

# How to Achieve a 70% Opt-In Rate for Website Consent

## Allow cookies & tracking?

Cookies and anonymous visitor tracking help us give you a better experience, improve our products, and keep our marketing costs down. We won't turn them on until you accept. [Learn more in our cookie policy.](#)

Customize

Accept

**Brian Clifton**

Data quality and privacy expert, best-selling author

# Table of Contents

2

---

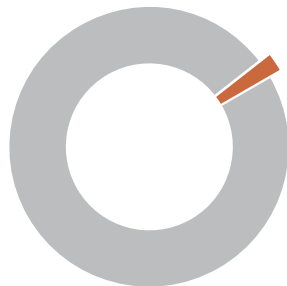
01	<b>Introduction</b>	3
02	<b>Consent is Good For Business</b>	4
03	<b>The Impact of Consent</b>	5
04	<b>The Five Key Principles of Consent</b>	7
05	<b>The Opt-in Challenge</b>	12
06	<b>Optimising Your Opt-in Rate</b>	15
07	<b>Conclusions</b>	17
08	<b>About the Author &amp; Other Contributors</b>	18

---

With the GDPR regulation, other privacy laws and the impending loss of many cookie based tracking solutions, getting your web/app data collection right has never been more important. And getting it right starts with the crucial first step, your user's consent.

There are two major hurdles to get right:

- **Verifying consent compliance** - a legal requirement for GDPR.
- **Optimising for high opt-in rates** - because low opt-in rates will seriously damage your ability to run your business.



**Only 2% of websites get consent compliance correct.\***

Compliance is the domain of your legal team - it is their job to protect the business. But beyond specifying the legal requirements and checking the banner displays correctly, legal teams rarely get involved verifying what happens next i.e. if and what data actually gets collected and under what conditions.

Obtaining a high opt-in rate is the focus of the data and marketing teams and is where your web design team also joins in. By definition, there will be people who come to your website that do not wish to be tracked and that must be honoured. However, your banner design can influence this dramatically. Get this right and your opt-in rate will be sufficient for you not to worry about data loss. Get it wrong and your online business will suffer. Businesses cannot compete, or even survive, without good data.

**This document is a best practice guide that bridges the gap between the legal needs for compliance and the business need for optimal opt-in rates.** Its purpose is to empower you so you can join the consent discussion. The approach taken is from the point of view of GDPR compliance.

\* Verified Data study, Superweek conference, Hungary, 2020. [Slideshare link](#) (see slide 8). Other studies reporting comparable numbers can be found at TechCrunch e.g. [Article 1](#); [Article 2](#).

In this context, gaining consent means the permission to track your website (or app) visitors and customers i.e. perform data processing on their actions. That is, the fact that they are on your website, how they arrived there - the campaigns and referrals that brought them to your pages, and what content they engaged with.

Such data is used by website operators to understand their online business and users, and is also usually shared with other third-parties - both within and outside the control of the website operator. For example, a Facebook tracker embedded as a Facebook “Like” icon, sends data to Facebook servers for the purpose of other advertisers being able to target ad campaigns to these same visitors as they browse elsewhere on the web. In this case, with the exception of removing the tracker, the third-party (Facebook) is outside of the control of the website operator.

The control of the privacy implications arising from the processing of user data and sharing it around the internet, has led to the development of consent management platforms i.e. banners, to manage user consent. That is, the granting, withdrawing and remembering of the user’s consent decision.

## Why consumers won’t use a brand again



Figure 1 - Image source: SAP/Hybris 2017 Consumer Insights Survey.

Implementing a consent management solution is an important part of protecting your visitors’ information and gaining their trust. Figure 1 shows that 8 out of 10 users will not do business with a brand again if they do not trust it. So its a no-brainer to ask for consent before tracking your visitors, as well as being a legal requirement of the GDPR.

**“This nicely highlights the two critical challenges legitimate businesses want to achieve:  
Be compliant, and achieve a high opt-in rate.”**

**Stéphane Hamel**

Senior analytics consultant and privacy advocate

Whilst gaining consent from your visitors to track is ethically correct, getting it done right is not as straight forward as you may initially think. In a nutshell, you are going to lose data - it's a simple fact that some people do not wish to be tracked and will not opt-in. It's the price you pay in order to gain the trust of your visitors.

