iubenda

iubenda.com

The future of cookie consent in Europe: what marketers should prepare for

A practical guide to cookie consent in Europe: how to build a marketing strategy that drives growth as Europe's digital rules evolve.

Certified CMP Partner

At a glance

Why should marketers care about cookie consent?

Because it directly affects their marketing performance. Every time a visitor declines cookies or dismisses your banner, that's a data point you lose, a conversion you can't attribute, and a visitor you can't retarget.

Your consent setup isn't a legal formality but should be seen as part of your marketing infrastructure. And how well it works shapes the quality and volume of data you can use.

Why is Europe rethinking how cookie consent works?

The current system creates friction on both sides. Users see banners on every site, rarely read them, and click through out of fatigue. Businesses face mounting complexity in keeping their setups aligned with regulatory requirements.

The EU has acknowledged the problem and is looking at ways to simplify, without weakening privacy protections. The direction is toward fewer, clearer consent interactions. Consent for advertising and tracking stays opt-in. The mechanism is evolving, not the principle.

Has anything actually changed yet?

No. As of the beginning of 2026, the EU has only published a proposal, not a law. The current GDPR and ePrivacy rules still apply. You don't need to change your setup today. But the trajectory is clear, and teams that prepare now will be in the strongest position when things do shift.

What should marketers focus on for 2026 and beyond?

- Treat your consent setup as marketing infrastructure, not a legal checkbox. Look at privacy practices as instrumental to brand trust and customer retention.
- Use privacy-aware approaches enabled by your Consent Management Platform (CMP): Google Consent Mode recovers more than 70% of ad-click-to-conversion journeys lost to cookie refusals. Integration with IAB's Transparency and Consent Framework (TCF) remains essential for advertisers.
- Build your first-party data strategy: consented data from your own audience is becoming the most reliable source of data for personalization.
- Track your consent rate as a performance metric and test your banner to optimize for opt-ins.

What's a consent rate and why does it matter?

It's the percentage of your visitors who actively accept cookies (opt in). Think of it as the entry point for all your marketing data: the more users consent, the more data your analytics and ad platforms have to work with. More data means better targeting, sharper attribution, and stronger results. Consent rate is a growth metric. Treat it like one.

In this guide

Going back to basics: how cookie consent works today

Before we look at what's changing, let's make sure we're on the same page about what cookies are, why consent matters, and how the system works today. Whether you're new to this or need a refresher, this section covers the foundations that everything else in this guide builds on.

What are cookies?

Cookies are small text files that websites store on your device when you visit them. They remember things like your login details, language preferences, and shopping cart contents. Some cookies are set directly by the site you're on. Others come from external services embedded on the page, such as an ad network, a social media plugin, or an analytics provider.

This distinction matters because EU privacy law treats them differently.

First-party cookies	Third-party cookies
Set by the website you're visiting	Set by external services (ad networks, social media platforms, analytics providers)
Help with core functionality: logins, preferences, cart items	Enable advertising, cross-site tracking, retargeting, and social media features
Generally lower privacy risk	Most require consent under EU law

In marketing, **third-party cookies** are the ones that power most of your day-to-day tools: retargeting pixels, conversion tracking, audience segmentation, and personalized advertising. They're also the ones most affected by consent requirements.

Why is consent required to install cookies?

Think of cookies as sticky notes a website leaves on your device. Some of those notes are useful, like remembering you're logged in. But others track where you go online, what you buy, what you search, and who you are.

The law says websites have to ask your permission before doing that, **because visitors should have control over their data and the right to say no to having their data collected and used.**

Existing rules around cookie consent

Two EU laws work together to protect users' data when it comes to cookies:

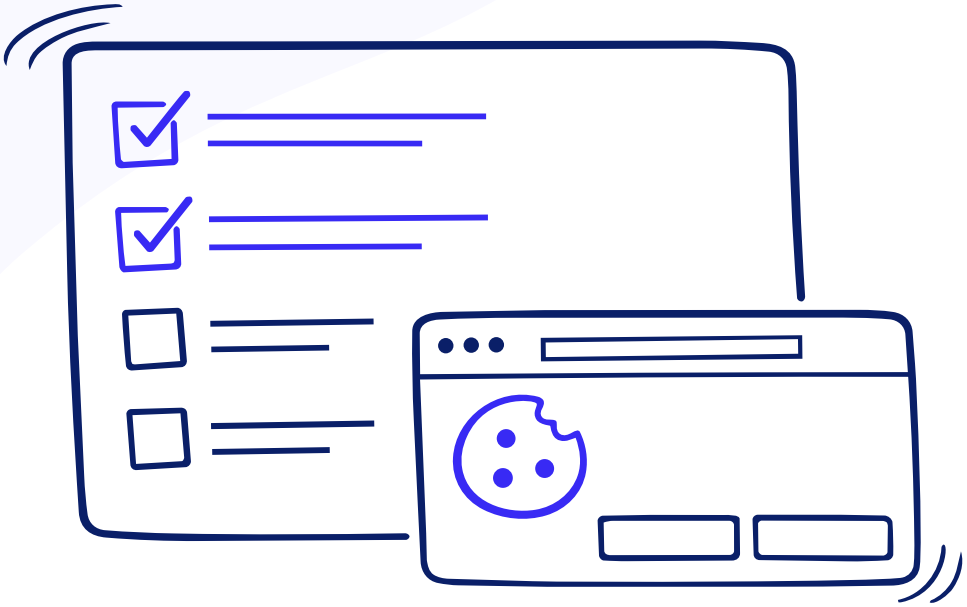
- **The EU ePrivacy Directive** (often called the "Cookie Law") requires websites to inform users and get consent before storing or accessing information on their devices.
- **The General Data Protection Regulation (GDPR)** sets strict rules for processing personal data, including data collected through cookies.

