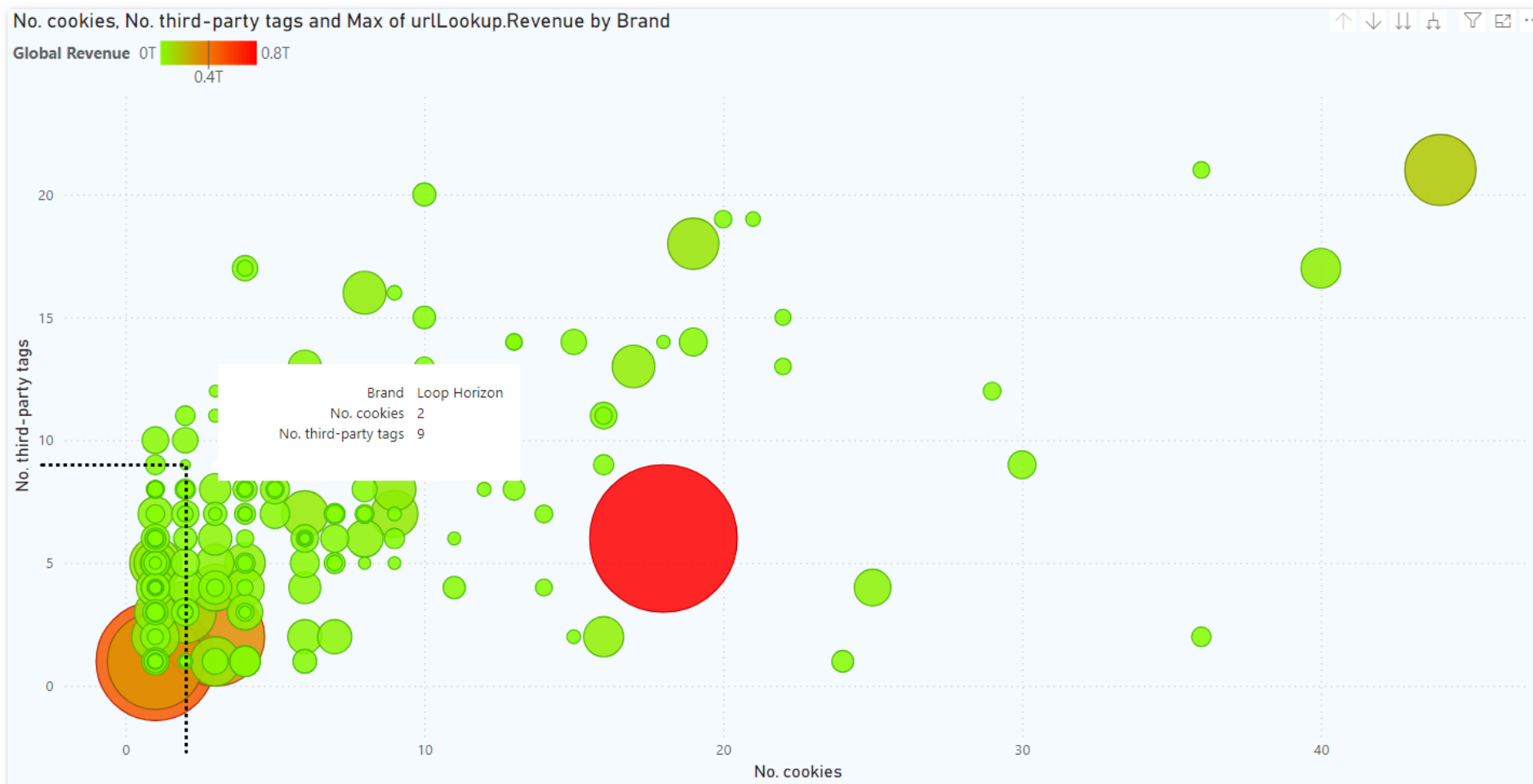
We will place your website into the compliance dashboard we email to you, and provide a deep-dive into your tag and cookie compliance performance, to help you understand your current-state, and give actionable insight into areas for improvement.