## What is a reasonable opt-in rate?

Depending how you implement your consent banner, **the price to be paid can be a disastrous 70% loss of visitor traffic, or it can be a manageable 20-30% loss.**

**“The jigsaw analogy used here encapsulates the problem of online anonymity and why these principles are so important.”**

**Stéphane Hamel**

Senior analytics consultant and privacy advocate

## Privacy, Not Cookies

Consent banners are often incorrectly referred to as “cookie banners” and focus on cookie settings as this has until now been the main method of tracking. However privacy laws such as the GDPR, are intentionally technology agnostic. Contrary to popular belief, even if your website does not set cookies, you still require consent to process anonymous visitor data - see Article 4 of the GDPR.

Essentially in the online world, anonymous data is considered personal data because A) IP addresses are always transmitted, and B) it is all too easy to triangulate a user's anonymous data and identify them as an individual - **the jigsaw effect**. In fact, academic research reports 99.98% of Americans would be correctly re-identified in any “anonymous” dataset using only 15 demographic attributes\*.

In this whitepaper a consent banner refers to the display of a notice to a website or app visitor, in order to ask permission to track their activity in a transparent way that may or may not involve the use of cookies.

\*Source: <https://www.nature.com/articles/s41467-019-10933-3>

See also: <https://www.zdnet.com/article/mozilla-research-browsing-histories-are-unique-enough-to-reliably-identify-users/>

## The Business Impact of Opt-Out

A 70% loss of data represents an opt-in rate of only 30%. Such a data loss will leave the organisation wondering what is the point running a website in the first place...

The significant operational and support costs of running a commercial website depend on the teams responsible knowing what works and what does not. Successful websites rely on deploying new ideas and quickly assessing if they have made an incremental improvement. Depending on the result, the change is either rolled back, edited or appended to. It is the cornerstone of agile product development, and it relies on data.

For example, if your new website design cost \$10,000 or \$100,000 or \$1M - how will you know if it has been successful? How will you know if user friction on your pages has reduced? How will the business know if its investment has improved things, had no effect, or made matters worse? In short, if you cannot measure it you cannot improve it.

Similarly, considerable sums of money are invested in the marketing costs of a website/app - marketing is typically the most significant expense of a company after salaries. An age old complaint from

marketers is: "I know half of my marketing expense is wasted, the problem is I don't know which half".

Accurately knowing conversion rates - what proportion of your marketing spend works versus what is wasted, and how visitors find your website - are key data points that allow organisations to reduce wasting money and ultimately stay afloat. It's how you measure success.

### **Measuring success (or failure) is at the heart of any smart business.**

Being able to track user activity allows the business to provide a better customer experience, improve products, predict stock levels and keep marketing costs down. It creates opportunities and cushions failure. Ultimately, it determines if a business or product survives or dies.

### **Be Smart - Don't Cheat**

**Note, this white paper is not about circumventing your users' consent choices or using dark patterns to deceive them. As shown in Figure 1, consent compliance is important and desirable for gaining consumer trust. Therefore an organisation's website needs to be **transparent** in what it's doing with visitor data, be **nondiscriminatory** (to those that do not consent), and **honour** (verify) the visitor's decision to not be tracked - ignorance is no excuse in law.**

# 04

## The Five Key Principles of Consent

7

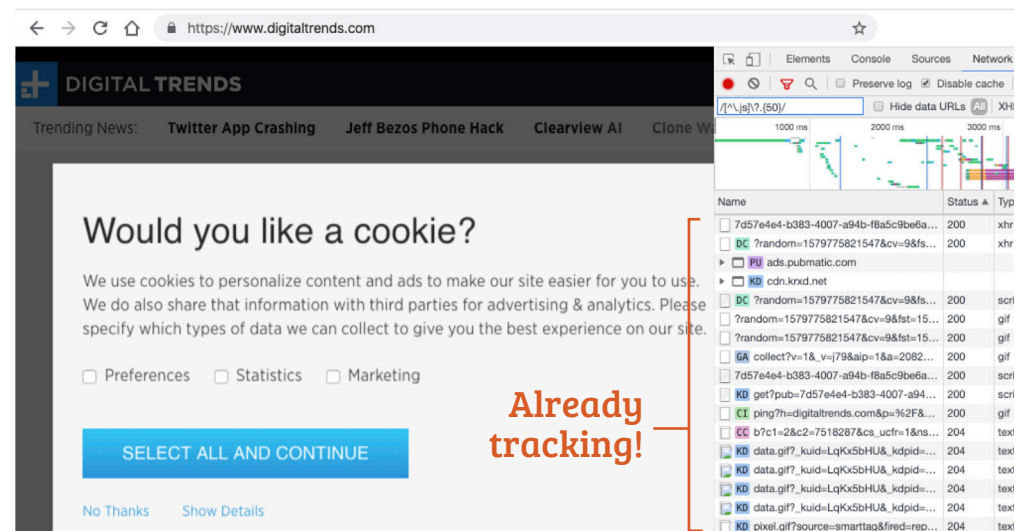
Although GDPR specific, these five principles will stand you in good stead regardless of your geolocation and applicable privacy laws. And because websites/apps constantly evolve, ensure you verify the following on a regular basis:

1. No Tracking Before Consent
2. No Pre-Selected Consent
3. Explicit Consent Only
4. No Cookiewall
5. Honour Explicit No

### 1. No Tracking Before Consent

This sounds obvious - you cannot commence visitor tracking until consent is given. However it is surprisingly common. Research from [Verified-Data.com](#) reveals **70% of enterprise websites with a consent banner, collect data before consent is given.**

Figure 2 is an example of this principle gone wrong. In this case, no decision by the visitor has been made - they are still reading the options available to them. Yet using a simple check of the browser's web developer tools, reveals a whole slew of data harvested by scorecardresearch.com, Google Analytics, DoubleClick ad network, KRXD.net, Pubmatic, and Chartbeat!



**Figure 2** - A website collecting visitor data before any consent is given. The right panel is available by viewing the web developer tools of any modern browser



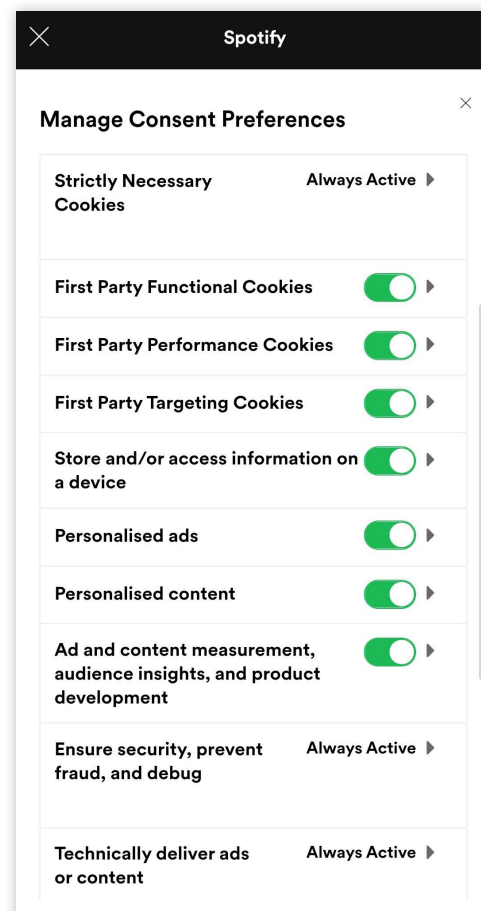
## 2. No Pre-Selected Consent

From an EU/GDPR perspective, tracking can only happen on an opt-in basis. That is, you cannot pre-select or enable options that you wish your visitors to select. Instead, these must be disabled by default, with the user consciously selecting these if they wish to enable them.

The only exception to this are what is often referred to as “Necessary” tracking or necessary cookies - those required for the website/app to function without tracking or profiling capabilities. Figure 3 is an example where this principal has failed - all tracking options are turned on by default.

### Avoid Copying Your Competitors Banners

In the examples shown, I have taken the approach to reveal the brand of the website that fails. This is not to name and shame - as already mentioned 98% of websites get consent wrong. Rather, the purpose is to illustrate that copying the consent approach of other well-known brands, just because they are big organisations, is not a good idea i.e. “if its good enough for big brand X, its good enough for us” is not valid.



