usercentrics

Usercentrics Whitepaper

Optimizing Consent Data and User Trust 2023

Table of Contents

PART 1:

Introduction

There is a treasure trove of data available to marketers that is provided by users online via various platforms. The kinds of data that are most valued and the technologies for collection and integration into marketing operations continue to evolve rapidly. The way regulators and companies think about users and their data is also changing.

More consumers are concerned about privacy and how their data is used. This means it's not only regulations that are mandating privacy compliance. Website visitors, app users, ecommerce customers, and others are as well, making transparency and data protection a condition of retaining their attention and spending. This can have a significant effect on brand reputation. Adding further complexity, consumers increasingly expect personalized experiences from the brands they rely on.

The implementation of the European Union's General Data Protection Regulation (GDPR) in 2018 was an influential point when attitudes and focus on data privacy really began to shift. An unfettered mentality regarding gobbling up user data in as great a volume and from as many sources as possible is no longer how smart companies do business.

It is becoming standard business practice to protect users' privacy and rights to their data and to provide them choices about its collection and use. This is no longer a novelty, but a legal requirement and competitive advantage. PwC found in 2022 that 71% of consumers surveyed won't buy from a company they don't trust[1]. Marketers understand that it's just good business. It builds user trust, and advertising partners increasingly require it.

Many data privacy regulations have been passed around the world since the GDPR, and more are coming. Gartner had predicted that by the end of 2023, 65% of the world's population would have their data and privacy protected by modern regulations[2]. Now they predict that by the end of 2024 it will be 75% of the population[3].

We have better technology, integrations and a better understanding of the value of high quality data and how it is obtained. Companies are also realizing the cost savings and revenue potential of investing in creating better user experiences. Those experiences, and the long-term engagement they represent, center around trust.

---

1 'Trust: the new currency for business - How trust impacts business and how companies can cultivate it', 2022 Trust Consumer Intelligence Series, PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/trust-new-business-currency.html

2 September 2020, 'Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations', Gartner, Inc., https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w

3 May 2022, 'Gartner Identifies Top Five Trends in Privacy Through 2024', Gartner, Inc., https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024

Marketers are embracing the next phase of this data evolution with privacy by design, and implementing consent into data strategy and marketing operations. They are developing their understanding of how consent can provide a competitive advantage and build user trust, leading to more and better data acquisition, positive brand reputation and long-term customer relationships.

Freely

Consent must be given freely, access must be possible without consent.

Informed

All relevant information must be given at the point of providing consent.

Granular

The purpose of the date collection most be granular. A general consent is not valid.

Explicit

Consent must be given explicitly eg. through a click or other activity; implicit consent is not valid.

In Advance

Technologies, not covered by legitimate interest, should only be loaded if consent is given.

Easy to withdraw

Consent should be easy to be withdrawn as it is to give.

Documented

The website must be able to prove that user has given consent and consent meets the requirements for a valid consent.

The seven criteria for valid consent laid out in the GDPR remain an excellent guide to consent management.

Organizations continue to have a four-pronged challenge:

1. maintain auditable privacy compliance with relevant regulations
2. get the data needed for marketing strategy, insights and ad revenue
3. enable legally valid user consent choices
4. build trust by demonstrating the priority of data protection with positive, transparent user experience

A consent management platform (CMP) helps achieve and maintain these goals across platforms, and we will share best practices for optimizing your CMP implementation. So, operationally speaking, when implementing tools like a privacy policy or cookie banner, what are the best ways to optimize user engagement and consent?

PART 2:

Introduction to Consent Management

One of the core provisions of many data privacy regulations today is that individuals need to be informed about data collection and processing, and most commonly have to consent to it.

In many cases a “prior consent” model is in effect, also known as opt in. Consent from data subjects — the people whose data will be collected, processed, and potentially shared or sold — must be obtained before any data is collected, including before cookies or other tracking technologies are activated on websites.

Some laws use the opt out model instead. In this case data can be collected and processed, often even shared or sold, before the data subject’s consent is given. The data subject does, however, have to be informed about data collection and processing, and given the option to opt out of some or all of it at any time.

A consent management platform (CMP) like Usercentrics’ is valuable for all of these regulations, notification requirements, and consent models. It detects and informs about cookies and other tracking technologies in use. It provides required data collection and processing information to users in a clear, organized way. It collects and securely stores user consent or opt out choices, and enables users to change consent preferences in the future. The CMP also enables automated updates, so organizations can maintain data privacy compliance as relevant regulations or the technologies they use change.

PART 3:

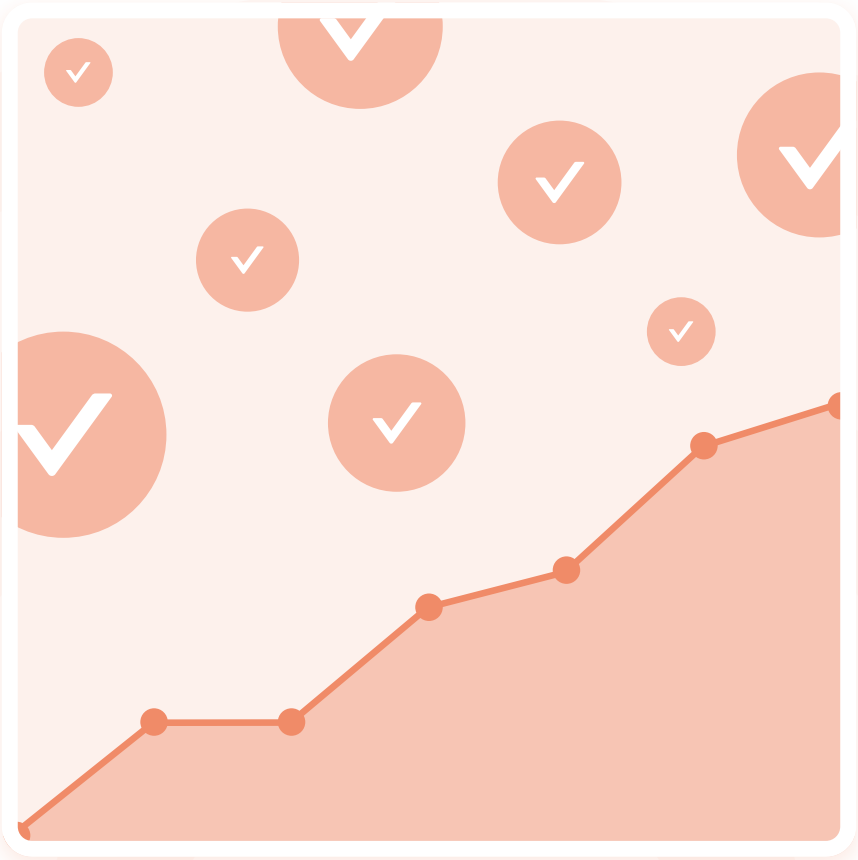
Introduction to the Consent Management Platform (CMP)

The Usercentrics CMP works across platforms like web, apps, or Connected TV (CTV). When displayed, the CMP banner or wall informs users about what Data Processing Services (DPS) are in use — like cookies and other tracking technologies in the browser — and what personal data would be collected. Usercentrics regularly updates the DPS database, enabling automated maintenance of Data Processing Services in use by the CMP for privacy compliance.

The CMP provides users with choices to consent to collection of personal data via all the DPS in use, a granular selection of DPS as chosen by the user — e.g. yes to tracking for analytics, no to tracking for personalized advertising — or to decline all personal data collection. Users can review all cookies and tracking technologies in use in detail.

The CMP securely stores users' consent choices, enabling users to update their preferences or grant or revoke consent at any time. The CMP enables a consent audit trail if requested by data protection authorities.