Loop Horizon

Global view

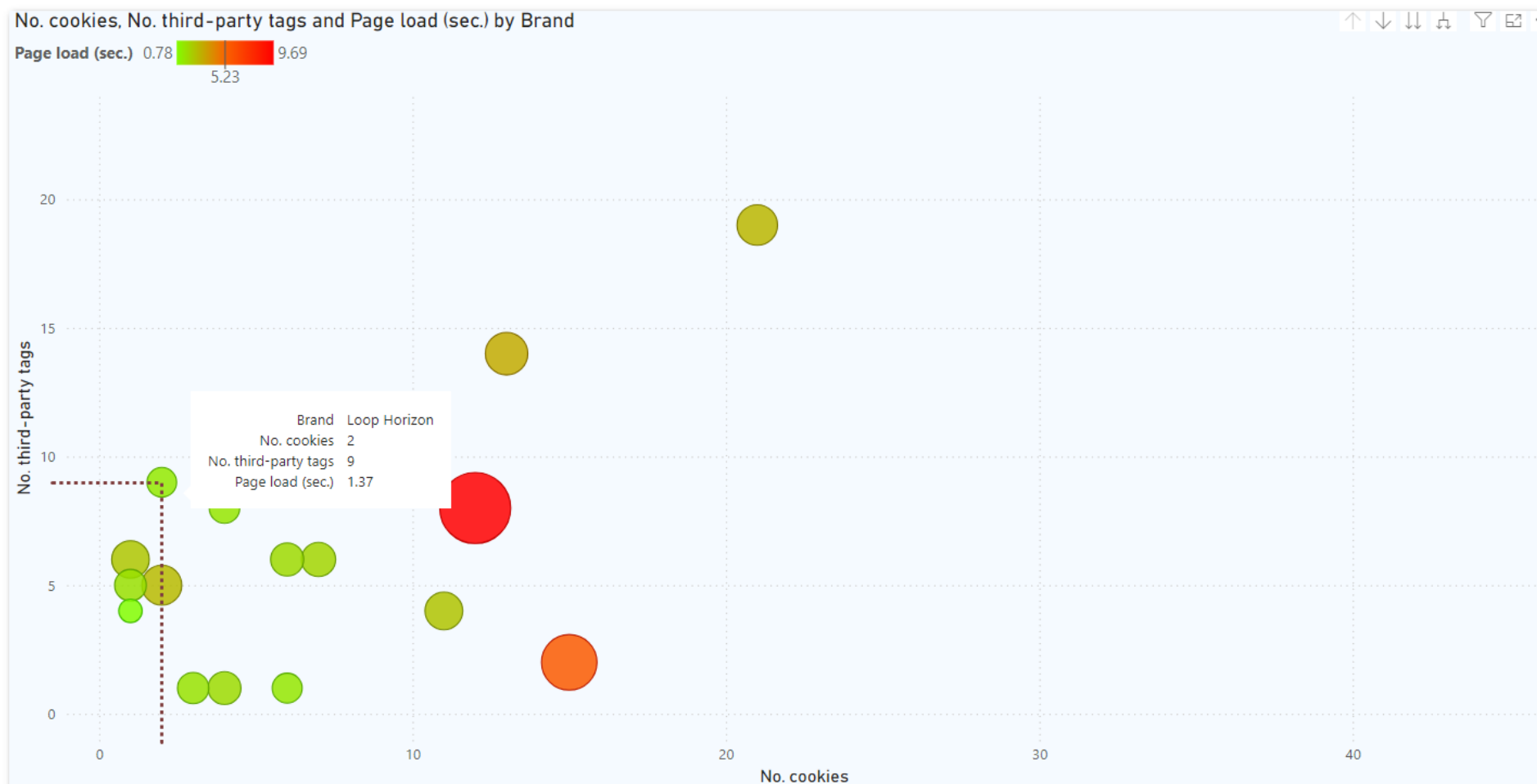
The Loop Horizon homepage sets 9 tags and 2 cookies before consent. This places Loop Horizon at the lower end of the scale.