Together, they establish a clear principle: before any non-essential cookie runs on a user's device, you need their informed, explicit consent.

The only exceptions?

- Strictly necessary cookies: the ones required for basic site functionality (like keeping a user logged in) or for transmitting a communication.
- In some EU Member States, certain analytics cookies may be exempt from consent when strict conditions are met (e.g., limited scope, anonymization, no cross-site tracking).

Everything else **needs a "yes" first**.



So what does "informed, explicit consent" actually look like in practice?

Here are the **main requirements in Europe**. If your website targets EU-based users and uses non-essential cookies, all of these likely apply to you:

Block cookies before consent

Non-essential cookie scripts can't run until the user actively opts in. No pre-checked boxes, no implied consent.

Make consent informed

Tell users what cookies you use, what they do, and who the third parties are. Link to each third party's privacy policy.

Offer a real choice

The option to reject must be as visible and easy to use as the option to accept.

Allow granular preferences

Users should be able to choose which categories of cookies they accept (e.g. analytics yes, advertising no).

Enable withdrawal at any time

Users must be able to go back and change or revoke their consent, typically through a privacy widget.

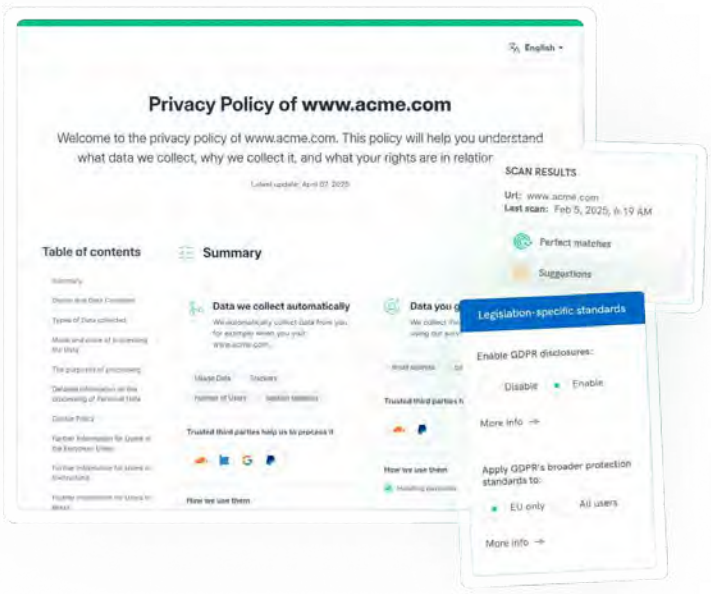
Store proof of consent

Record when and how each user gave consent, so you can **show you met your obligations** if needed.

If you use third-party cookies, both you and the third party are responsible for informing users properly. This is usually done with a **privacy and cookie policy document**.

Your cookie policy should list each service by name and explain its purpose. This level of transparency isn't optional: it's a core part of meeting European requirements.

Drafting and keeping a legal document like this can be tedious.

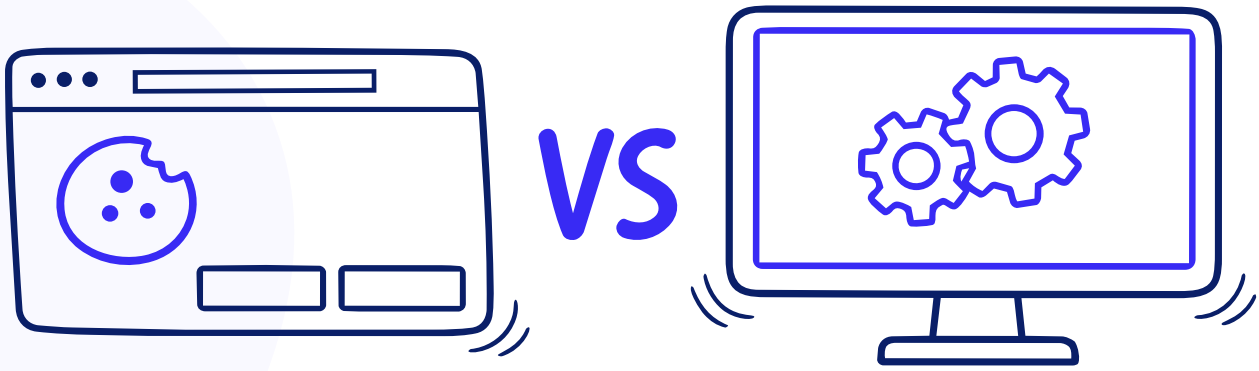


Check out our privacy and cookie policy generator

The roles of cookie banners and CMPs

When people hear "cookie consent," they usually think of the banner that pops up when they visit a site. **But the banner is just one piece of a larger system**. Behind it, there's usually a Consent Management Platform (CMP) doing the technical enforcement work.

These two work together, but they do different things:



Cookie banner

The banner is what your visitors see. It's the notice that appears on their first visit, informing them about cookies and giving them the option to accept, reject, or customize their preferences. Think of it as the front door of your consent setup.