Visual components on your website that collect user data, such as videos or maps, can also be automatically blocked via the CMP with Usercentrics' Smart Data Protector feature, unless the user has given consent. This provides an extra layer of security for data privacy compliance.



PART 4:

Introduction to Consent Measurement

There are a number of rate metrics tracked in consent management, and for simplicity we will generally refer to them as “consent rates”. However, for clarity, let’s look at other common terms that mean the same, as well as Usercentrics’ CMP’s Analytics and various rate metrics that make up consent rates.

What is included in the consent rate?

Opt-in rate and acceptance rate are other terms that can be interchangeable with consent rate. Overall they refer to how many people have opted in to share some amount of their personal data by providing consent in the CMP (e.g. clicking “Accept All”). However, in Usercentrics’ CMP they refer to specific user actions and types of consent.

Introduction to Usercentrics Analytics

The Usercentrics CMP includes two kinds of analytics that are unrivaled in sophistication, user-friendliness, and depth of data and insights. These are Interaction Analytics and Granular Analytics, with multiple types and rates of consent measured between them.

Interaction Analytics enables monitoring of your CMP setup and user interactions with it. These analytics enable gaining accurate insights quickly to drive optimization of a wide variety of the visual, textual, and functional aspects of your CMP implementation, e.g. with A/B testing.

Granular Analytics provides detailed information about consent at the service and category level. Among the benefits, this information helps you perform in-depth analyses and find the best categories for your Data Processing Services.

Interaction Analytics

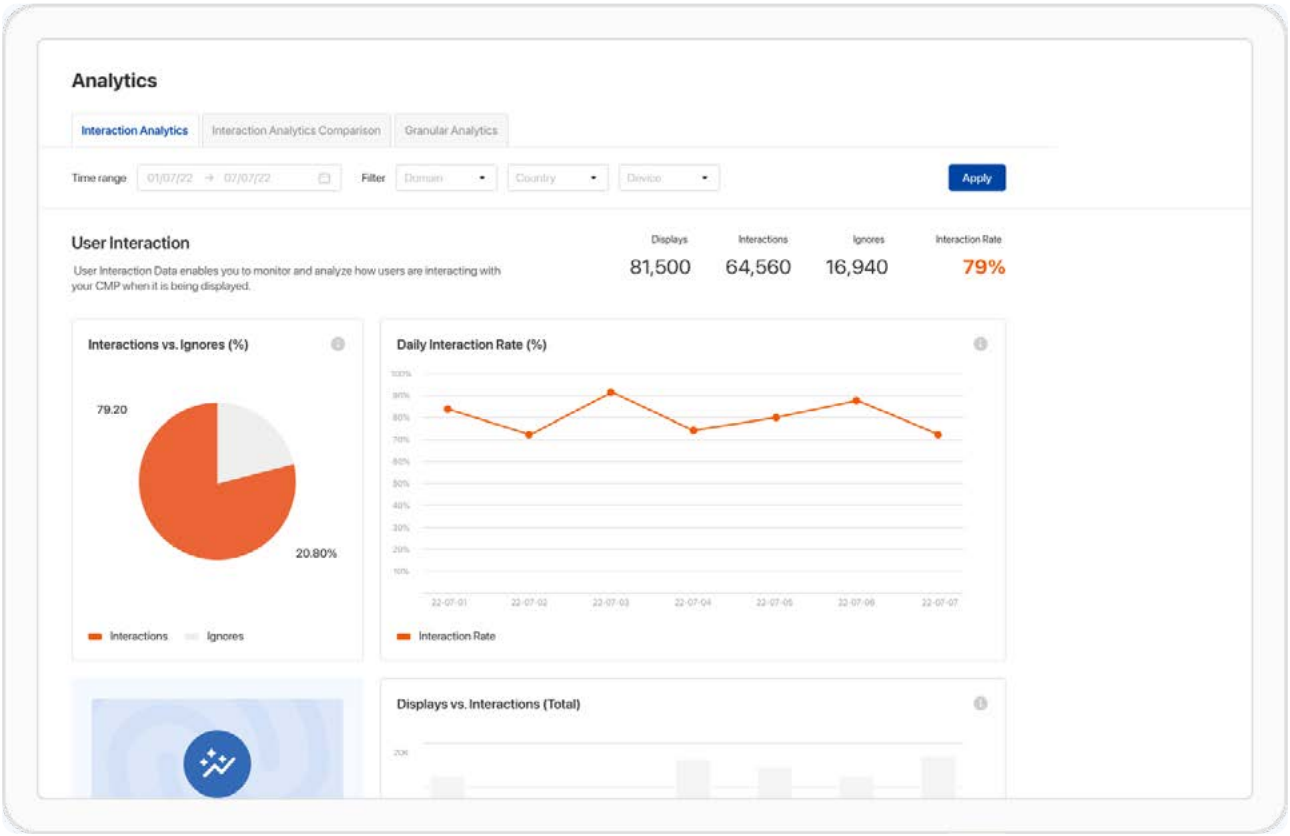


Fig. 1: Usercentrics branded CMP example, Interaction Analytics dashboard featuring User Interaction metrics

Interaction Analytics provides two KPIs: Interaction Rate and Acceptance Rate. The Interaction Rate shows how much your users interact with the CMP, giving you the full picture on users who make consent choices or who ignore the CMP. The Acceptance Rate is the percentage of “Accept All” choices based on all interactions. It includes users who have consented to collection of personal data collection from the Data Processing Services in use via the “Accept All” button. The results of the A/B Testing feature are also displayed in the Interaction Analytics dashboard.