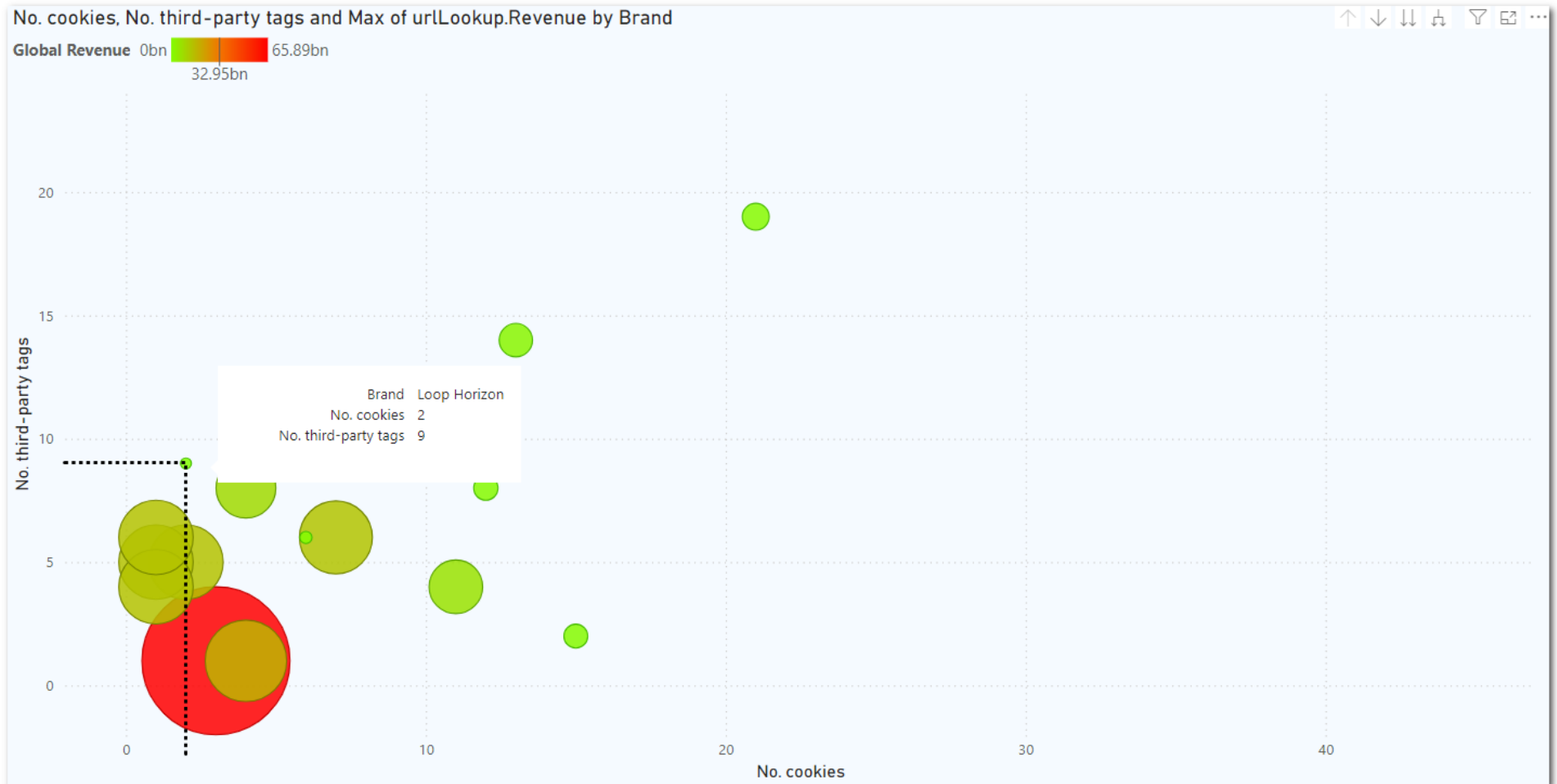




Consulting sector

However, among companies within the same industry sector, while the number of cookies set is low in comparison, the number of tags set by Loop horizon is relatively high.





The numbers

Below is how Loop Horizon compares to global and industry mean averages:

	Loop Horizon	Global avg.	% difference
Cookies	2	7	-72%
Tags	9	7	+26%

	Loop Horizon	Industry sector avg.	% difference
Cookies	2	7	-70%
Tags	9	7	+36%

Averages can be skewed by outliers.