Consent management platform (CMP)

The CMP is the system behind the banner. It handles the technical and legal work:

- **Collects and stores consent preferences**
- **Blocks or unblocks cookie scripts based on user choices**
- **Keeps proof of consent for your records**
- **Connects with your ad platforms, analytics tools, and marketing stack**
- **Supports frameworks like the IAB Transparency and Consent Framework (TCF) and Google Consent Mode**

The banner asks the question. The CMP enforces the answer.

Without a proper system, your banner is just a pop-up with no follow-through. Scripts would still fire regardless of what the user chose, and that is not compliant.

Why cookie consent matters for marketing growth

"Before joining iubenda, I used to assume cookies and privacy were not a marketing topic. Legal set the rules, and marketing worked around the constraints. I was wrong. If you're a marketer and you can't speak to how you're collecting and using data, that's a gap worth closing."

Andreea Mandeal,
CMO at iubenda

Cookie consent directly affects your marketing performance.

Every time a user declines cookies or ignores your banner, that's an **opportunity for collecting data that you lose, a conversion you can't attribute, and a visitor you can't retarget**. When you multiply that across your entire audience, the impact adds up fast.

Here's where it hits your marketing performance hardest:

Data quality

When users don't consent, you lose visibility into their interactions. Your analytics show an incomplete picture, and bidding algorithms work with partial information.

Attribution and conversion tracking

Without consent, you can't track conversions, retarget visitors, or personalize ads for those users. Your attribution models become less reliable, making it harder to understand what's actually driving results.

Campaign optimization

Ad platforms rely on conversion data to optimize delivery. Less data means less accurate optimization, higher costs per acquisition, and lower return on ad spend.

Brand trust

How you handle consent shapes how users perceive your brand. A confusing or aggressive banner erodes trust. A clear, respectful one reinforces it. According to the **Cisco 2024 Consumer Privacy Survey**, 75% of consumers say they won't buy from companies they don't trust with their data, so the stakes go beyond just measurement.

The end of an era?
Cookie consent is at a turning point

Cookie consent in Europe has worked the same way for years: show a banner, ask for permission, block cookies until the user says yes. The system was built to protect people's privacy, but it also created a fair share of **friction**, prompting the European Union to try to improve the situation.

Why is change needed?

The current consent model puts pressure on both sides of the screen. Users are overwhelmed by banners. Businesses are weighed down by complexity. Neither side is getting the best outcome.

On the user side

Users are more privacy-conscious than ever, and are concerned about their data... According to **Eurostat's 2025 data**, 76.9% of EU internet users actively took steps to protect their personal data online, up from 73.2% in 2023. People care about their privacy and increasingly act to protect it.

...but consent fatigue is real. This is how it goes for most of us. We see cookie banners on nearly every site. We don't read them and just click "Accept" to make them go away, or reject everything out of frustration. Either way, the consent isn't truly informed, and constant re-prompting is tiring.

Poor banner UX makes things worse. Some websites are just difficult to reach because of a slow or intrusive banner. Users would rather leave the page. Many still use manipulative design: accept buttons that are bigger or brighter, reject options that aren't available, pre-ticked boxes that assume consent.

On the business side

Legal and technical complexity is a drain. Legal requirements are many. They can vary from country to country or by legislation.

Keeping up takes real work. Compliance isn't a one-time setup. Obligations keep changing as new regulations come into force. Companies have to handle constant updates, adapt their setups, and face costs that compound. For smaller teams, the burden can feel disproportionate.

Negative impact on revenue and higher risk. The combination of poor consent flows, incomplete data, and rising compliance costs creates a drag on performance. And if your consent setup doesn't meet the requirements, there's regulatory risk on top.

The cookie consent system in Europe, originally designed to give users control, often leaves them disengaged.

In its **Explanatory Memorandum**, the European Commission itself has acknowledged that "a regulatory solution on the consent fatigue and proliferation of cookie banners is long-overdue."

The EU's response

Introducing the Digital Omnibus proposal

In November 2025, **the European Commission published its Digital Omnibus Regulation proposal**.

It's part of a broader package to **simplify and modernize EU digital rules without weakening the fundamental privacy rights** that European law has built over the past two decades.

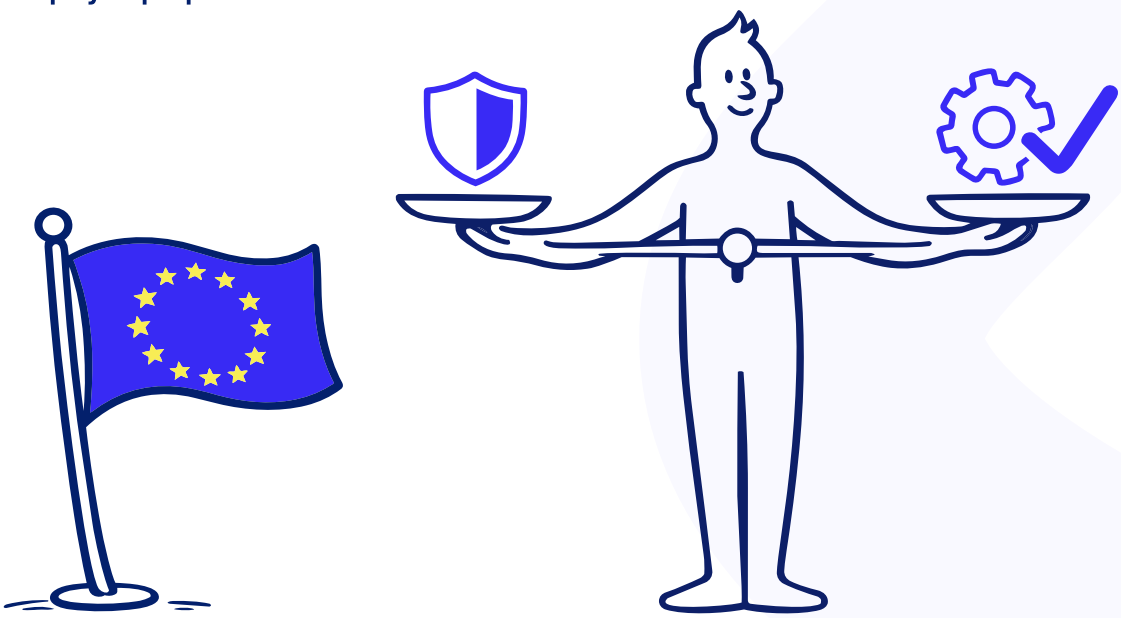
With this, the EU declares its desire to tackle the challenges we've seen previously and find a balance that reduces friction for users and lowers complexity and costs for businesses.

