usercentrics

Optimising the Opt-in Rate -
A new discipline in online marketing

June 2020

Table of Contents

A new KPI for your digital marketing

Everything was better in online marketing before, wasn't it? We knew exactly who our customers were, what they liked and how they moved around our website. But the times of "transparent people" are past: Across the world, legal regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) or guidelines of national data protection authorities (e.g. the German DSK, French CNIL etc.) are setting new benchmarks for existing data protection laws. Many digital marketers therefore fear limitations in their digital marketing strategies and associated advertising losses.

However, this fear is largely unfounded because every radical change brings with it completely new chances and opportunities. Marketers should therefore seize the chance now to take ownership of data protection and the technological management of consent in the form of a new marketing KPI: the opt-in rate. Because one thing is clear: **In the long term, consent and the user trust associated with it will become the new currency in marketing.**

The GDPR places concrete requirements on online marketing tools: According to Recital 30 GDPR website operators require a legal basis for the use of technologies such as cookies, pixels etc. (Article 6 GDPR or where applicable Article 9 GDPR). This can be consent, especially when speaking of the processing of user data gathered for advertising purposes. The DSK (German Conference of Independent Data Protection Authorities of the Federation and States) has made its position clear in a policy paper that tracking is only possible with consent, if at all.

Seven criteria must be fulfilled in order for the consent to be legally valid and GDPR compliant. Consent must be easy to withdraw - informed - documented - in advance - granular - freely and explicit. More information regarding the criteria and their use in a cookie banner can be found here.

The ECJ has likewise underpinned this perspective in two landmark rulings from 1st October 2019 (C-637/17) and 29th July 2019 (C-40/17). And: After even industry giant Google announced that it would follow the IAB Transparency & Consent Framework (from 15th August 2020 in Version 2.0), this will establish itself more and more as a standard. This framework was brought into being by the Interactive Advertising Bureau (IAB), the international commercial association for the online advertising sector, to support the sector in implementing the policies stipulated in the GDPR. This essentially means that website operators will no longer be able to get around the use of a consent management platform (CMP) if they wish to continue running their advertisements.

However, this is not the end but rather a great opportunity for all digital marketers - providing they do it right! In the following we will show you how you can protect your advertising revenues using a suitable CMP, strengthen the trust from your users and in so doing gain a long-term competitive advantage. What do you need to do? **Make data protection your priority and the optimisation of your opt-in rate your new marketing KPI!**

Furthermore: The use of a consent management platform (CMP) will not only please the data protection authorities but also gain trust and buy-in from your website users.

- You demonstrate that data protection is important to you.
- The trust from customers in your brand will increase because you are transparently dealing with the topic of data protection.
- Your opt-in rate will increase as customers increasingly engage with the privacy solution.

What does opt-in optimisation mean?

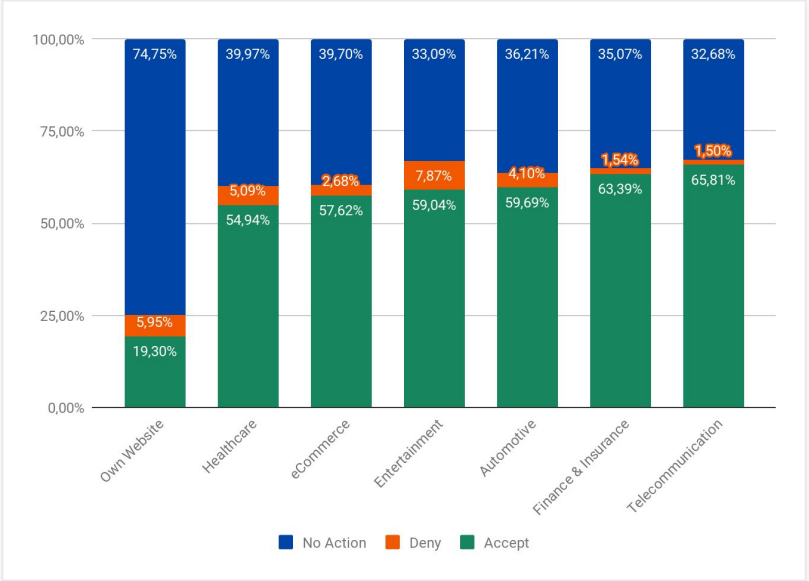
A consent management platform (CMP) helps website operators to obtain, manage and document the user's consent to process data through technologies built into the website. But the journey does not end here. When selecting a suitable CMP you should always pay attention to features which will enable you to optimise your opt-in rate. These include but are not limited to individualisation, AB testing and contextual consent.