Looking at ranking position (sorting low to high, where position 1 is the fewest tags / cookies served before a user has granted consent):

Loop Horizon	Global	Industry sector
Cookies	Joint 39/163	Joint 4/18
Tags	Join 119/163	14/18

If we look at the unique-value median averages, this is borne out:

	Loop Horizon	Global unique median	% difference
Cookies	2	15	-87%
Tags	9	11	-18%

	Loop Horizon	Industry sector unique median	% difference
Cookies	2	8	-75%
Tags	9	7	+29%

Deep-dive

Our deep-dive moves beyond manually scanning for tags using the ObservePoint Debugger Chrome Extension (excellent though this is). We have access to our own instance of the paid ObserveOoint platform and have used this to scan your homepage. Here are the results.

Tags

The majority of the tags set are for: consent; providing content to the end user; tag management. That is to say; tools to deliver website content and to decide which tracking tags to set rather than setting the tags themselves.

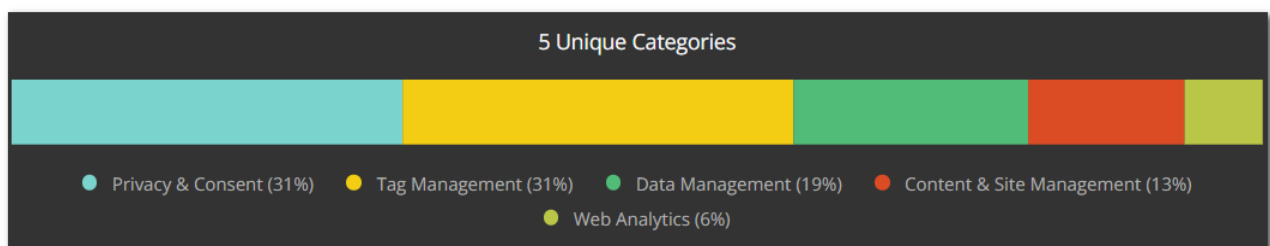


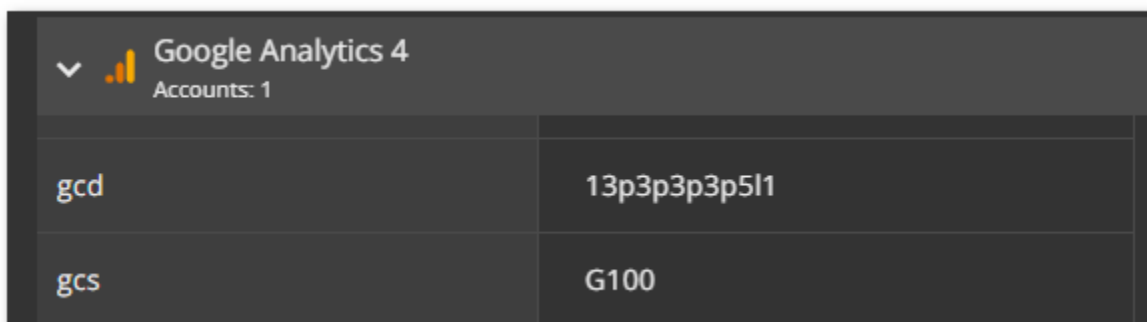
Figure 5: Author note - Loop Horizon has three tag management systems because we offer services for these vendors to our clients, so deploy these to our website for testing, validation and demonstration purposes.

Here are the vendors found:

1. Adobe Launch
2. Cloudfront
3. Data Layer
4. Google Analytics 4
5. Google Fonts
6. Google Tag (gtag)
7. Google Tag Manager
8. OneTrust
9. Tealium iQ

There is one exception – Google Analytics 4 – which is categorised as “web analytics”. This is being set before consent.

On further investigation, this is being set in Google’s “advanced consent mode v2” where no cookie is set to the site, and data collection is sent as anonymous hits.



Google Analytics 4 Accounts: 1	
gcd	13p3p3p3p5l1
gcs	G100

- The “p” values in the GCD string means - denied by default (no update)
- The GCS value of G100 means - no consent has been granted

While consent mode v2 is required for all Google tags, and while advanced consent mode v2 is designed to help track activity in a way that complies with privacy laws, there is debate as to whether advanced consent mode v2 actually does comply with regulatory requirements.