**Figure 3** - A non-GDPR compliant consent banner with all tracking options pre-selected.

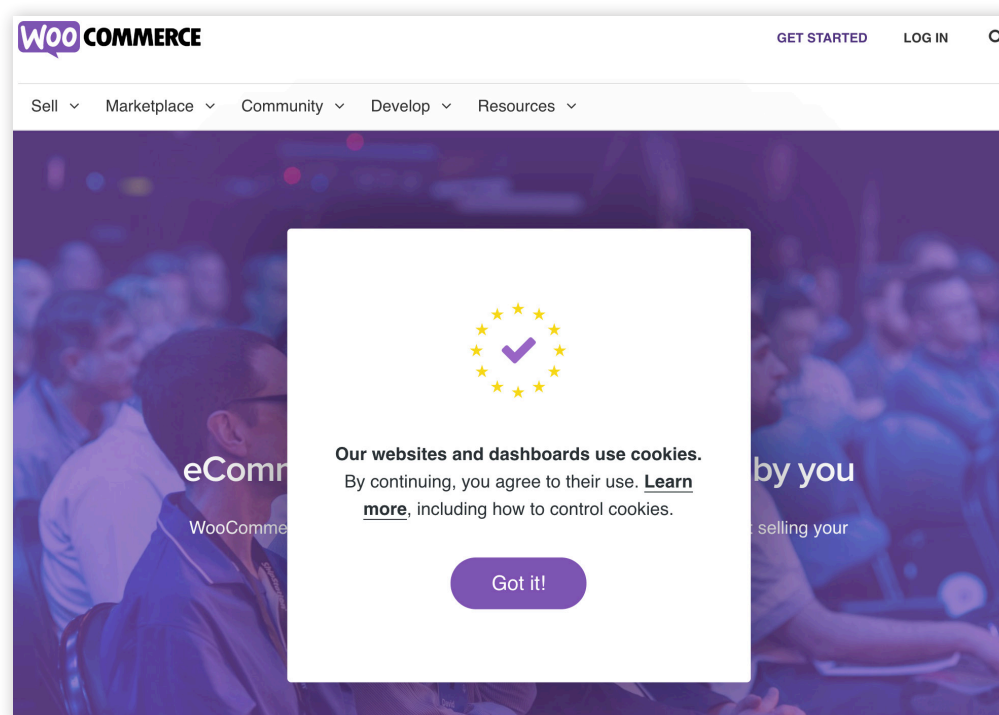


### 3. Explicit Consent Only

From a GDPR perspective, all consent must be informed and explicit. That is, it is transparent to a reasonable user what it is they are consenting to i.e. in plain language, and they must explicitly make their own choice to opt-in. In other words, it is not acceptable to state in your banner wording: *"by continuing to use this site we will track you"*. A classic example of a non-compliant implied consent banner is shown in Figure 4.

### 4. No Cookiewall

Of course all website and app operators want to maximise the opt-in rate for tracking consent. However, it is discriminatory to deny or block access to content until you get your desired consent - a cookiewall approach. The site/app must allow people to access the content even if the user does not give their consent to be tracked.



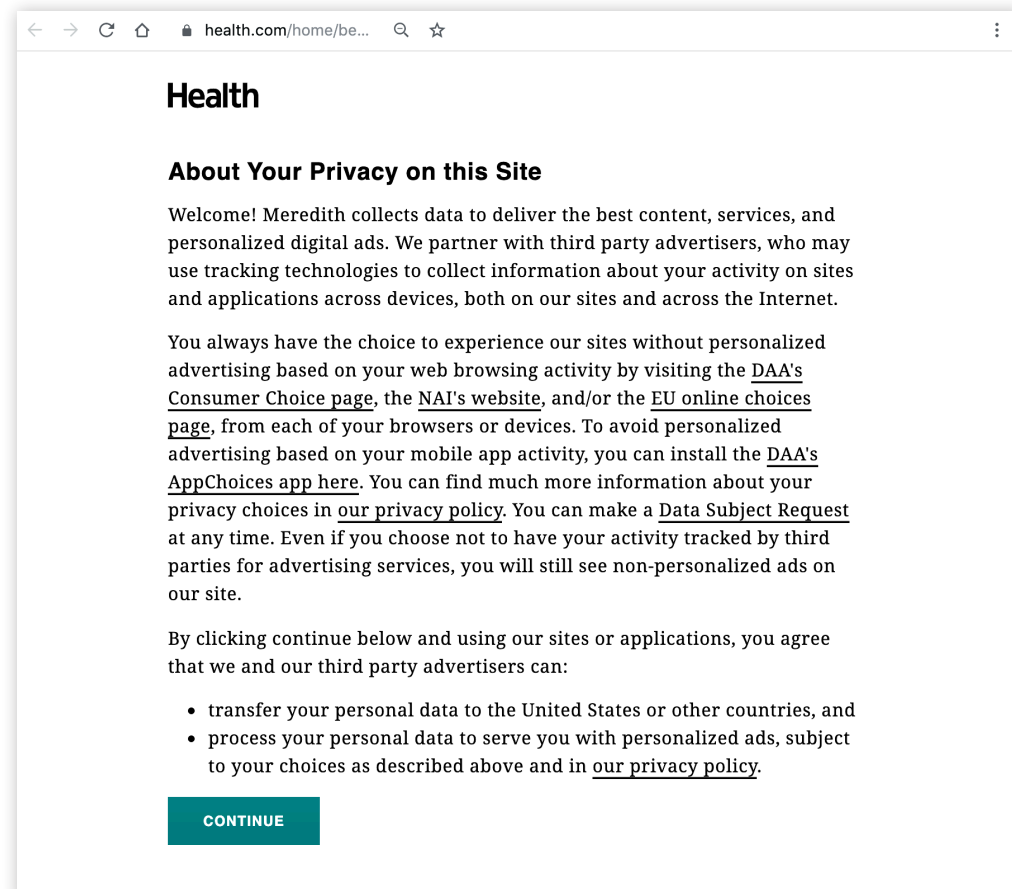
**Figure 4** - A non-GDPR compliant consent banner using implied consent.