But what does opt-in optimisation actually mean? Opt-in optimisation depends on design and technological factors. These include, for example, the placing of a privacy solution on the website, colour adjustments or emphasising certain elements, as well as running the banner programmatically und incentive possibilities.

After analysing our figures we see the biggest lever in the following context: **Opt-in optimisation = no-action minimisation**

In other words: Ensure that users actually interact with your banner

Figure 1: The biggest challenge is the absence of any user reaction, not rejection per se



Source: Usercentrics Analysis (106,109,588 unique visitors), April 2020

What does opt-in optimisation mean?

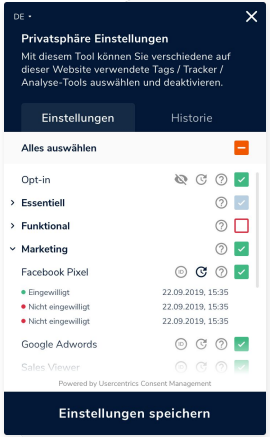
The motto must always be “less is more”. This means that your website visitors should always be encouraged to opt in but never coerced. Too much pressure (e.g. through forced interactions or conspicuous signal colours which do not match the website design) can quickly lead to visitors leaving the website (bounce rate) or not providing their consent at all.

Achieving the first interaction with a website visitor is the key to a high opt-in rate as the visitor is likely far more interested in the website’s content than its privacy settings. At the end of the day the user does not need the website to configure his or her data protection preferences; he is usually far more interested in, for example, checking the latest football results or buying a new pair of trousers from Zalando.

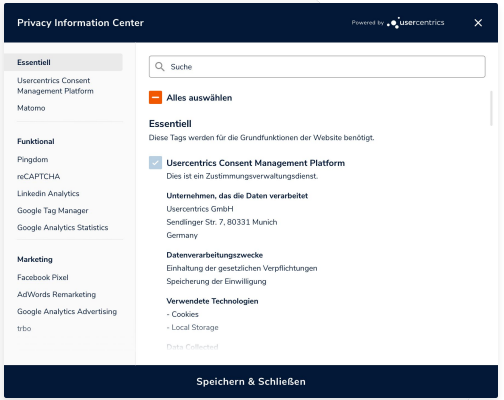
An internal Usercentrics evaluation (as of April 2020) showed: Across all sectors, most users (97.82%) interact exclusively with the first banner level (first layer) and select hardly any granular settings or adjustments to the privacy settings (< 3%).

Figure 2: Interaction rate with the Usercentrics CMP

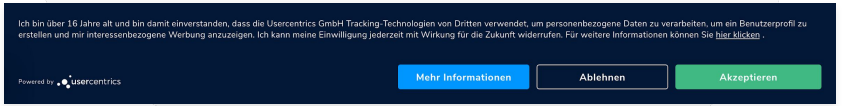
Privacy Settings (Side): **1.56 %**



Privacy Information Center: **0.31%**



Privacy Banner: **97.82 %**



Rest: **0.31 %**

What does opt-in optimisation mean?