You may wish to reach out to your legal and compliance team (if you have not done so) to give confidence that your business accepts the risk of deploying Google Analytics 4 in advanced consent mode v2.

The alternative approach is to block Google Analytics 4 from firing until explicit user consent has been granted for “web analytics”, and only then send data to Google Analytics 4 (with the required consent mode v2 variables included). This is known as basic consent mode v2.

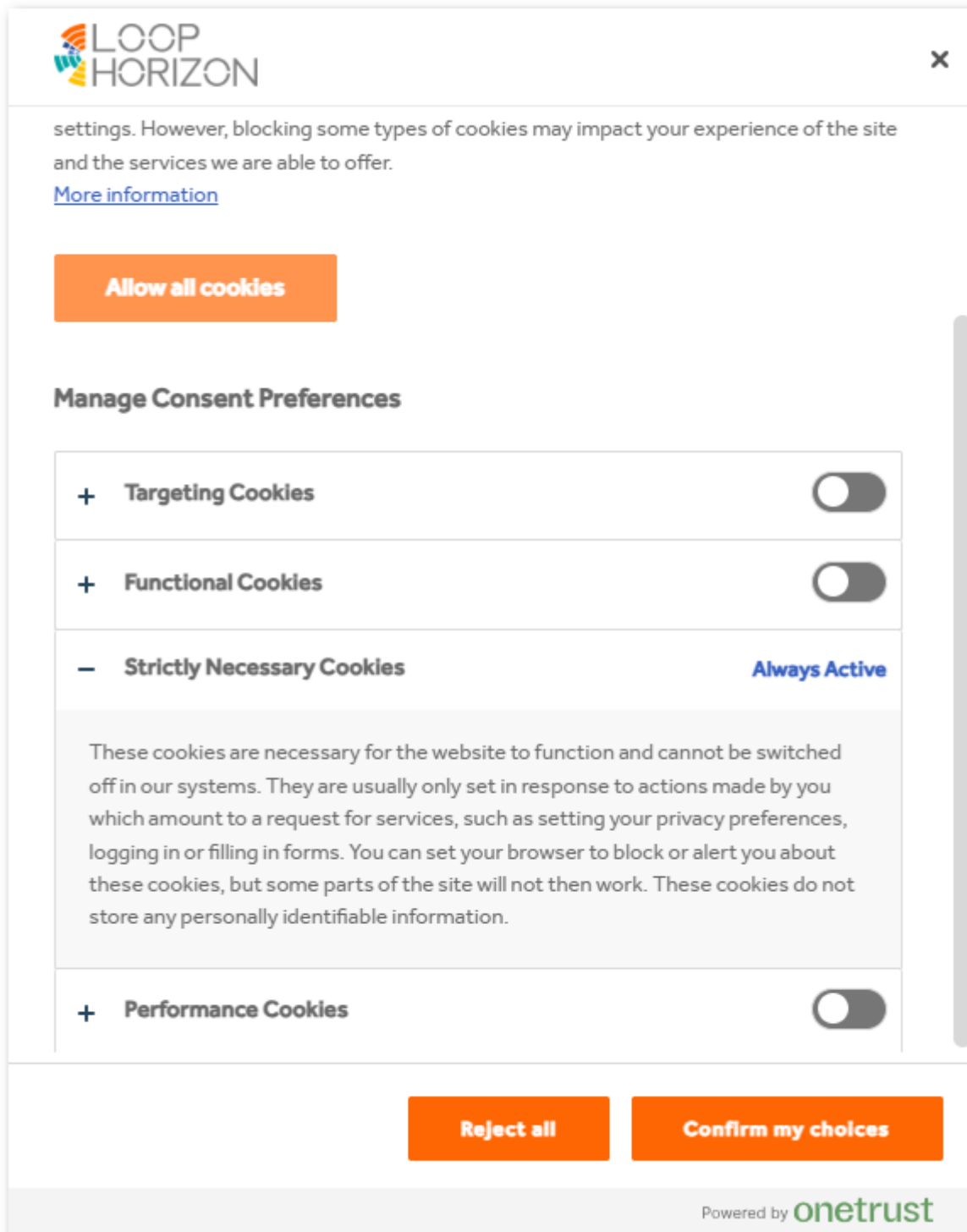
Cookies

Only two cookies are set. One relates to consent management and helps the site remain compliant. The other relates to tag management. Both are first-party cookies; set to the main website domain.