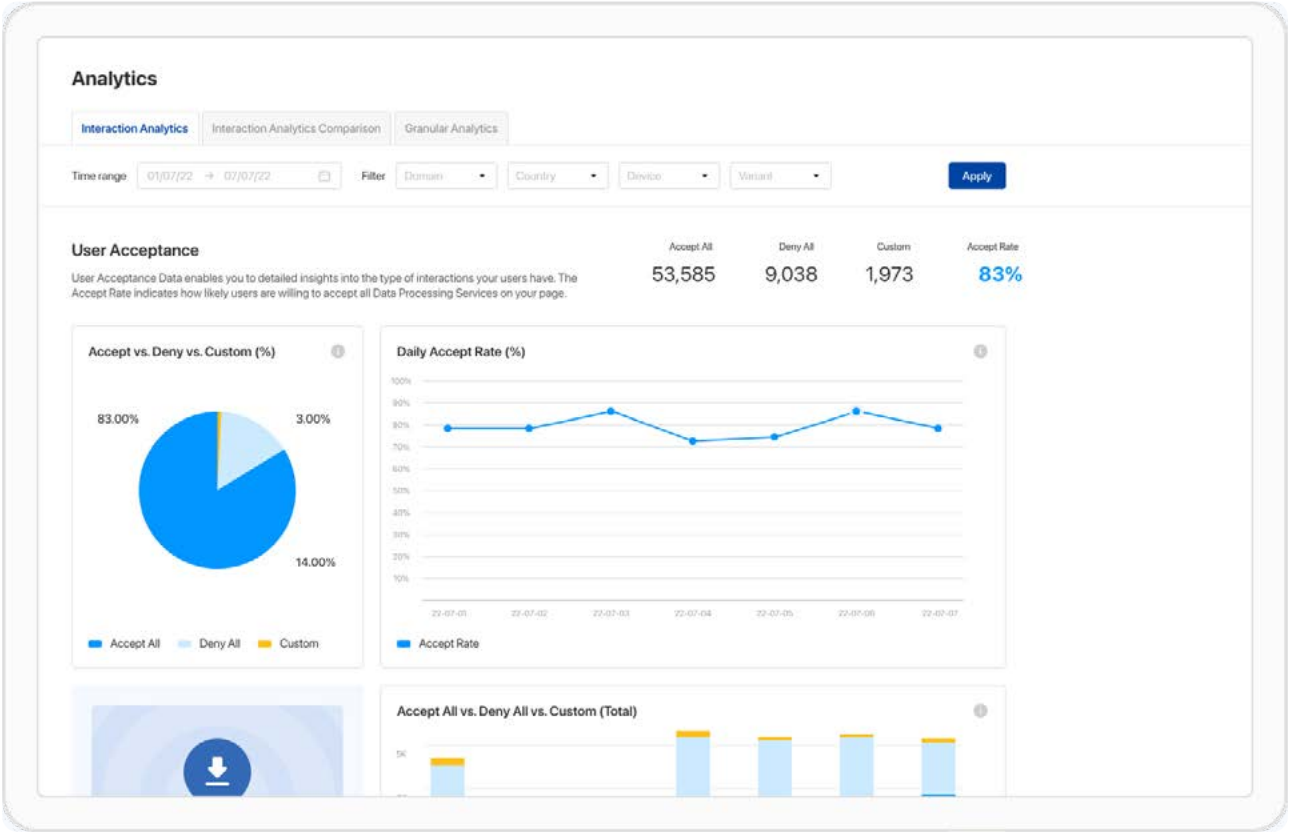


Fig. 2: Usercentrics branded CMP example, Interaction Analytics dashboard featuring User Acceptance metrics

Granular Analytics

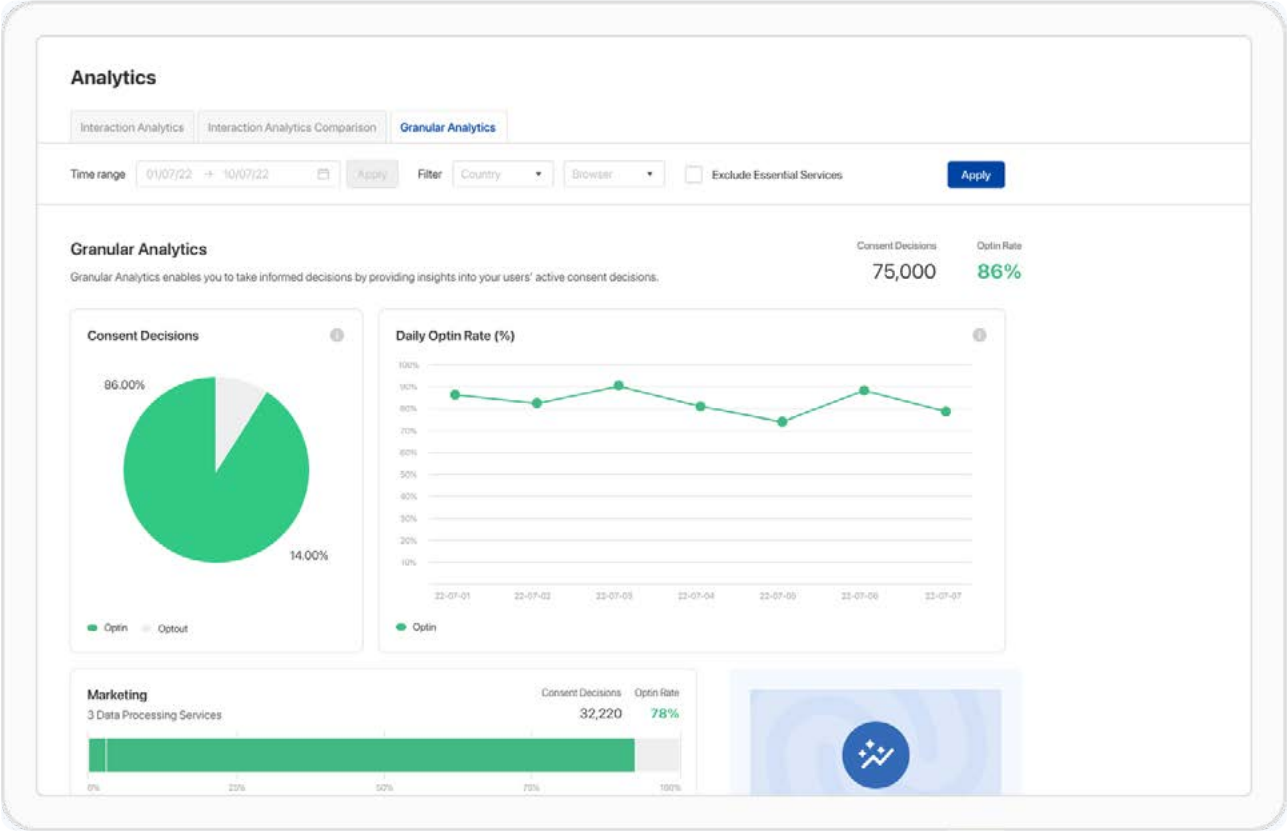


Fig. 3: Usercentrics branded CMP example, Granular Analytics dashboard featuring Consent Decisions and Opt-in Rate metrics

Granular Analytics provides in-depth data to improve categorizations, get consent rate data for all or individual services, and drive better decision-making to optimize every aspect of your CMP implementation. It is specific to individual consent choices.

Included under Granular Analytics is the Opt-in Rate, which is the percentage of opt-ins (Accept All, Deny All, or Granular Acceptance) for all consent decisions. Granular Analytics provides the insights for categories, such as Marketing, or for each individual Data Processing Service, e.g. Google Ads. There is also a Daily Opt-in Rate, which is the overall daily percentage of opt-ins in all consent decisions.

PART 5:

Introduction to CMP Optimization

When we look at optimizing consent rates, we need to consider two main things: interaction and optimization.

When the user arrives on-site, your organization is making its first impression. You want the CMP user experience to be positive and seamless to engage them. Capturing this first engagement and making the experience clear, streamlined and easy to use will help you achieve higher acceptance rates.

However, non-engagement is also relevant to the interaction KPI and improving it. Under a number of data privacy regulations, clicking away from a banner or scrolling past cannot be construed as valid consent. Users need to look at it, read it, and be able to quickly understand it to make choices. They need to be provided with clear options presented equally. Manipulative design elements to push users toward desired actions have been commonly used online in the past. Today they are strongly frowned upon by data protection authorities and are illegal under some regulations.

Actions that manipulate or "nudge" the user toward a desired action are also called "dark patterns". They are bad design or consent strategy.

LEARN MORE

What are dark patterns and how do they affect consent?

Interactions

Once users have noticed the CMP display, you need them to actually interact. As noted, for valid consent, passive actions like scrolling by or clicking away are not accepted. There need to be equally presented “accept” and “decline” options displayed, and information must be clearly and succinctly provided to explain what the user is accepting or declining. Web and app users are often impatient about waiting, so ideally you want the consent banner to feel like a seamless part of the site’s user experience, not like it’s getting in their way.

When users understand what they’re being asked for, why, by whom, and what the benefit to them is, there are better odds of them engaging positively with the consent banner and providing their data.

CMP Optimization

Once you have implemented the CMP, that is version one. You set it up and customize it according to your corporate branding and messaging, regulatory requirements and user experience best practices.

From there, as users start to interact with the banner, you gain data, which is obtained when users consent to collection and use of personal data. But also data about their actions and interactions with the consent banner itself.

Then you can use this data to start optimizing the banner itself to increase consent rates. This can include size, color, messaging, location, and other elements. There are plenty of ways to determine how to make it work best for your website experience and audience.