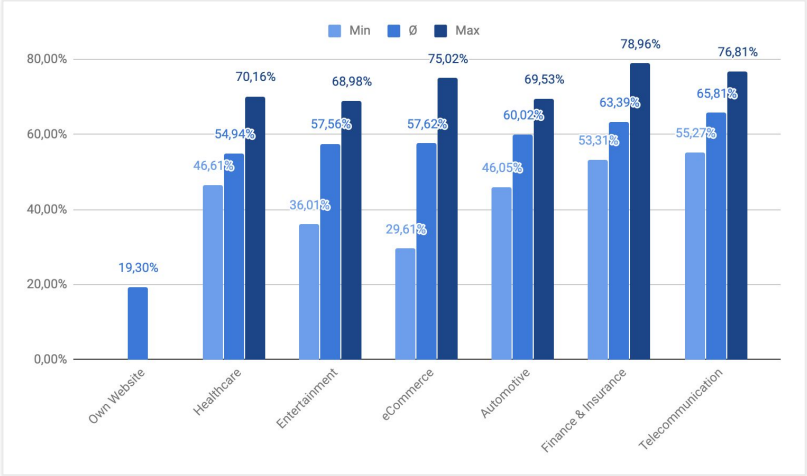
In a direct comparison of the individual sectors, differences in consenting behaviour related to various elements of the CMP can be observed. Especially in the areas of health and insurance, website visitors utilise the granular settings options up to four times more frequently. The reason for this could be the high sensitivity of the data. There is an enormous difference in a person's private sphere between being interested in the colour of a T-shirt or a specialised type of medication.

However, considering the sector alone (such health or insurance in this instance) is not enough to draw hasty conclusions from this number. The biggest driver for an increased opt-in rate is and remains the interaction with the website's visitors.

Generally, the data do not point to any trend showing the sector to have significant influence on the opt-in rate.

What is significant is the increasing number of customers achieving positive results with AB Testing. The results are higher opt-in rates of up to 20 percentage points from 54.99% to 75.02%. This represents an increase of 39% in consent actually granted.

Figure 3: Consent behaviour in various sectors



Source: Usercentrics Analysis (41 CMPs, 106,109,588 unique visitors), April 2020

Summary: The most important points

1

According to General Data Protection Regulation (GDPR), website operators require a legal basis for the use of technologies such as cookies, pixels etc. (Article 6 GDPR or, where applicable, Article 9 GDPR). This is generally speaking the user consent.

2

The opt-in rate is becoming a new KPI in marketing and its optimisation a new marketing discipline.

3

Achieving the first interaction with a website visitor is the key to a high opt-in rate as the visitor is likely far more interested in the website's content than its privacy settings.

4

Ensure that visitors actually interact with your banner. An internal Usercentrics evaluation (as of April 2020) showed: Across the sectors most users (97.82%) interact exclusively with the first banner level (first layer).

Strategies and best practices for opt-in optimisation

Two aspects play a decisive role in opt-in optimisation:

Design optimisation

- Focus on the banner
- Colour adjustments
- Placing the privacy solution on the website

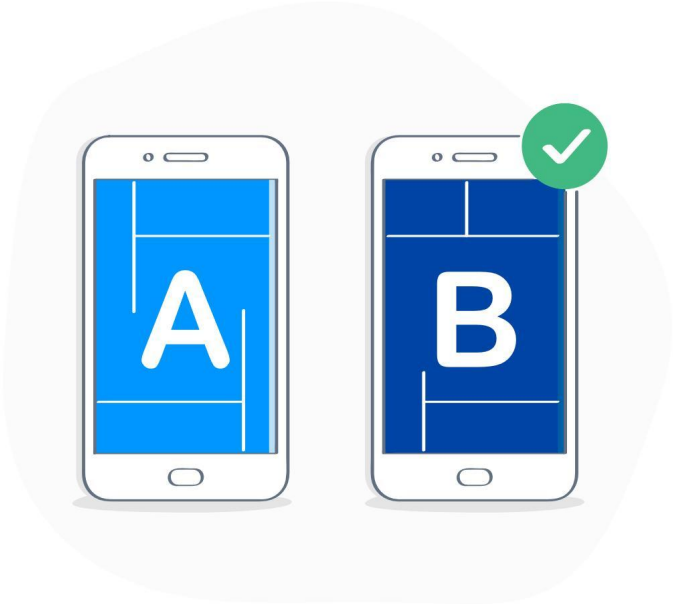
Technological optimisation

- Running the privacy solution programmatically
- Contextual opt-in
- Incentivised opt-in

Best Practice: AB Testing

AB Testing

Thorough testing is indispensable if you wish to realise the full potential of your opt-in rate. The most common method for this purpose is AB testing. The term AB testing (aka split test) describes the direct comparison of two or more variations of a privacy banner which differ from each other in terms of their colour, appearance or position. These are randomised and presented to user groups of equal size so that an analysis can be undertaken after a predefined time period as to which settings favour higher opt-in rates or which settings would lead to increased opt-in rates.