When it comes to cookie consent, among other things, the proposal would:

- Simplify the interaction between ePrivacy rules and the GDPR.
- Lower consent fatigue and how often users are prompted with the same consent request.
- Clarify which limited purposes (like first-party aggregated audience measurement) can operate without consent.

It's important to say this upfront: **this is a proposal, not a final law**. The text may change substantially as it moves through various approvals from European Parliament and Council before adoption. Many **important stakeholders like the European Data Protection Board (EDPB) have already issued opinions** and recommendations.

The rollout will be phased and could take up to 48 months after entry into force. Until then, the current GDPR and ePrivacy rules apply. **You don't need to change anything right now. But understanding where things are headed helps you prepare.**



In a nutshell:
what does the Digital Omnibus mean for marketing professionals?

What's new

Clearer banner UX rules
The proposal requires a single-click reject option that's as visible and easy to use as the accept button. No dark patterns. If a user refuses consent, you can't re-prompt them for the same purpose for at least six months.

More clarity on first-party analytics.
Aggregated audience measurement using first-party data only, without sharing, selling, or repurposing the data, could operate without consent under specific conditions.

Central consent signals (e.g., at the browser or OS level).
Users could set privacy preferences once and have those preferences communicated automatically to every site they visit. Websites would need to be able to read, respect these signals, and enforce whether tracking can run or not.

What stays

Opt-in for ads and tracking.
Consent remains the rule for advertising, profiling, cross-site tracking, and most third-party analytics. The core opt-in model doesn't change.

In practice: you'll likely show fewer banners to the same user over time, but **you'll still need a solid consent infrastructure behind the scenes.**

The banner is just the front end. What matters is how your system handles signals, enforces rules, and connects consent to your analytics, ads, and customer platforms.

The proposal includes a specific exception for media service providers. Those whose revenue relies primarily on advertising are explicitly exempt from the obligation to respect machine-readable preference signals. Learn more **here**.

This signals something broader: the EU's position is pragmatic, not rigid. The goal is to simplify, not to shut down entire business models. That's a good indicator for how the final text might balance privacy protection with commercial reality.

What our experts think about the future of cookie consent

> “Consent is no longer just a compliance step, it is the legal gateway to how data can be collected and used. As regulatory frameworks continue to require valid, enforceable user choice, access to data increasingly depends on consent itself. In that context, the ability to capture, interpret, and operationalize consent signals is becoming a determining factor in both compliance and marketing performance.”

Giulia Stancampiano,
Head of Legal (Privacy & Tech) at iubenda

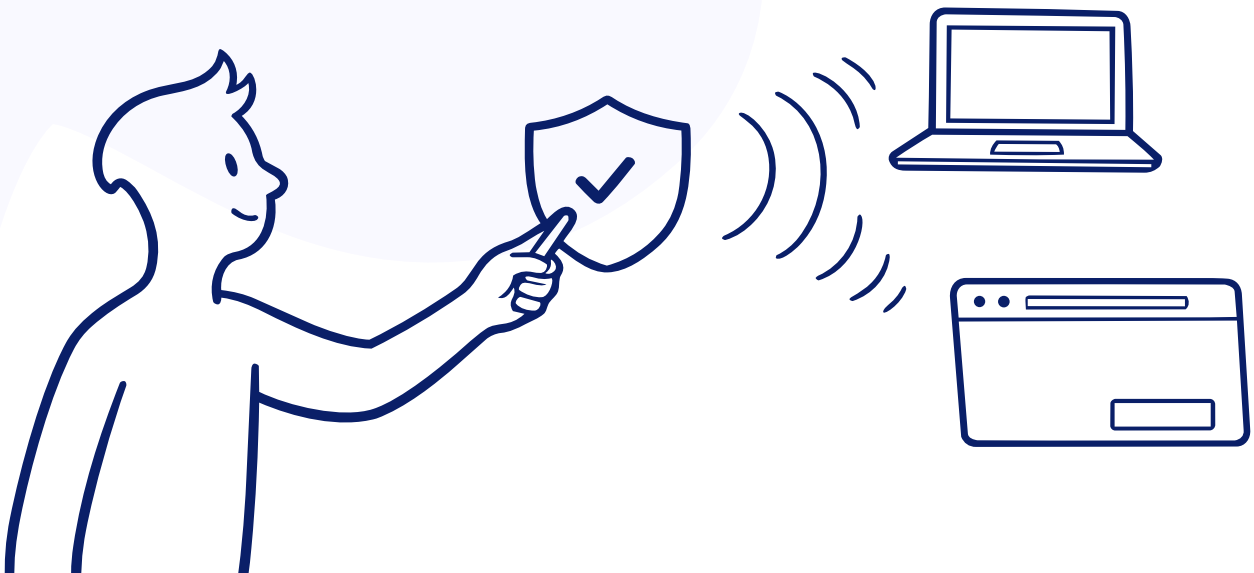
A shift in mechanism, not in requirement

Consent isn't going away. What's changing is how it's expressed, remembered, and enforced across systems.