COOKIE NAME	DOMAIN	INITIATOR(S)	1ST/3RD PARTY	PARTITION KEY	DURATION	SAMESITE	SECURE	HTTPONLY	AVG SIZE (BYTES)
> OptanonCons...	loophorizon.com	1 	1st	---	365d	None	true	false	249
> utag_main	loophorizon.com	1 	1st	---	365d	---	false	false	141

Consent Management Platform

Looking at Loop Horizon's consent management platform banner, we see that all non-essential cookie and tag categories are off by default. This aligns with what we see in ObservePoint.



The screenshot shows a consent management banner for Loop Horizon. At the top left is the Loop Horizon logo, and at the top right is a close button (X). Below the logo, there is a paragraph of text: "settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer." followed by a link "More information". Below this is a large orange button labeled "Allow all cookies". Underneath is a section titled "Manage Consent Preferences". This section contains four rows, each with a category name, a plus or minus icon, and a toggle switch. The categories are: "Targeting Cookies" (plus icon, toggle off), "Functional Cookies" (plus icon, toggle off), "Strictly Necessary Cookies" (minus icon, toggle always active), and "Performance Cookies" (plus icon, toggle off). The "Strictly Necessary Cookies" row has a blue text label "Always Active" to its right. Below the "Strictly Necessary Cookies" row is a detailed explanation: "These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information." At the bottom of the banner are two orange buttons: "Reject all" and "Confirm my choices". At the very bottom, it says "Powered by onetrust".

LOOP
HORIZON

settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.
[More information](#)

Allow all cookies

Manage Consent Preferences

- + Targeting Cookies ☐
- + Functional Cookies ☐
- Strictly Necessary Cookies **Always Active**

These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.
- + Performance Cookies ☐

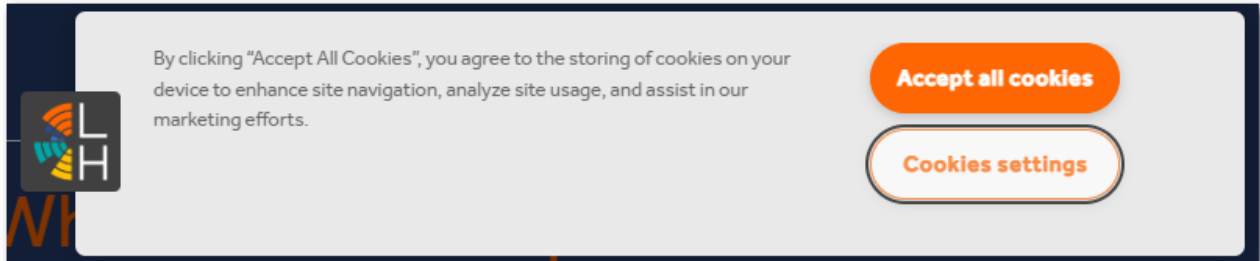
Reject all **Confirm my choices**

Powered by **onetrust**

However, the banner does not contain a "reject all" option. To meet ICO guidance you may wish to investigate adding a "reject all cookie" option that has equal prominence to the "accept all cookies" button.

This should be done with careful consideration – please ensure that your business carefully validates the impact on consent rates, and therefore on reporting, marketing, personalisation programs (and beyond), and ultimately on revenue, that adding a “reject all” button will cause.

This will help you make an informed choice, understanding the impact of reduced consent rates on your business.



Additional information

ObservePoint provides a top-level summary across a range of measure. Because this scan only covered your homepage, not all the summary measures are relevant. A large sample size brings these measures into play.

Audit Score 62.9/100	Tag Presence 30/30	Tag Performance 20/20	Rules 0/30	Page Performance 2.9/10	Cookies 10/10
trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	No rules assigned to this run	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed

Audit score

This is an aggregation of the wide range of variables ObservePoint measures, intended to give a top-level view of your website’s alignment to best practices.