Optimizing Interactions

Optimization here means minimizing the amount of non-interaction with the consent banner and maximizing the number of users, visitors or customers who engage with it. Ideally, you want everyone to interact with it and to provide consent, but at the very least the CMP's analytics will provide data to drive further optimization insights.

Optimizing Acceptance

Optimization here means maximizing the number of users who interact with the consent banner and provide consent (ideally "Accept All").

Focusing Optimization Efforts

Most users who interact with the CMP do so on the first layer, i.e. the UI displayed to them when the website loads. So this is the best place to focus optimization efforts.

For interactions where we have the layer information, from a total of 1,897,537,157 layer-specific interactions, 93.42% of the interactions are on the first layer and 6.58% are on the second layer.

1,897,537,157
layer-specific interactions

93.42%
on the first layer

6.58%
on the second layer

The industry or sector, and the purpose of the user's visit to the website or app, can affect the degree of user interest in managing their data privacy. For example, a visitor to a healthcare or insurance website may be thinking more about their data privacy and have a greater interest in protecting it at a more granular level, than someone visiting a news site to catch up on current events, or an ecommerce site to buy a t-shirt.

Users' motivations should be considered with regards to the optimization strategy for the CMP. Different organizations also have access to different incentives to offer users or customers to encourage consent, e.g. the t-shirt website could offer a discount code or free shipping, but a healthcare website can't.

PART 6:

User Interaction and Acceptance Rates

We analyzed in-use customer configurations of the Usercentrics CMP over several months, with a number of parameters. The goal was to test assumptions of what factors contributed to higher interaction and acceptance rates, and to get real world data on what factors contributed.

All CMP configurations that we analyzed had interaction and acceptance rates over 80%. Additionally, the percentage of banners using specific elements that can contribute to interaction and acceptance rates are outlined below.

We will look at individual elements of successful banner configurations, but overall, what are the interaction and acceptance rates we found?

For the CMP configurations analyzed, the interaction rate was 66.28%. The overall acceptance rate for CMP configurations analyzed was 81.49% (of the 66.28%).

the interaction rate was

66.28%

the acceptance rate was

81.49%

These metrics always go together, which is why we looked at customers' in use CMP implementations that had both interaction and acceptance rates over 80%.

The data was sourced over a period of 30 days from late 2022 to early 2023, and included 1.09 billion CMP displays.

Within the data set there were 722.62 million interactions with the CMP and 588.83 million uses of Accept All.

IMPORTANT NOTE:

These numbers are based on various differing CMP configurations, not one standardized one. Additionally, they encompass a variety of industries, company sizes and relevant legal frameworks. Identified bots were excluded from the data.

PART 7:

Data Insights by CMP Element

There is a variety of elements that can be customized and optimized with Usercentrics CMP, including:

- banner or wall
- access to website (CMP interaction or not)
- colors
- text / language
- banner appearance (e.g. branding elements)
- appearance of buttons / links
- overlay (CMP background overlaying website)

We will look at various options for these elements and what analysis has shown for best performance. As always, we cannot provide legal advice, and organizations, particularly their data protection officer (DPO) and/or privacy expert, should consult qualified legal counsel regarding privacy compliance and consent management for relevant regulations. User experience professionals should also be involved in the design and implementation process to ensure best practices.

For our analysis to find the best performing CMP elements, our specifications were:

- configurations with more than 1,000 monthly sessions (also ensuring exclusion of test accounts)
- interaction and acceptance rates above 80% (selected based on industry experience and benchmarking)

569 configurations fulfilled these requirements. In the tables below you will see elements of the CMP divided into three categories:

- elements in the first layer
- elements in the second layer
- general elements of/around the displayed CMP