Legal Fact Check

Is offering incentives to opt in compliant with GDPR?
The significant factor with incentives is the extent to which the consent is voluntary. Depending on the scale of the advantage realised by an incentive, this may no longer be the case. However, the voluntary nature can be confirmed by incentives typical in the e-commerce sector such as free shipping or small discounts.

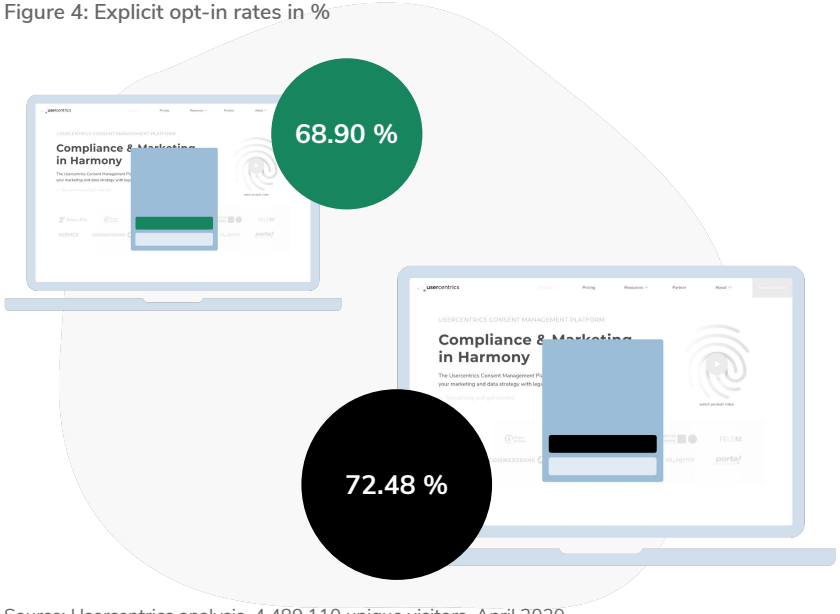
Best Practice: Colour Design

Colour Design

As is typical for many online marketing strategies, a technique known as “nudging”, i.e. the subconscious control and influence over the user’s decision making process, is used in the configuration of the privacy solution. By accentuating certain fields with certain colours, attention can be diverted to the “Accept” button and the user motivated to give consent.

Furthermore, if such eyecatchers are created in accordance with the corporate design, this leads to a harmonious overall look as well as increased total opt-in rates.

Figure 4: Explicit opt-in rates in %



Source: Usercentrics analysis, 4,489,110 unique visitors, April 2020

Legal Fact Check

Does the GDPR allow “nudging”?
Yes, provided the user still has the ability to make an informed decision! The influence is never allowed to be so great such the user can no longer freely decide. With regard to the colour design it may be assumed that an informed decision is nevertheless possible.