Figure 5 is an example banner that completely obscured the health.com website content (the site has since updated its approach). The banner could not be removed, and the content of the site could not be viewed unless consent was given. The only user choice was whether to allow personal data to be used for personalised advertising - an arduous task in itself given the number of different websites that must be visited to opt-out

Despite the discriminatory impact of Figure 5, it is acceptable to block content access until a decision is given. That is, the visitor must make a choice about tracking - either yes or no, before they can view your content.

## 5. Honour Explicit No

If the visitor has chosen not to be tracked, that of course must be honoured for ALL tracking pixels. However, even when consent is explicitly denied, collection of data often still happens. Potentially this is deliberate, though often it is by mistake - or more correctly, by misunderstanding the obligations set out when asking for consent.



**Figure 5** - An example of a non-compliant banner blocking all access to content until the user provides consent. That is, a user that does not consent cannot view the content.

For example, simply having Google Analytics consent compliant is not valid (only blocking Google Analytics tracking). In this context, it is the entire website that must be compliant, not any specific technology. Hence, all tracking tools such as Facebook, LinkedIn, Google Ads etc., must be considered. In essence, **your organisation needs to have a governance process to verify all tracking is disabled if no consent**.

If your organisation controls tracking pixels via a tag management solution, such as Google Tag Manager, you are in a good position. GTM can be

### Trackers Flying Under the Radar

Developer type tools can fly under the radar if not deployed via a centralised tag management platform. Examples to check for include: Amplitude, New Relic, Heap etc. Such tools are known as “product analytics”, as opposed to Google Analytics that is referred to as “web” or “digital analytics”.

configured to fire all tags based on rules (known as “triggers” in GTM) defined by your visitors consent choices.

However GTM can easily be bypassed by developers who can deploy their own tracking pixels directly on to pages. From the development team’s point of view, that can be perfectly valid. However, no matter how tracking pixels are deployed, good data governance is required to ensure all data stakeholders follow the privacy law. Hence, it is important to monitor and verify all potential trackers. Figure 6 is an example page audit showing how tracker pixels can fly below the radar.

Compliance Coverage Table	
~ Hide Table	
To account for platform variations, checks are performed on 10 subdirectories. Failures are shown for any subdirectory that sends hits without consent.	
Subdirectory Tested	Compliant
> <a href="#">www.████████.com/ecatalog</a> ( 14 trackers )	N
> <a href="#">www.████████.com/en</a> ( 3 trackers )	N
bam-cell.nr-data.net/1/60████████	
js-agent.newrelic.com/nr-1208.min.js	
www.████████.com/layouts/system/VisitorIdentification.js	
> <a href="#">www.████████.com</a> ( 4 trackers )	N
> <a href="#">www.████████.com/media</a> ( 3 trackers )	N
> <a href="#">www.████████.com/investors</a> ( 3 trackers )	N
> <a href="#">www.████████.com/about-us</a> ( 3 trackers )	N
> <a href="#">www.████████.com/career</a> ( 3 trackers )	N
0% pages compliant	

**Figure 6** - A page inspection audit verifying what trackers are still sending data when no consent to track has been given. Courtesy of [verified-data.com](#).