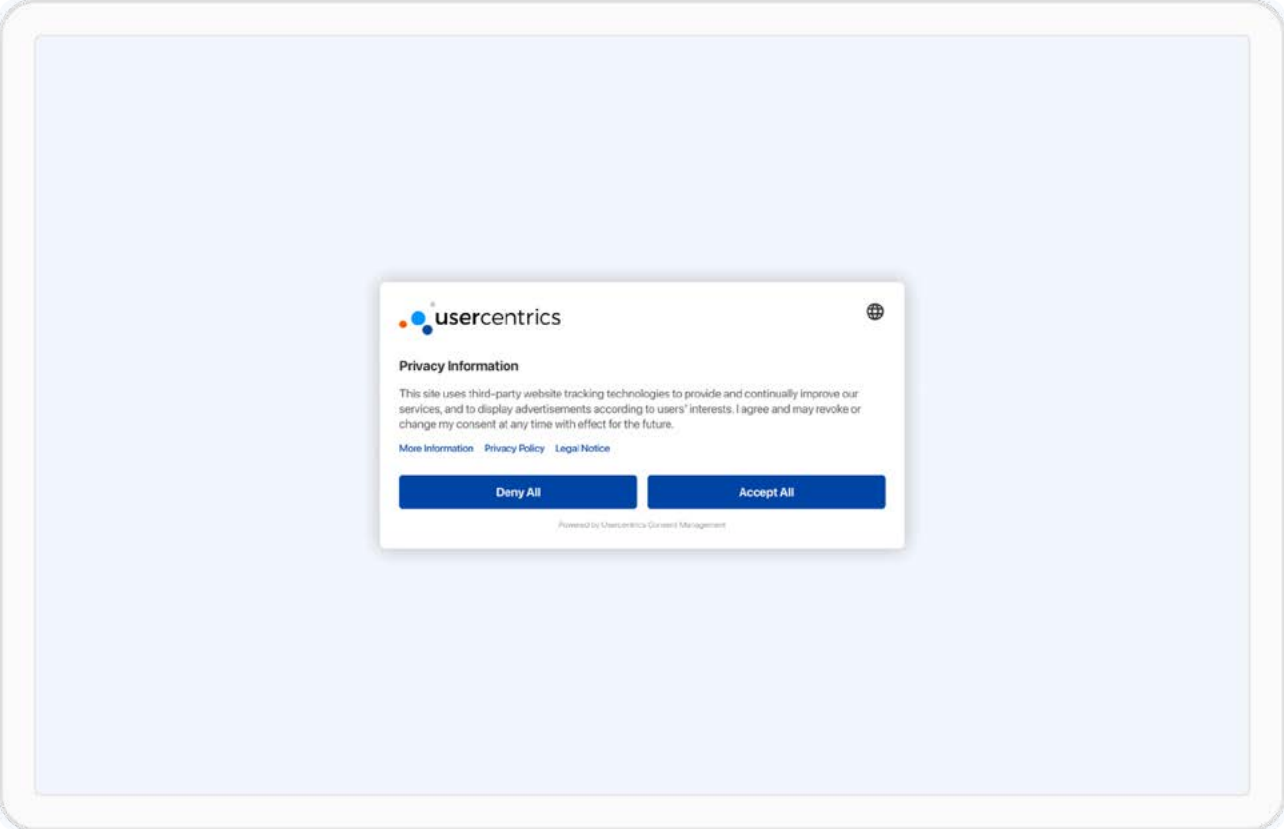


Fig. 4: Usercentrics branded CMP example, wall configuration, first layer

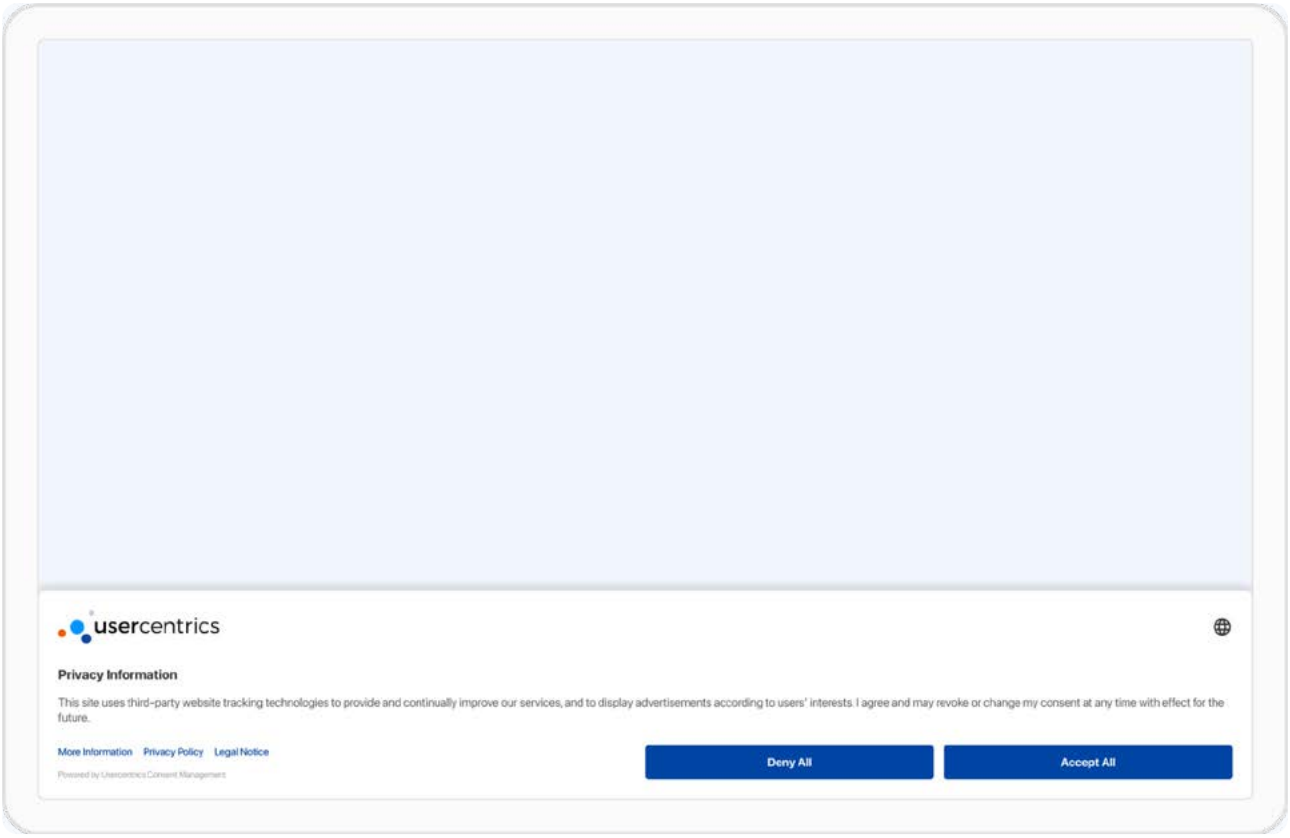


Fig. 5: Usercentrics branded CMP example, banner configuration, first layer

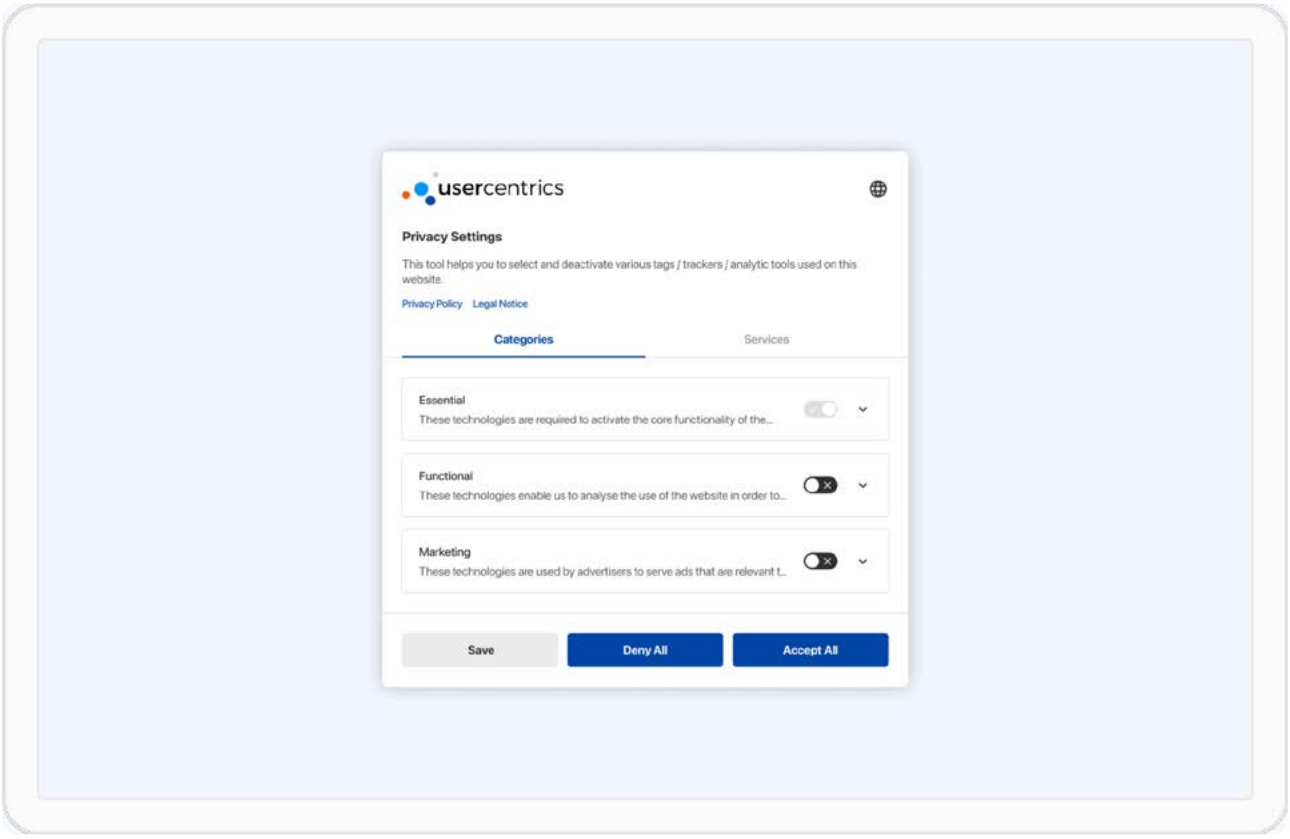


Fig. 6: Usercentrics branded CMP example, display of Categories of Services in use, second layer