Best Practice: Placing and Appearance

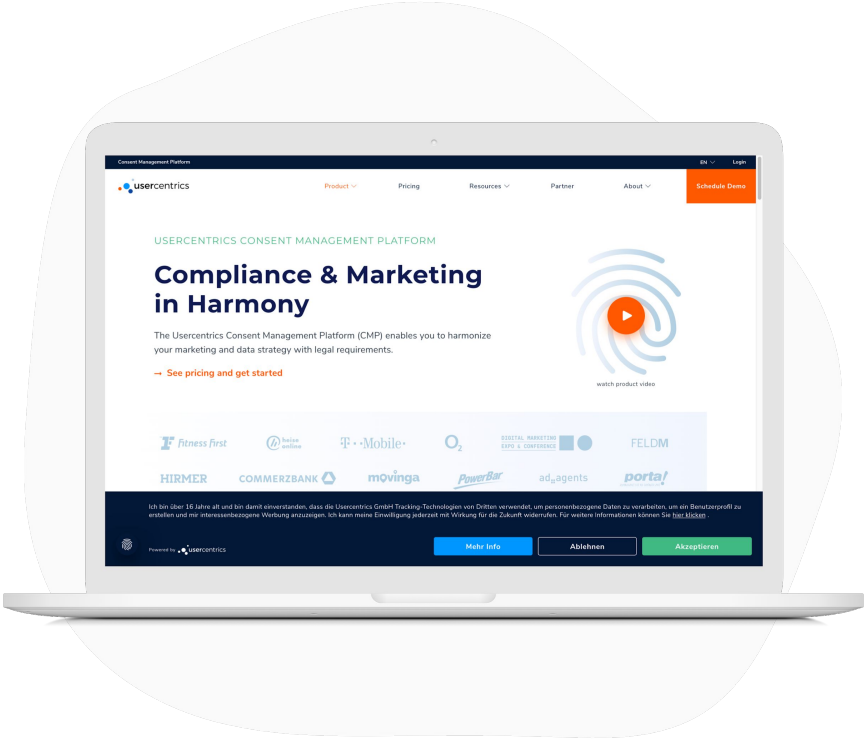
Placing and Appearance

Numerous variants are also possible with the placing of the cookie banner. Important: The links to the data privacy statement, general terms and conditions and the company's legal notice may not be hidden by the banner under any circumstances!

1. **Permanent:** With this variant the banner remains where it has been placed for as long as the user takes to provide consent to the use of cookies, or reject their use.

2. **Temporary:** Here the banner disappears as soon as the user begins to scroll through the website.

Each placement or appearance form brings with it advantages and disadvantages. While "permanent" variants lead to increased opt-ins as users are constantly reminded to provide consent, "temporary" banners score higher in user-friendliness as the banner is not perceived as intrusive. However, the danger here lies in users leaving the website without having provided consent.



Best Practice: Positioning and Design

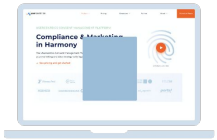
Positioning and Design – Cookie Banner vs. Privacy Wall

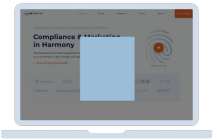
There are two basic types of banner. The classic banner at the top or bottom edge of the screen and a field placed in the centre. In addition it is possible to create an overlay for both banner types, i.e. the rest of the website is darkened until the cookies are accepted, rejected or other settings configured - that is until interaction with the banner occurs.

Our internal analysis shows: The opt-in values from the use of a privacy wall exceed those from classic banners by around 10%. While 52.19% provide consent with the privacy banner, it increases to 62.75% with the privacy wall. There's more: With a classic banner without overlay 9.76% more opt-ins can be obtained (68.63% with overlay vs. 78.39% without overlay).

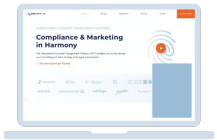
Our tip: If you wish to use a classic banner, you should place it at the bottom right of your webpage. Our evaluations show that doing so achieves the highest opt-in rates (8.85%).