Tag presence

This is one of the measures that needs a scan across multiple pages. It gathers data about tag presence across multiple pages and gives a score based on tags that are present on some pages and missing on others. This will always score top-marks when the scan only covers a single page.

Tag performance

This scores the load time of your tags and calculates the score based on those that have load time under 500ms vs over 500ms. The more tags loading in over 500ms, the lower the score. Your score is 20/02 – only if we see a score under 20/20, will we include a list tags that are loading slowly.

Rules

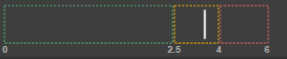
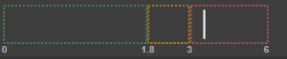
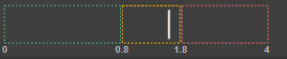
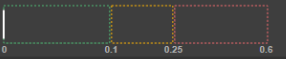
This metric only applies if specific “rules” have been defined for an audit, so does not apply to this scan. The usual approach is to run a discovery phase and identify pain points impacting a

company's digital estate. The audit is then tailored to monitor and explain these pain points, with rules being applied to automatically assess and alert you to any failures.

For example, a business may have concerns about data quality. The pain point identified in discovery may be consistency of variables collected by Google Analytics 4. A rule could set up a rule to monitor data flowing into GA4 and identify any pages where it does not meet the defined standards. This can be set up to result in email alerts and would be reflected in the top-level "rules" score.

Page performance

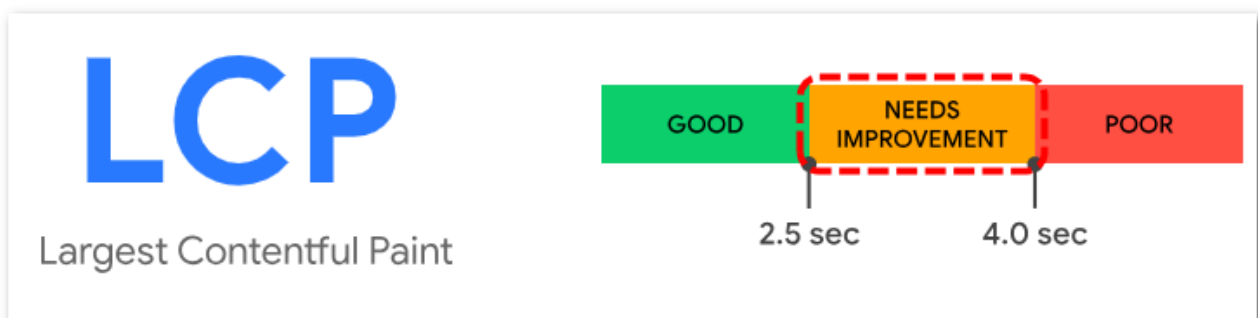
This score reflects how quickly pages are loading. Your score of 2.9/10 reflects a fairly slow website. Given your "tag performance" score is good, this is more likely to be an issue with the website itself rather than a tagging problem.

Pages Scanned	Average Page Load Time 3.59 sec	Broken Initial Pages 0	Broken Final Pages 0	Pages with Broken Links 0
1	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed
WEB VITALS - 75TH PERCENTILE ?				
Largest Contentful Paint 3.511 sec	First Contentful Paint 3.511 sec	Time To First Byte 1,582 ms	Cumulative Layout Shift 0	
trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	trend lines will appear as new runs are performed	
				

ObservePoint assesses performance using industry-standard measures called Core Web Vitals - performance metrics developed by Google to understand and improve user experience.

Largest Contentful Paint (LCP) – 3.511 seconds

This measures the time it takes for the largest visual change to happen on the page. As visible content changes (text, images, and so on), the size of the change is measured in pixels. If the size is bigger than the previously recorded visual change, this is recorded as LCP.



First Contentful Paint – 3.511 seconds

This number measures the time it takes for the first visual content to appear on the page.

FCP

First Contentful Paint



Time to First Byte – 1,582 ms

This number measures the time it takes for your website to respond to the user's browser with any data at all.

TTFB

Time To First Byte



Cumulative Layout Shift - 0

Sometimes pages move content while they are loading, which can be very frustrating if you are trying to interact with the page. CLS measures the amount of movement.

CLS

Cumulative Layout Shift