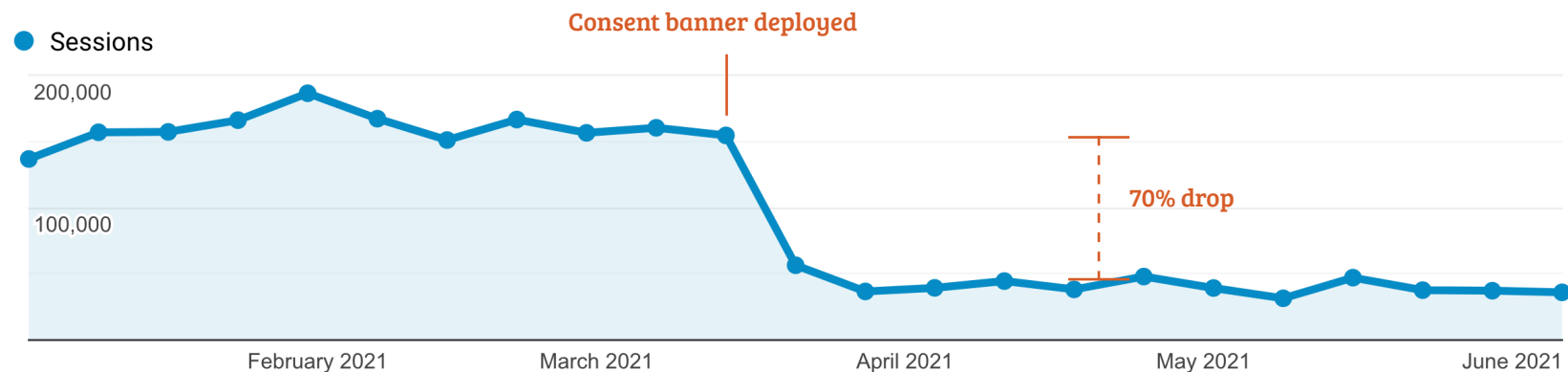
Because being compliant is a legal process, optimising the consent opt-in rate is often simply not considered. Essentially, the legal team finish their work, and once done, data stakeholders dare not mess with it!

Figure 7 is a real-world example taken from the Google Analytics account of a global brand. The opt-in rate is steady at approximately 30%. Such a catastrophic loss has been observed for similar sites using the same consent banner design.

**“All organisations struggle with the opt-in challenge. The truth is, it is entirely legitimate and within the law to optimise this - so long as the nudge is transparent and it’s equally simple for the user to not be nudged.”**

**Axel Tandberg**

Senior advisor and data protection expert at LegalWorks Advisory



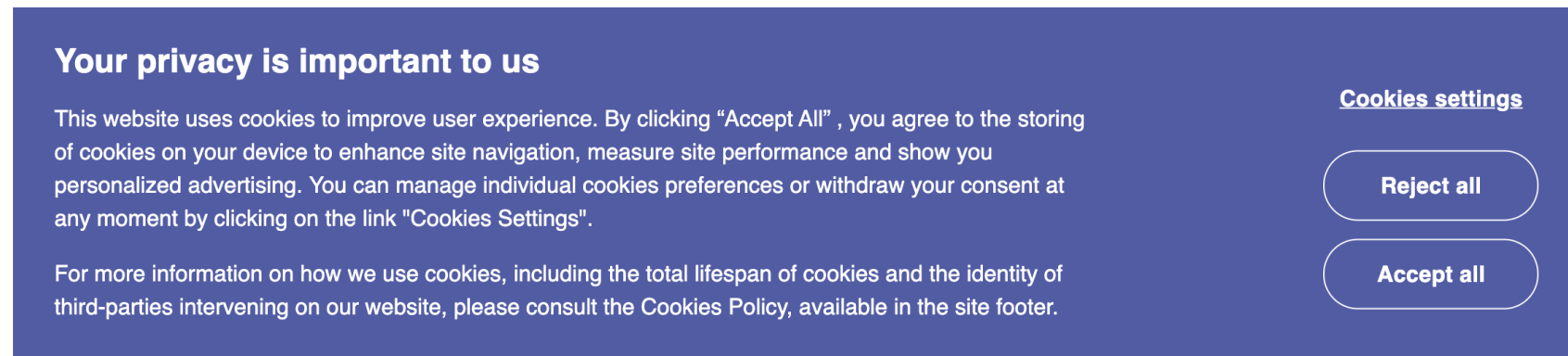
**Figure 7** - The catastrophic data loss for a global brand after implementing their consent banner

## What Is Killing the Opt-in Rate?

Users, even privacy conscious ones, want to click and move on to your content as soon as possible. Any pop-up banner is a distraction and an annoyance to achieving the goal of the visit, regardless of its good intentions. Therefore the user will take the quickest and simplest route to remove the banner. Though note, the desire for a quick result does not mean users do not care about privacy - such an assumption would be dangerous.

The following is a real-world case from a major global healthcare brand. When you visit their website you are presented with the three options shown on the right side of Figure 8.

Put yourself in the shoes of a privacy conscious visitor. **Which option is the strongest candidate for a click?**



**Your privacy is important to us**

This website uses cookies to improve user experience. By clicking “Accept All” , you agree to the storing of cookies on your device to enhance site navigation, measure site performance and show you personalized advertising. You can manage individual cookies preferences or withdraw your consent at any moment by clicking on the link "Cookies Settings".

For more information on how we use cookies, including the total lifespan of cookies and the identity of third-parties intervening on our website, please consult the [Cookies Policy](#), available in the site footer.