Privacy Wall	62.75 %	VS.	Privacy Banner	52.19 %





without overlay	78.39 %	VS.	with overlay	68.63 %



Banner to the right	60.51 %	VS.	Banner below	51.66 %

Source: Usercentrics 578,586 unique visitors

Best Practice: Other variables

Design

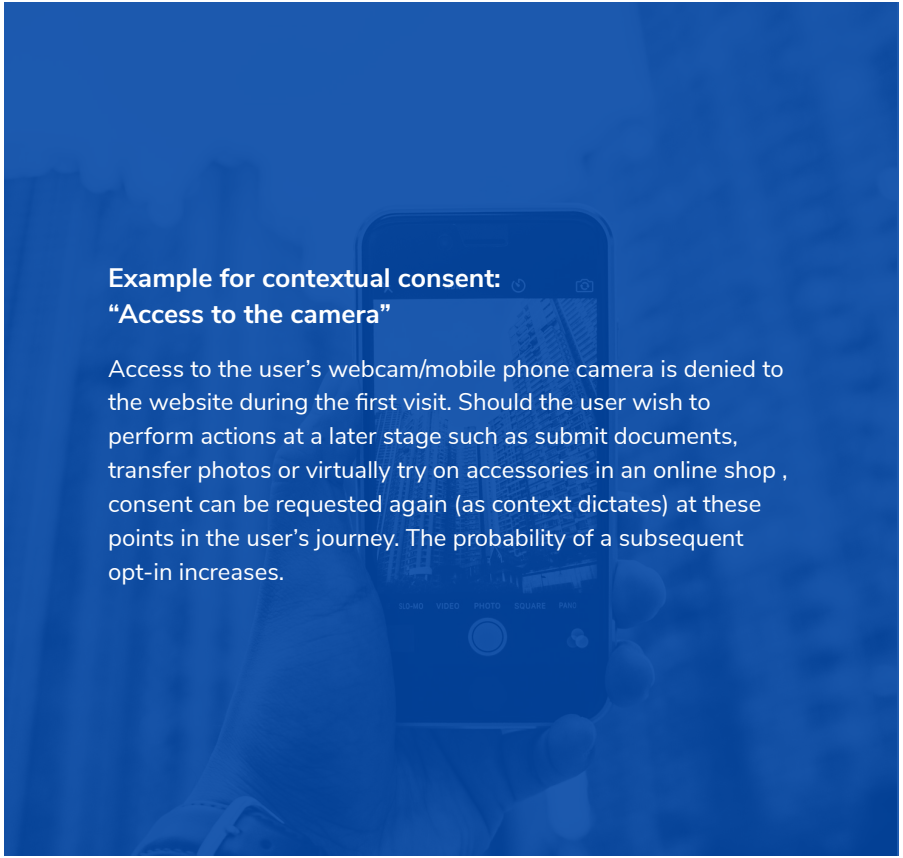
Selection options Offering a “Reject” button vs. Rejecting/changing via a link in the information text

Tonality/wording: The language or language style must be customised as much as possible to the target group and contain terms with positive connotations.

Technical options

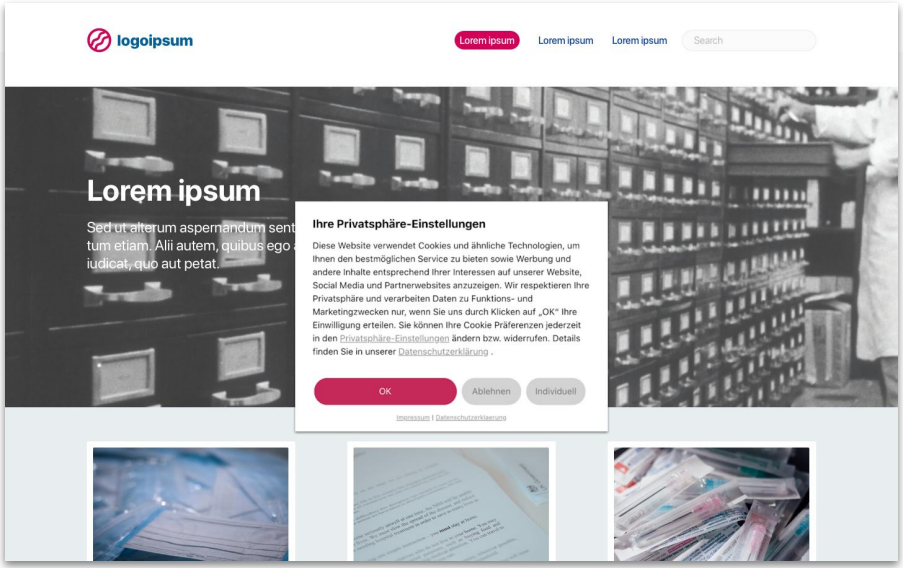
Contextual consent: A Usercentrics analysis shows that most website visitors only interact with the first banner (First layer) and detailed privacy settings are hardly viewed at all. Most banners already work by the principle of requesting consent once, during the first visit to the website.