With browser- or device-level preference signals on the horizon, users could set their privacy choices once and have them applied across sites, rather than responding to the same banner on every visit. **This doesn't change whether consent is required. It changes the mechanism.**

For this to work in practice, a few things need to hold:

- Signals need to work with existing standards (interoperability).
- Signals need to trigger real technical behavior across websites and services.
- The model shouldn't concentrate control in a small number of platforms.



In practice: more connected systems

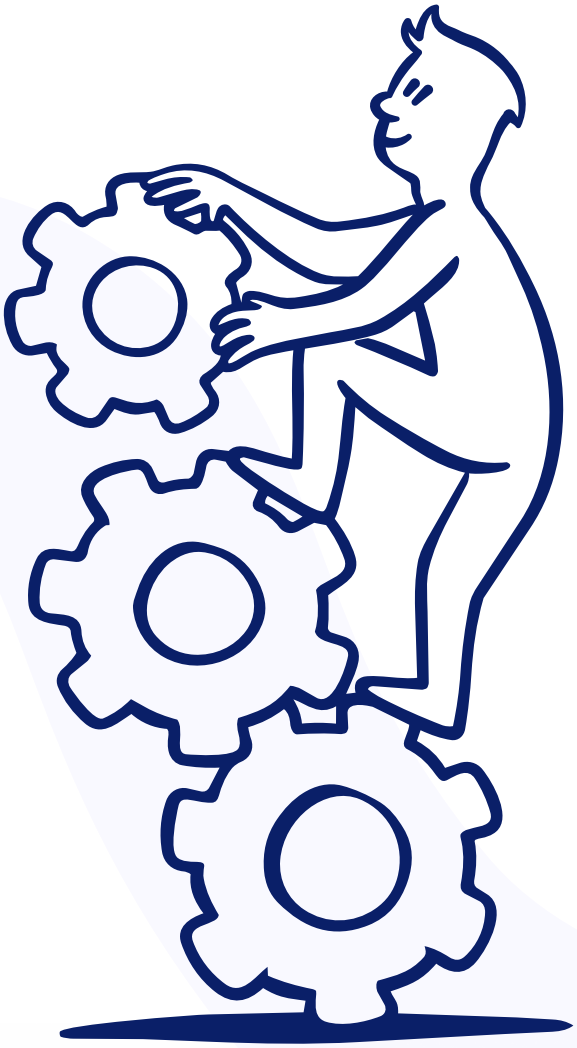
Over time, users may see fewer repetitive consent prompts. But behind the scenes, the job doesn't get smaller. Consent infrastructure will work in a broader, interoperable framework. This means the implementation becomes more complex with:

- Different sources of consent signals (banners, browsers, apps)
- Multiple downstream systems (analytics, advertising, data platforms)
- Ongoing requirements for proof, enforcement, and user control

Your Consent Management Platform is not just an interface for collecting consent. It will play a central role in this. As new signal sources emerge, that role becomes more important, not less.

Browser-level signals don't replace your CMP. They give it another input to work with. It still has to translate user preferences into real, enforceable technical behavior across the entire digital stack, from websites and apps to analytics or advertising services.

In short, the future of cookie consent is about making consent mechanisms more connected, interoperable, and frictionless.



Disclaimer: This e-book discusses a legislative proposal, not final law. The content reflects iubenda's interpretation as of May 2026 and should not be relied upon as legal advice. Consult your own legal counsel for guidance specific to your business.

What will differentiate winning marketers in 2026 and beyond

The marketing teams that come out ahead are building on a foundation that holds up regardless of what the law says next. Compliance is the baseline, and what separates growth-oriented marketers is how they turn it into a competitive advantage.

This section covers four areas where the way you handle privacy, data, and consent can directly improve your marketing performance.

01 Rethink compliance as trust built in

What it means

Most marketing teams treat privacy compliance and cookie consent as a separate track: legal sets the rules, product builds the banner, and marketing works around the constraints. That approach has a cost.

In reality, **your consent banner, your privacy policy, and the way your data flows work must be well-curated by marketers as they represent trust moments for your visitors** that impact overall customer acquisition and **retention**.

When banners don't enforce your visitors' preferences, policies are years out of date, or consent flows frustrate users rather than reassure them, the legal risk is real. The trust cost is just as real.

Ipsos stated that more than two-thirds (68%) of those surveyed said they felt skeptical about the way companies used their data in marketing. Only 3% of respondents believe they have complete control of the disclosure and removal of their data online.

Why it works

Marketing teams that give compliance the right importance early move faster later. No surprises mid-campaign, no analytics teardown when your tracking setup turns out to be non-compliant.

As **Adam Taylor, UK Privacy Lead at Google Marketing Platform (GMP), put it for The Drum:**

> "Privacy is no longer a specialist subject in marketing, it's a core competency. That comes through in a number of ways – the way you hire, train, and upskill yourself and your team, the decisions you make on technology and partners, and how you communicate effectively across disciplines and functions."