[Cookies settings](#)

**Reject all**

**Accept all**

**Figure 8** - A consent banner displaying the three user options typical of a default setup. Which option is the strongest candidate for a click?

### Cookie Settings...?

Visitors who venture into your Cookie Settings expect a long-winded process requiring the reading of cookie descriptions and terms of usage. Even privacy advocates do not wish to figure out how you classify cookies (of course the documentation must be present for transparency).

### Reject All...?

For anyone who has the slightest concern about online privacy, the Reject All button is the strongest candidate for a click. Essentially it is the easiest to do. The only privacy alternative is to click on Cookie Settings that the vast majority of people wish to avoid for the reasons given above.

### Accept All...?

Clicking the Accept All button is a possibility, but unlikely in a privacy conscious world. Even if the emphasis is changed so the Accept All button is bigger, bolder and brighter than the other options, visitors smell what you are attempting to do - manipulate their decision into handing over their data.

If you are an organisation with a very high trust value with your visitors (I cannot think of one, as even the most sincere of organisations have had data breaches and been known to send the occasional spammy email), then of course a visitor may well click on Accept All. Existing customers, where you already have a strong relationship, and staff users are obvious candidates for this click. And perhaps some visitors do not care about privacy. Although some consent clicks come via this button, it will not be the majority.

In addition to the banner options shown Figure 8, some consent banners present the visitor a menagerie of choices - see Figure 9. However, when presented with too many unwanted choices (remember interruption banners are always unwanted from a visitor's point of view), a privacy conscious visitor will still attempt to take the path of least resistance i.e. minimise their data exposure. In this case, the black button "Use necessary cookies only" stands out and results in no tracking.

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services

**Use necessary cookies only** **Allow selection** **Allow all cookies**

☒ Necessary ☐ Preferences ☐ Statistics ☐ Marketing Show details ▼

**Figure 9** - A menagerie of options for the user is rarely a good idea on interruption banners.

# 06

## Optimising Your Opt-in Rate

15

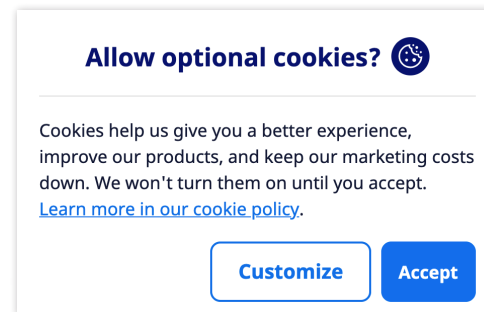
The purpose of optimisation is to apply standard user experience principles to improve your consent opt-in rate. This is not about tracking by stealth, rather doing the right thing in an optimised way. In this case the fix is very straightforward - move the Reject All option.

Figure 10 is a transparent example of the alternative two-click approach to reject all.\*

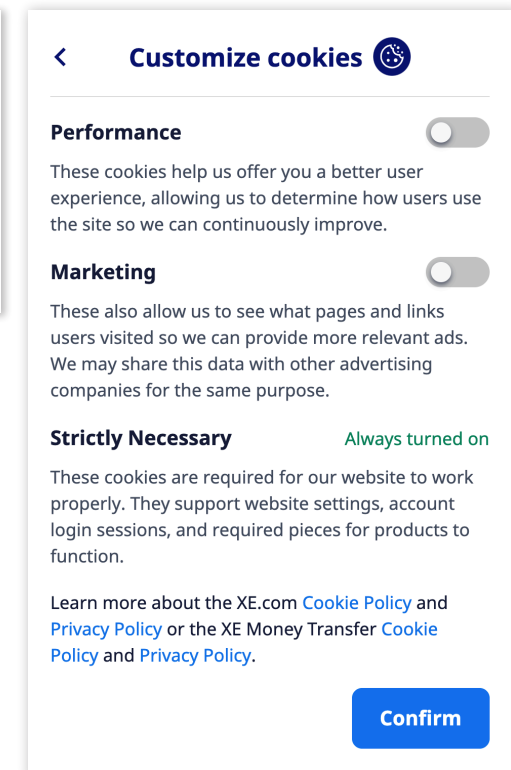
Essentially, having Reject All on the first screen is not required to be compliant - as long as the reject option is available which is equally as clear and easy to select. In this realworld example from xe.com, it is simply one click away.

The user is either comfortable with being tracked - in which case they click on Accept (all) of Figure 10A, or if there are any doubts about privacy, they can click on Customise where confirming the default i.e. no tracking selected, is the equivalent of reject all (Figure 10B).

\*A caveat of the real-world example of Figure 10, is the over focus on technology i.e. cookies. For GDPR, consent is required for the processing of visitor data, regardless of the technology used.