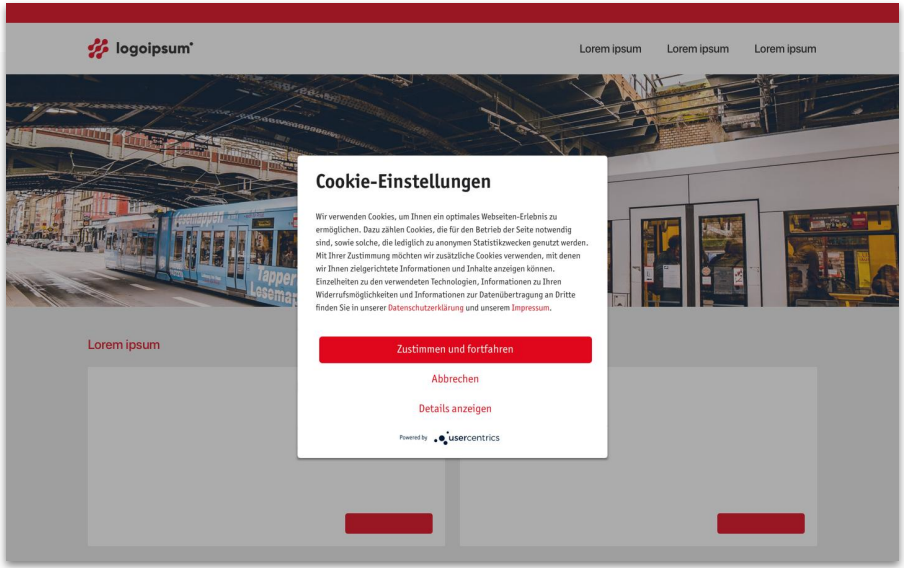
There are, however, cases in which it makes sense to work with contextual consent. Here the user is once again asked to provide consent at a specific point during the website visit. Consent which was not provided the first time around can be obtained retrospectively, thereby increasing the opt-in rate.



Practical Examples

What does a data protection compliant cookie banner still capable of achieving a high opt-in rate look like? We will show you below, using practical examples, which possibilities exist in banner design. These cookies have a few things in common in addition to the comparably higher opt-in rates: The reference text is easy to read and contains all necessary information for the user. There is an option to reject cookies directly and settings can later be revoked or adjusted. Furthermore, the privacy wall is used.





Summary: The most important points

1

The opt-in optimisation depends on design and technological factors.

2

Thorough testing is indispensable if you wish to realise the opt-in rate's full potential.

3

Options for design optimisation: Colour adjustments to match with the corporate design or emphasis of elements, placing of the privacy solution on the website (cookie banner vs. privacy walls, use of overlays etc.)

4

Options for technological optimisation: Running the privacy solution programmatically, contextual or incentivised opt-in

Checklist: How to optimise your opt-in rates

I. Design Aspects

- ✓ Make use of the privacy wall and place your banner in the centre
- ✓ Use your CD/CI as orientation during the design process.
- ✓ Do not accentuate the banner using an overlay -i.e. by darkening or blocking the background
- ✓ Use language customised for your target group

II. Technical Aspects

- ✓ Reduce the “no action” rate by repeatedly reminding website users to provide their consent (within reason)
- ✓ Request contextual consent where appropriate
- ✓ Offer incentives for opting in

III. General Tips

- ✓ Utilise the possibilities of AB testing
- ✓ Consider the possibility of building in a “Reject” button → for more legal certainty, transparency & user trust

Key Takeaways & Conclusion

Key Takeaways

Opt-in rates can be increased by up to 39% with the help of AB testing. Users interact almost always at the first banner level only. As the figures show: 97.82% of 106,109,588 make their opt-in decision in the first banner only. The privacy wall achieves more opt-ins in comparison to the banner. If you do decide to use a cookie banner, the best opt-in rates will be achieved by placing it at the bottom right of the screen. The colour design of the banner in the personal corporate design leads to an increased opt-in rate.