Treating compliance as infrastructure and a trust enabler means key touchpoints are designed correctly from the start, not patched after users have already formed an impression.

It works because that's what visitors want to see. **A consumer study on data privacy and security from Deloitte** has found that

> "the vast majority of respondents want more protection and control over how their data is used. Almost 9 in 10 agree they should be able to view and delete the data that companies collect about them."

What you can do now

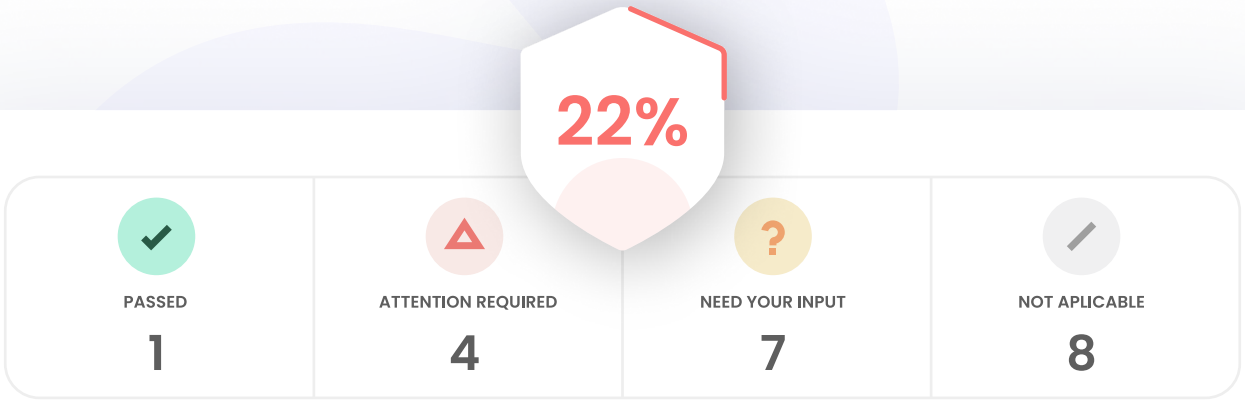
- **Put yourself in your visitor's shoes.** Walk through your consent experience as a first-time user. Where does it feel unclear, intrusive, or hard to navigate? Those are the moments where trust breaks down before it's ever built.
- **Audit your current setup.** Map every tool that sets cookies or processes personal data. Identify gaps between what your banner or privacy policy says and what's actually running.
- **Bring compliance into your marketing kickoffs.** Before launching a new campaign, adding a tool, or entering a new market, run a quick compliance check.

> “Many marketers see compliance as a constraint, but we see it as an opportunity to strengthen trust with customers. Transparent consent and responsible data practices lead to better relationships and ultimately better performance. That’s why we’re making it a priority across team.blue and our 60+ brands."

Shelby Torrence,
Group Marketing Director at team.blue

Check your compliance in seconds

Run a quick free scan to see if your site meets privacy, cookie, and accessibility requirements.



Insert your URL and get a compliance report

02 Use privacy-aware measurement

What it means

Privacy-aware measurement means building a privacy-friendly approach to marketing performance that works accurately with the data you have, and models intelligently for the data you don't.

It prioritizes user privacy and data security over invasive, individual-level tracking. Here are two impactful privacy-aware measurement strategies you must consider:

- **Google Consent Mode.** When a user declines consent, **Consent Mode** sends limited, cookieless signals that allow Google to **model conversions** in an aggregated way to help measurement continuity. Signals are received by Google's systems like Google Analytics, which use AI modeling to **estimate conversions from unconsented users based on patterns from consenting users**.

- **Server-side tracking.** Server-side tracking is emerging as the most reliable measurement alternative for e-commerce and marketing teams. Instead of embedding tracking in the user's browser, server-side tracking captures events directly on the server and assigns a server-generated ID to each action before forwarding signals to analytics and ad platforms.

Neither server-side tracking nor Google Consent Mode replaces the obligation to obtain valid user consent. Both should be used in conjunction with, not as a substitute for**, your Consent Management Platform (CMP)** that collects and stores users' choices.

E.g., Google Consent Mode is a mechanism that adjusts how Google Analytics and advertising tags behave based on users' consent choices and communicates those choices to Google services. Your CMP ensures tags respect user preferences. See how this works:

Why it works

Consent Mode is now non-negotiable for EEA and UK traffic. From July 2025, Google began actively disabling advertising features for accounts that didn't activate it.

Conversion modeling through Consent Mode recovers more than 70% of ad-click-to-conversion journeys lost to cookie refusals. For you, that recovery translates directly into more accurate bidding, better campaign optimization, and a clearer picture of what's actually driving results.

"Ad tech and privacy used to feel like they were pulling in opposite directions. Then we implemented Google Consent Mode for our clients. When users declined cookies, Google modeled the conversions we'd lost, our bidding algorithms had more to work with, and our campaigns performed better. Privacy compliance and ad performance aren't opposites. Once you understand the tools, you can make them work together."

Virginie Rivet,
Senior GTM & Marketing Strategy Consultant at Cremanski & Company

What you can do now

- **Implement Google Consent Mode if you haven't already (check if it's active on your site).** This is the single most impactful measurement step you can take right now. Your CMP should handle valid consent collection and the technical integration. After carefully checking with your legal team, you may consider using more performing features like Advanced Consent Mode (sends cookieless pings before consent is granted) or Enhanced Conversions (sends first-party data to Google for better attribution).