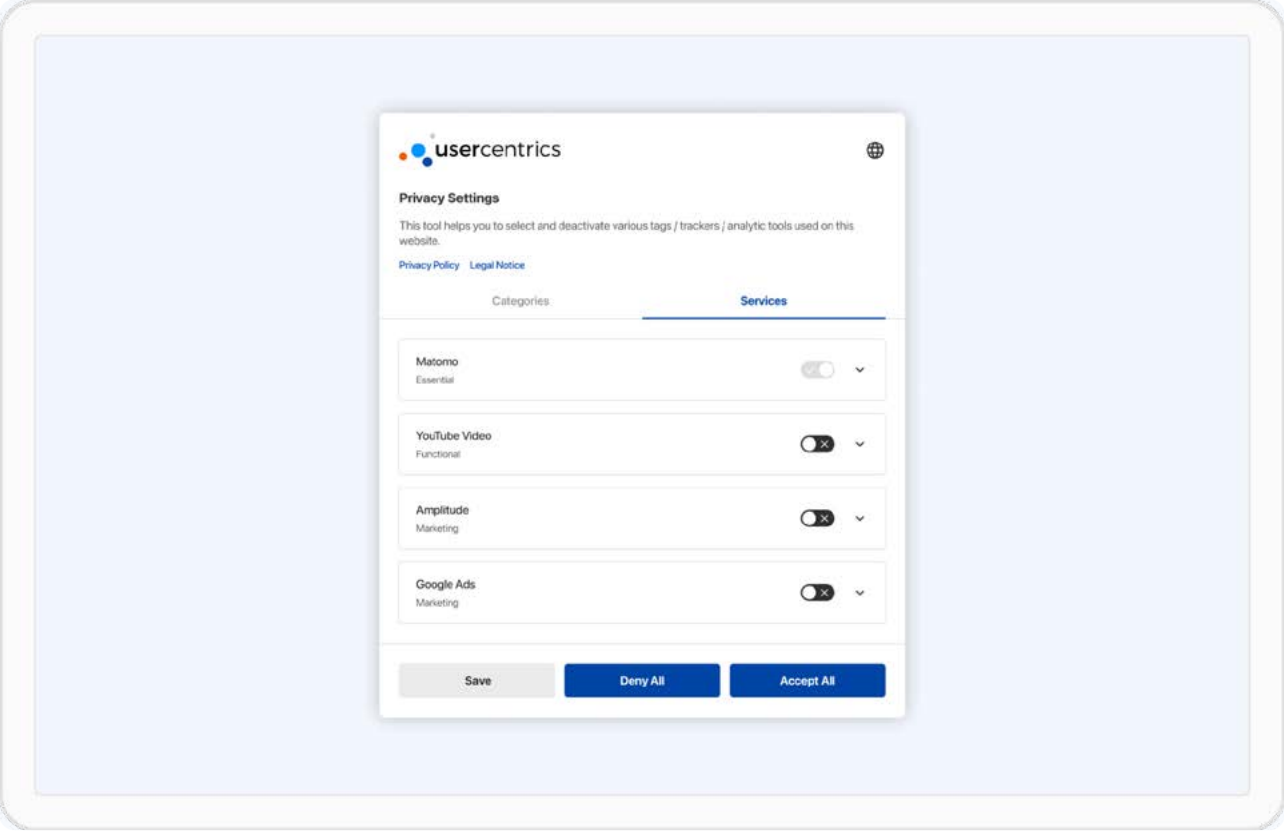


Fig. 7: Usercentrics branded CMP example, display of specific Services in use, second layer

The percentage shown is for the number of configurations analyzed that used that element, resulting in interaction and acceptance rates over the 80% threshold. It does not show a specific percentage of opt-ins when that element was used. E.g. 99.3% of CMP configurations analyzed had the Background Overlay activated. That means almost every CMP analyzed used that element, and had a consent rate over 80%.

While some elements can quite safely be seen as contributing to high consent rates, it is important to think of various elements as part of the whole user experience. It is also important to be careful that display and user experience choices for the display of the CMP do not dip into manipulative design elements that could be construed as dark patterns.

Temporary high consent rates that result from manipulative design choices are not worth the scrutiny of data protection authorities, regulatory fines, or loss of data or brand reputation. Enforcement of compliance, including how it is obtained, is increasing and becoming more widely publicized.

Data analysis insights

First Layer

These are the element activation results for the **first layer of the CMP,** for configurations with a consent rate over 80%. These elements are what users see in the CMP display when they first arrive at the website or app.

Element	Percentage (%) of Configurations with Feature Selected
Wall (FirstLayerLayout)	84.53
Custom banner message (FirstLayerBannerMessage)	84.18
Deny All button not included (FirstLayerShowDenyAll)	73.99
Link as more information trigger (FirstLayerMoreInformationTrigger)	68.37
Categories not included (FirstLayerDisplayCategories)	65.03
Default banner title (FirstLayerBannerTitle)	63.09
Custom logo (CustomLogo)	51.32

Second Layer

These are the element activation results for **the second layer of the CMP**, for configurations with a consent rate over 80%. These elements are what users see and the functions accessible (like categories) if they click through from the first layer.

Element	Percentage (%) of Configurations with Feature Selected
Center display of modal (SecondLayerLayout)	88.93
Default banner title (SecondLayerBannerTitle)	77.50
Deny All button not included (SecondLayerShowDenyAll)	66.26
Custom banner message (SecondLayerBannerMessage)	52.90

General Elements

These are the element activation results for other design elements of the CMP, for configurations with a consent rate over 80%. They relate to the overall UX and are not specific to which layer is displayed.

Element	Percentage (%) of Configurations with Feature Selected
Background overlay activated (BackgroundOverlay)	99.30
Background shadow activated (BackgroundShadow)	97.37
Link as privacy trigger* (PrivacyTriggerType)	80.49
Preset font family used (FontFamily)	67.66

*This is the mechanism to open the CMP again once the user has already initially interacted with it, e.g. if the user wants to check or change consent choices. One option for this mechanism is the “fingerprint” button, and the other option is a link.

Summary of insights

Your organization's specific CMP implementation and customizations will depend on:

- your branding
- Data Processing Services used on your website or app
- regulations relevant to your company and audience
- purpose of your website
- your audience

Your DPO and qualified legal counsel should always be involved in ensuring that implementation and optimizations are in line with regulatory requirements. UX input to ensure overall positive user experience is also important.

First Layer results

Location and style of modal display

As with use of background overlay and shadow, using a wall as opposed to a banner also encourages more focus on the CMP, as well as higher user interaction and consent rates. Please be aware that it can be a violation, or at least significantly frowned upon, to prevent/block user access to the website or its functionality if they do not engage with the CMP or decline consent.

What belongs on the first layer

Not including a Deny All button on the first layer is a configuration that we cannot recommend and should be discussed with your DPO. It may improve consent rates if people don't have much choice but to provide consent to get access to the site or remove the banner, or if they have to go hunting in the banner message or in another layer for the "Deny All" option.

Design elements that slow down or prevent the user's ability to make the consent choices they want could increase the bounce rate if people get frustrated by being blocked and leave the website. For example, not being able to access the website without interacting with the CMP, or not being able to find a "Deny" button. Data protection authorities could also view these as manipulative tactics, potentially a violation of data privacy law.

What belongs on the second layer

Not including categories in the first layer is a bit of a different situation. Trying to include this information on the first layer could make the CMP's appearance confusing and overly cluttered. Most users do not access or customize their preferences to that degree, so locating that information and customization options in the second layer enables a clearer layout and user experience.

Using a link to access more information in the CMP is a popular choice, and may have advantages over a button in preventing confusion if your configuration already has several different buttons, as the link can display user-friendly wording.

Customizing all the elements

Customizing the banner's messaging is highly recommended. The CMP has a short amount of time to make a good first impression. Messaging should be clear, informative and brief. The tone, like the visual elements, should also match the company's brand.

Only about half of the CMPs analyzed used a custom logo, which Usercentrics recommends to present a cohesive brand impression and build trust. Though it may not have a significant effect on consent rates, your logo provides an immediately recognizable signal that this messaging comes from your organization and is not phishing or an ad.

Almost two-thirds of banners analyzed used the default banner title. Customizing this can be an opportunity to clearly indicate the banner's purpose, though by now many internet users are familiar with cookie banners and their purpose.

Second layer results

Location and style of modal display

Close to 90% of banners analyzed kept the center display of the banner for the second layer, which gets 6.58% of user interactions. This choice makes sense, especially if information like categories is included, and keeps the banner focused in front of the user.