**Figure 10a** - An example of a concise cookie banner without a Reject All button. To reject, the user clicks Customize - see Figure 10B.



**Figure 10b** - Confirming the default unselected options is the equivalent of a Reject All option.



At first glance, the difference of moving the Reject All option appears trivial. But it has a dramatic affect on the opt-in rate. Now the privacy conscious visitor requires two clicks to remove the banner when previously it was just one. This subtle difference makes the visitor think just a little longer about how much they value their privacy with respect to your brand.

And that's the point. As a data manager, you want the user to think just a little more about a decision that will make your job a lot harder.

**When the Reject All option becomes two clicks instead of one, and with all other consent compliance obligations met, the data loss it typically only 20-30%.**

**“Whether to opt-in or not needs to be simple and transparent, and it is entirely valid from a legal perspective for an organisation to not make these choices identical.”**

**Axel Tandberg**

Senior advisor and data protection expert at LegalWorks Advisory

## The Optimising Myth

There are numerous privacy advocates saying consent banners cannot be optimised for improved opt-in rates. That they are set in stone and it just the luck of the draw what opt-in rate you get. This stems from the wording of Article 7 (3) of the GDPR: “It shall be as easy to withdraw as to give consent.”

However, as the UK's data protection authority points out in its guidance document\*:

*“..the UK GDPR is clear that the right to the protection of personal data: is not absolute; should be considered in relation to its function in society; and must be balanced against other fundamental rights, including freedom of expression and the freedom to **conduct a business**.”  
(emphasis mine).*

Optimising your consent banner for opt-ins, also referred to as “nudging”, is simply a part of being smart at conducting business. Legitimate nudging has always existed.

Note, that a nudge is just that - this document is not about tracking visitors by stealth. It is about legitimately and transparently wanting to maximise the opt-in rates of consent.

\*See page 30 of: <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf>

Privacy compliance with respect to gaining consent from your website visitors requires a good understanding of your organisation's obligations in addition to how these will impact on user experience and the quality of the resulting data i.e. the expected data loss due to low opt-in rates.

Often the people making decisions about compliance are far removed in the organisation from the data teams that are impacted. They may even be outside the organisation. **This compliance-gap results in a key dilemma for data teams: Who is responsible for optimising opt-in rates?** Often there is no answer, or the reply is: "We can't".

However, there is no set way, or law, for designing a consent banner. Granted, following the five key principles for consent means there is little scope for user experience testing. Nonetheless, what small scope is available can have a dramatic impact on the results.

The simple solution presented here of moving the Reject All option so that it is two clicks instead of one, has been shown to reverse the data loss from a disastrous 70% to a manageable 20-30% loss.

An important part of the approach is putting the visitor first when considering the privacy obligation of the organisation. Although this approach sounds obvious, legal and compliance teams are often too far removed from the website/app user experience to take this into account. Hopefully this document will help you bridge this compliance-gap.



**Brian Clifton PhD** is recognised internationally as a Google Analytics expert and best-selling author who has helped shape the industry over the past two decades. His books are used by students and professionals worldwide.

As Google's first Head of Web Analytics for Europe, Brian built the pan-European team of product specialists, a legacy of which is the online learning test, known as the GAIQ.

Brian has guest lectured at University College London, Copenhagen University, and the Stockholm School of Economics.

Brian is Director of Analytics Data Quality & Compliance at Search Integration, Sweden. [BrianClifton.com](http://BrianClifton.com)



**Verified Data** is an automated Google Analytics auditing tool. It combines a data inspector with a page inspector to uniquely provide a complete picture of a website's data quality and data governance. [Verified-Data.com](http://Verified-Data.com)



**Axel Tandberg** is a Senior Advisor and data protection expert at LegalWorks Advisory - a modern

legal services company based in the Nordics. As a qualified lawyer of over 20 years, Axel specialises in legal advice for business data protection in a digital world. [LegalWorks.se](http://LegalWorks.se)

Axel reviewed and assessed this whitepaper from a European privacy point of view, and states: **"The consent approach outlined in this whitepaper is consistent with GDPR law."**



**Stéphane Hamel** is a seasoned independent digital marketing and analytics consultant, innovator, keynote speaker and privacy advocate. He is also Digital Marketing Academic Advisor for the Faculty of Business Administration at Laval University. [StephaneHamel.net](http://StephaneHamel.net)

# Get in touch

---

For enquiries about this whitepaper, please contact:

**Brian Clifton**

**e** [brian@advanced-web-metrics.com](mailto:brian@advanced-web-metrics.com)

**w** [brianclifton.com](http://brianclifton.com)