- **Explore server-side tracking.** EU privacy regulations keep evolving, and browser-based tracking may face more and more restrictions. Find out more about it and see if it could fit your needs for more reliable measurement.

- **Check your IAB TCF integration.** If you run programmatic advertising, a misconfigured TCF setup means consent signals aren't reaching your ad tech stack. Users who said no might still be tracked.

03 Use first-party data

What it means

For marketers, rethinking how they use first-party data is a smart move. First-party data has become the most dependable source for driving cross-channel performance and staying close to your customers.

First-party data is the information you collect directly from the people who interact with your business, like signups, purchases, preferences, and on-site behavior.

Why it works

It starts with transparency. When customers understand how their data is used and stay in control of it, the data you collect becomes more accurate, more reliable, and more valuable.

1

Transparency at every touchpoint

Your cookie policy, preference center, and opt-out flow aren't just legal requirements. They're the first signal you send to customers that you respect their privacy. Make them clear, accessible, and easy to act on.

2

Customers opt in willingly

When people understand what they're agreeing to and trust that you'll honor their choices, they share their data willingly because they stay in control of their own information. That consent is what makes first-party data so powerful.

3

You get more accurate consented data

Data collected under clear consent reflects genuine interest. It's more reliable than anything collected through third-party tracking, and it holds up as privacy regulations evolve.

4

Your marketing gets smarter

Learn what your audience actually cares about or who's genuinely interested. Cut wasted spending on what's not working and sharpen your focus for better targeting.

5

You deliver more relevant experiences

Give customers what they actually want. When you understand your audience on their own terms, you can personalize at every stage of the journey and build stronger relationships.

6

Improved marketing performance and revenue

Customers who opt in, feel respected and in control of their information, and who get relevant experiences are more likely to buy and stay. On your side, better data means less wasted budget, higher conversion and retention rates, and stronger long-term customer value.

The result is a loop that benefits everyone. Trust builds on both sides: your marketing data, and your customers. First-party data is a growth strategy.

According to **a 2023 Deloitte industry report on first-party data commissioned by Meta:**

> “**82% of marketing leaders** are prioritizing first-party data to create immediate value for customers" with an emphasis on transparency. Leading brands are informing customers how their data will be used to support key tasks.
>
> It also states that businesses that invest in tailored, data-driven experiences based on first-party data saw:
>
> - **27% increase** in conversion rate
> - **23% increase** in customer satisfaction
>
> Deloitte Digital for Meta

"Privacy compliance is often treated as a legal obligation and nothing more. We see it differently. It's a commitment to our audience: give people a genuine choice over their data, respect it, and the benefits follow."

Diana Dee Rabba,
VP of Marketing at Accessiway

What you can do now

- **Identify the data points that actually drive decisions.** Focus on signals that connect to your goals: email signups, purchase history, product preferences. Collect less, make it more useful.
- **Give people a clear reason to opt in.** The value exchange needs to be explicit. "Get early access to new drops" works better than "enhance your experience."
- **Build a preference center.** Give users a simple page where they can update their communication preferences, email frequency, and privacy choices at any time.
- **Keep consent connected to your tools.** Your banner should control what runs in your analytics and ad platforms. Your CMP should enforce this automatically.
- **Use first-party data to improve lookalike modeling.** Customer lists fed into Meta's or Google's platforms improve audience quality, especially as third-party signals shrink.

04 Optimize your consent rate

What it means

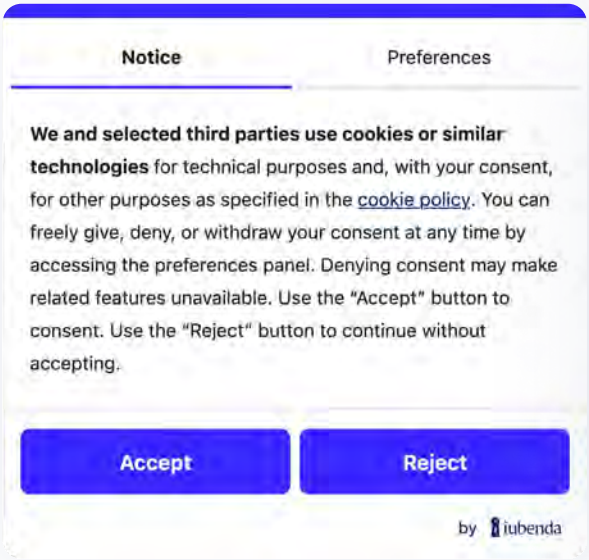
Consent rate, the **percentage of users who actively accept cookies** or **opt in**, rarely makes it onto the marketing performance dashboard. It should.

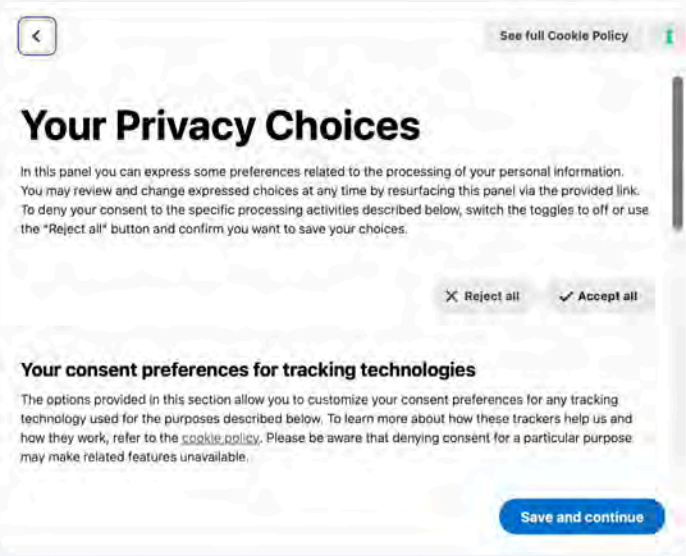
Every percentage point of improvement means:

- More observable conversions
- More accurate attribution
- Better bidding signals and higher return on ad spend

Consent rate optimization means improving that rate through **better banner design, clearer language, smarter positioning, and recovery flows** for users who initially decline.