Use of default banner title

Over three-quarters of the banners analyzed used the default banner title. Arguably a customized title would be more important in the first layer when organizations are trying to initially capture users' attention. Users that click through are already likely fairly engaged with the banner's functions and have specific goals when accessing the second layer, which wouldn't require notice of the title.

Custom messaging

Only a little over half of the banners analyzed used custom messaging on the second layer. For the reasons outlined above, custom messaging would likely be less important on the second layer. However, if your organization customizes the second layer in other ways beyond just presenting more granular services and consent information, and wants specific interactions from the user there, some customization of messaging may be beneficial.

Use and location of “Deny/Deny All” option

Not including the Deny All button in the first layer is a potential concern from a user experience standpoint, or if audited by a data protection authority. We recommend discussing this with your DPO.

Two-thirds of banners did not include the Deny All button in the second layer. If this means it was included in the first layer, likely best practices are being used. But if it’s not included in the first or second layer, that means the consent options are not equally displayed and is a violation of a number of data privacy laws. Ensure a clear and equally presented opt-out option is included.

General elements results

Location and style of modal display

Background overlay and shadow and use of a wall (with center of the page display) of the CMP focuses user attention and encourages engagement to boost interaction and consent rates.

However, the opacity or mobility of these elements is the important factor. Under a number of data privacy laws, it is a violation, or at least significantly frowned upon, to prevent user access to the site, its content, or functionality if they do not engage with the CMP. Under the GDPR, for example, it violates the requirements that consent be freely given and unambiguous. Also, remember that insights still can be gained from users who do not interact.

Re-access link vs. graphical button

Using a link to re-access the CMP is a popular choice, and may have some advantages over the “fingerprint” button. A link’s text can make it clearer right away that it enables access to the CMP, and thus be easier for users to find to update their consent preferences.

Customizing fonts

Using the preset font family can ensure good readability, though your corporate branding, UX and accessibility should be considered as well. The messaging is more critical for optimization.

Keep the UI tidy

Limiting the amount of interactive content has a positive effect on consent rates. However, be careful using this strategy if it leads to unequal display of information or access to consent choices.

PART 8:

Usercentrics CMP Features for Customization and Optimization

Setting up the CMP is a great first step in achieving data privacy compliance and building trust with users. As soon as the consent management platform is live, you will begin to collect data. Not just users' consent preferences, but also if and how they interact with the CMP, what they consent to, etc. This data will help you optimize the configuration and user experience on an ongoing basis to increase consent rates. The Usercentrics CMP has a variety of features to customize and optimize the CMP for user experience and increased consent rates.

First, A/B Testing and a use case to show you how to draw insights from your data, decide on changes, and test how those changes perform to enable rapid optimization.

We'll look at some additional features to customize the user experience, enabling more opportunities to request consent in specific contexts while complying with data privacy requirements. We'll also look at tools and options to still gain compliant data and insights when users decline consent.

Late consent or incentives (like with our partner trbo) can also be used to boost consent rates, depending on your audience and business goals.

A/B Testing

A/B testing removes guess work from your CMP optimization and can increase consent rates faster by enabling you to determine which testing variants produce desired results.

The Usercentrics CMP provides built-in A/B testing functionality via the Admin Interface. This enables displaying two versions of the CMP, e.g. with different text and UI elements, and measuring the effectiveness of each to choose the one that performs better. A/B Testing is available for the CMP for both web and apps.

The Usercentrics CMP also integrates with third-party tools like Optimizely, Kameleoon, trbo, Dynamic Yield and Google Optimize for web, or Firebase AB Testing and Optimizely for apps, so you can achieve an even broader range of insights. We provide guides to use these tools with the CMP.

Web CMP A/B Testing Documentation

App CMP A/B Testing Documentation

A/B Testing Example

Note: Example banner displayed shows the element tested for KPI optimization, but has been anonymized.

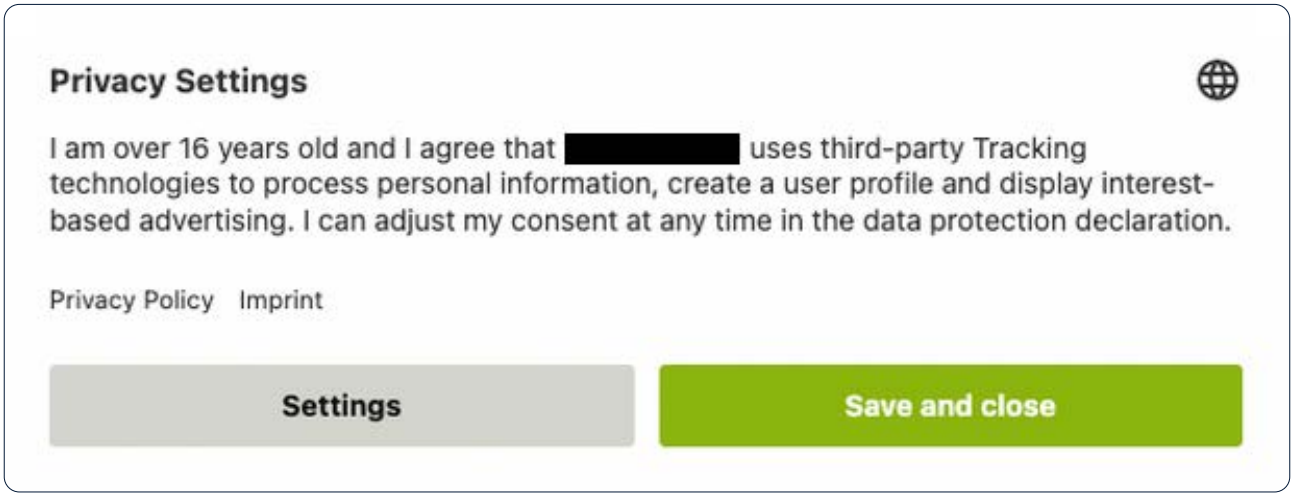


Fig. 8: Branded but anonymized CMP example, tested for KPI optimization, display of first layer

Use of Overlay Example

The customer tested the use of the CMP banner with and without the background overlay over a period of four months from late 2022 to early 2023. Each of the banner variants — with and without the background overlay — was displayed about 1,200,000 times.

Without Background Overlay		With Background Overlay	
Interaction Rate	72%	Interaction Rate	97.37
Acceptance Rate	87%	Acceptance Rate	97.37

For the test case, use of the background overlay helped to increase the combined Interaction and Acceptance Rates by 9 percentage points. This means that the overall percentage of acceptances on CMP displays increased significantly. A/B Testing is a great tool to test and optimize a wide variety of CMP setups and elements down to a granular level.

Contextual Consent

Contextual consent enables websites to obtain explicit, timely consent for a specific use. It can prevent consent fatigue by not requiring users to weigh consent options right when they arrive on a site or app or consider a lot of consent options at once.

For example, there is a YouTube video embedded on the website and the user wants to watch it, but hasn't opted in to YouTube's tracking. You can display a customized overlay to request consent for YouTube, which will enable this video to be played for the user. The user is informed of the necessity of this specific consent request, as well as the context.

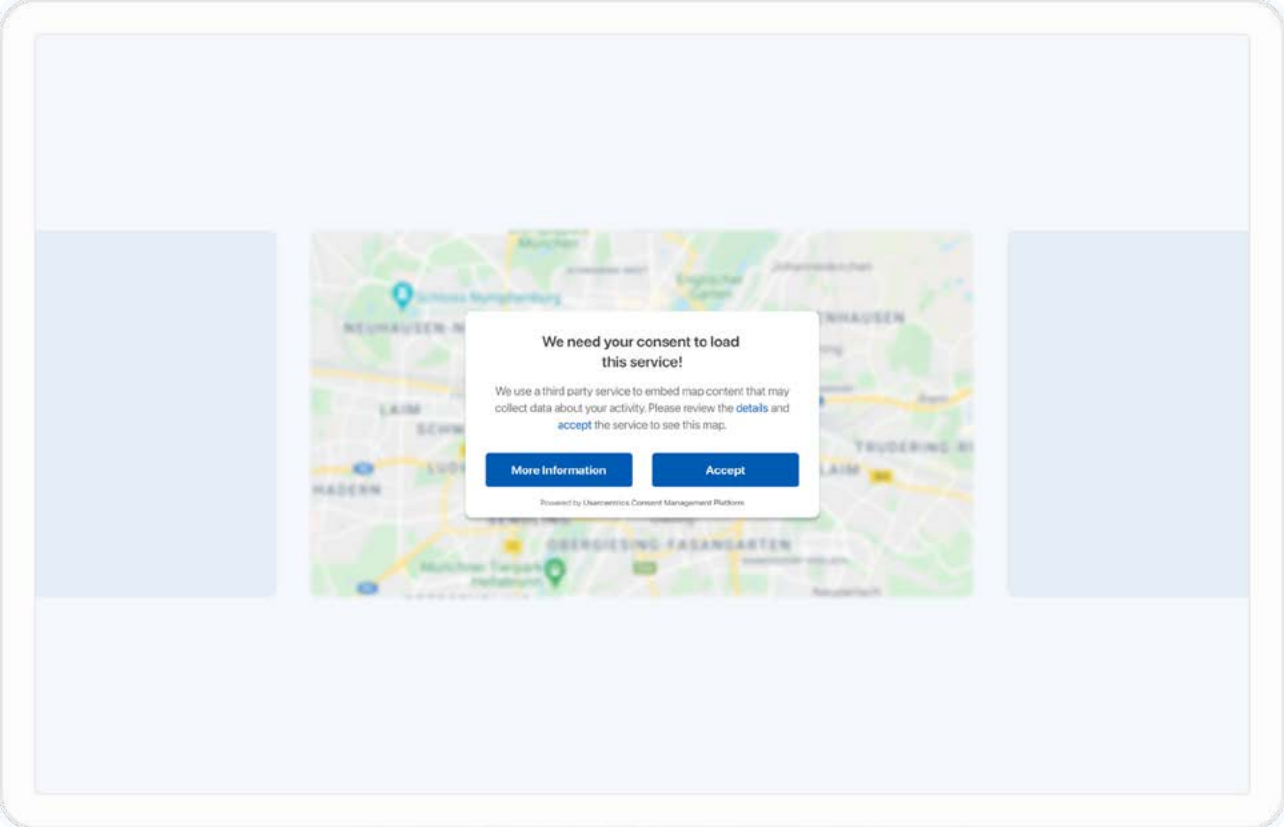


Fig. 9: Usercentrics branded CMP example, display of Contextual Consent in use over embedded map

Contextual consent can be implemented in two ways, via the CMP's Smart Data Protector feature, or manually via API.

Smart Data Protector

The Smart Data Protector is a service that automatically blocks many third-party technologies and prevents transfer of user data to these services unless the user provides consent to activate them. It automatically presents an overlay for services with a visual component when consent is needed to activate them, e.g. YouTube, Google Maps, Calendly, etc. (See full services list.) The Smart Data Protector is not only a great feature for those sorts of visual interactive services, but also a highly useful tool for auto-blocking for a wide range of services.

Usercentrics' Smart Data Protector service will also provide users with a preview image of the video, provided by our servers (so no data transfer), so users can quickly see if they want to provide consent in order to view it.

API

In addition to the Smart Data Protector, our JavaScript API can also be used with events to programmatically check whether the user has opted in to specific services or all services, e.g. during a user's ecommerce checkout process.

If no consent has been obtained, a manual consent request relevant to the workflow can be displayed, similar to blocking visual elements such as YouTube videos with the Smart Data Protector. The API gives you even more possibilities. For example, during the checkout process, customers could be programmatically offered a 20% discount voucher for consenting to certain services.

Which offers can be displayed, and in exchange for what user action or information, will vary by jurisdiction, as there can be legal debate of the voluntary nature of consent in exchange for incentives if they are too substantial. As always, you should consult legal counsel and/or your data privacy specialist.

Google Consent Mode

Usercentrics is a certified partner for Google's CMP Partner Program. Using Google Consent Mode enables the CMP to send a consent-based signal upon which Google services act, and helps manage scenarios where users select "Deny All". It is a helpful tool for data-driven marketing, enabling companies to get back a significant percentage of data for advertisers and gain conversion insights even from users who do not provide consent.

Google Consent Mode enables adjustment of Google tags and scripts behavior based on users' consent status. Tags are loaded on web pages before the consent dialog appears, so tag behavior will adjust dynamically depending on users' consent choices. Measurement tools will only be employed for specifically determined purposes if the user has given consent.

The CMP collects users' consent status, which is transmitted by Google Consent Mode to Google for further processing. Only information about consent choices is transmitted, but no personal data, thus maintaining user privacy at every step.

Learn more about Google Consent Mode.

PART 9:

Key Takeaways and Next Steps

There is a treasure trove of user data online that's available to marketers, but the rules for obtaining and using it are changing. Many data privacy laws have been passed around the world since we published our first Opt-in Optimization whitepaper. Web, app, Connected TV platforms, and the marketing technologies integrated with them, continue to become more sophisticated. Consent management is evolving as well.

Consumers continue to become more aware of data privacy issues and concerned about who can access their data and what it is used for. All of these elements mean significant change for marketers and the data privacy industry. They also contribute to an exciting opportunity. Not only can companies achieve data privacy compliance and protect business interests, but also build real trust and long-term relationships with users and customers. To get the highest quality data, with consent, and provide exceptional user experience to boost revenue.

As our research has shown, attention to a few key elements can have a big impact on the success of your Consent Management Platform implementation and optimizing your consent rates. We summarize best practices for convenience in the handy checklist at the end of this whitepaper.

Overall, the key elements to consent management optimization are good UX practices to get user attention and make it fast and easy for them to make consent choices, plus

clear branding and messaging to communicate what is being requested and by whom.

Beyond that, make sure you work with your data protection officer and qualified legal counsel to ensure you understand your responsibilities for the data privacy regulations that are relevant to your organization, and the cookies and other tracking technologies you use.

We're also happy to help, whether you're figuring out your data privacy compliance responsibilities or want to know if Usercentrics' CMP will integrate well into your tech stack. Book a demo to see how it all works and get your questions answered. Schedule a chat with one of our experts when it's convenient to you.

Our data privacy experts are happy to address your questions and help you meet your business' goals for data privacy, consent rates, and data-driven marketing.

Get expert help now

About Usercentrics

Usercentrics is a global market leader in the field of Consent Management Platforms (CMP). We enable businesses to collect, manage and document user consents on websites and apps in order to achieve full compliance with global privacy regulations while facilitating high consent rates and building trust with their customers. Usercentrics believes in creating a healthy balance between data privacy and data-driven business, delivering solutions for every size of enterprise. Cookiebot CMP is our plug-and-play SaaS, our App CMP handles user consent on mobile apps, and Usercentrics CMP serves companies with enterprise-grade custom requirements for unifying consent and data from capture to processing. Helping clients like Daimler, ING Diba and Konica Minolta achieve privacy compliance, Usercentrics is active in more than 180 countries, with 2000+ resellers, and handles more than 100 million daily user consents.

Usercentrics GmbH
Sendlinger Straße 7
80331 Munich

Telephone: +49 89 21 54 01 20
Email: sales@usercentrics.com