Why it works





Did you know that banner design, and specifically position, has a measurable impact? **Our own data** shows that placing your banner at the top of the page rather than the bottom can boost consent rates by 16%. Adding your logo increases trust and improves opt-in rates.

Poor consent UX	Better consent UX
Accept and reject buttons in different sizes or colors	Accept and reject options equal in size and visibility
Reject option buried in a secondary menu	Both options visible on the first layer
No way to update preferences after first visit	Accessible preference center at any time through a widget
Banner re-appears every session	Consent remembered across sessions, re-prompted at appropriate intervals
No branding on the banner	Logo visible, design consistent with your site
Slow banner loading	Banner loads quickly, doesn't disrupt page experience

What you can do now

First, get the basics right: your banner needs to load fast and not disrupt the page. A slow or intrusive banner drives visitors off before they've seen the consent choice. You can't optimize a rate that never had a chance.

- **Check your current consent rate.** If you're not measuring it, start. Your CMP dashboard should show opt-in rates by device, country, and banner placement.
- **A/B test your banner.** Test position, button labels, and copy. Even small changes can move rates meaningfully.
- **Use a consent recovery flow.** Our **rejection recovery feature** lets you show a follow-up prompt to users who initially declined, within regulatory limits.
- **Match your banner design to your brand.** A branded banner feels like part of your site. The more natural it feels, the more likely users are to engage thoughtfully rather than dismiss it.
- **Check your mobile experience separately.** Consent rates on mobile often differ significantly from desktop. Test both.

The advantage goes to teams who start now

> "When consent, privacy, and compliance are built in from day one, product, marketing, and growth teams can move faster with confidence. You test more, ship more, and scale without hitting invisible walls."

Andreea Mandeal,
CMO at iubenda

The teams in the strongest position move before they have to. They question assumptions, keep testing, and treat compliance as part of their marketing infrastructure, not a legal formality.

Regardless of how rules around cookie consent is evolving, great marketers start with what they can control today.

💡 Privacy regulation isn't going away. For teams that build well, it stops being a constraint and **starts being a filter: one that separates brands that have earned their customers' trust from those that haven't.**

A partner built for compliance and growth

iubenda has been helping businesses navigate privacy regulation since 2011, long before most marketing teams had ever heard of GDPR. Today, trusted by 150,000+ businesses worldwide, we build tools that handle the legal complexity so you can focus on performance.

Built on legal expertise

Our legal team has been tracking privacy regulation since before it was mainstream. Our Privacy and Cookie Policy Generator creates lawyer-crafted documents covering global privacy laws, including the GDPR in Europe or the CCPA in the US. Update your compliance documents and processes at any time with ease.

Analytics for marketing growth

· Track your consent rate by device, per category, and country.

· A/B test banner designs or obtain first-party data with consentmanager by iubenda to find out what increases opt-in rates.

· Use rejection recovery to give users who initially declined a second, well-timed prompt. Every percentage point of improvement in consent rate translates directly into better data, stronger attribution, and more efficient ad spend and targeting.

Tools that save time

Set up a fully-configured consent banner with preference management center, generate your legal documents, and connect your consent signals to your analytics and ad platforms, all from one place. Our Privacy Controls and Cookie Solution:

· Offers flexible banner design and UX

· Loads fast and doesn't affect your SEO

· Blocks scripts until users consent

Google-certified CMP Partner
with Consent Mode built in.

IAB-validated CMP
with Transparency & Consent Framework (TCF 2.3) support.

400K+
sites and apps supported

27
languages (no AI translations)

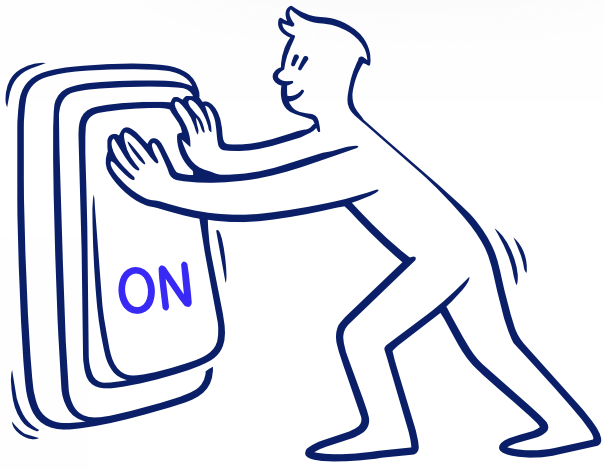
Get started for free

Talk to us

iubenda

Built for compliance.
Designed for growth.

Integrations for all major CMSs:



Disclaimer: This e-book discusses a legislative proposal, not final law. The content reflects iubenda's interpretation as of March 2026 and should not be relied upon as legal advice. Consult your own legal counsel for guidance specific to your business.