Do's	Effect
Use a binary solution instead of a category solution.	**+21.49 % points**
Use your CI in the privacy wall	**+20.03 % points**
Use a privacy wall, not the banner	**+10.56 % points**
Do not use an overlay, if you are using a privacy wall	**+9.76 % points**
Use the colours of your own CI when designing the buttons	**+3.58 % points**

Use opt-in reports and the possibilities of AB testing

Conclusion

Absent or questionably obtained user consent has enormous consequences for companies. In addition to large fines, there also looms the huge risk of losing user data due to court-ordered deletion because the data was not obtained in compliance with applicable laws. Furthermore, there is no correlation between conformity and opt-in rates. Which means: Whether or not you have high opt-in rates is not necessarily due to the absence of a "Reject" button. For example, there are CMPs which generate a higher opt-in rate using a privacy wall with a "Reject" button (70.16%) than a banner without a "Reject" button (21.25%). Get away from the idea that dark patterns are required to achieve high opt-in rates and remain compliant.

Tilman Harmeling
Entrepreneur in Residence

Usercentrics GmbH
Sendlinger Straße 7
80331 Munich, DE

The perfect tool for your Privacy Management

With the Consent Management Platform from Usercentrics you can obtain user consent in compliance with the law whilst simultaneously optimising your opt-in rates step by step.

Obtain consent in compliance with applicable laws

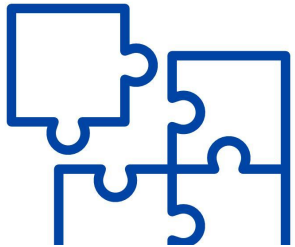
Legal certainty through compliance with all legal requirements (GDPR, ECJ, IAB Transparency and Consent Framework).

Optimise opt-in rate step by step

Increase the opt-in rate with features such as AB testing, contextual consent and opt-in reporting

Individually adjustable design

Wide selection of ready-made layouts from the theme gallery or flexibly adjustable design in accordance with your own CI



Compatibility with all widely used marketing tools

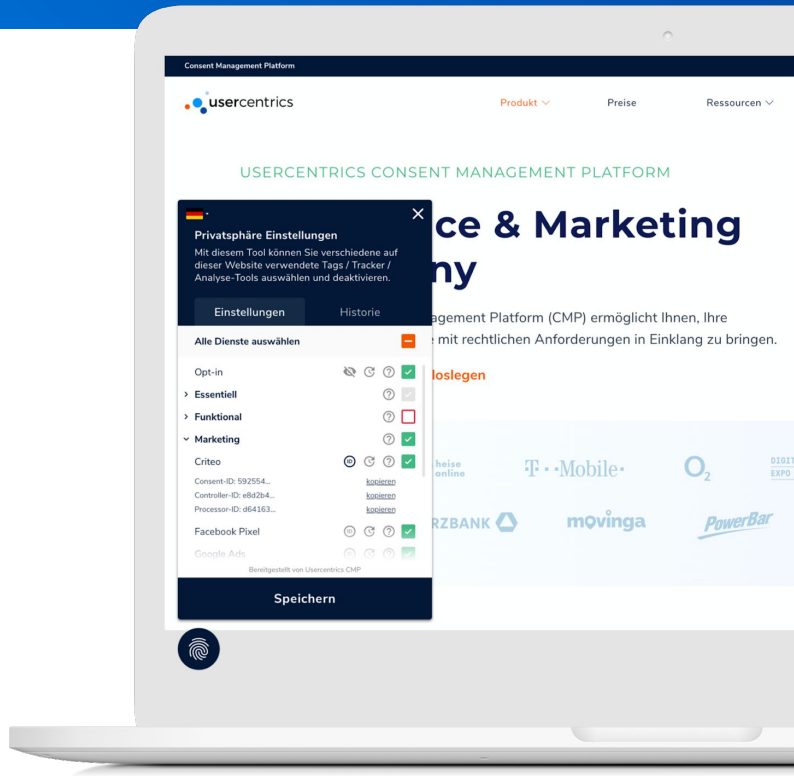
The Usercentrics CMP is compatible with all conventional tools such as analytics, AB testing, tracking or retargeting.

Our tip: Use “inhouse tracking” whenever possible. Use tools such as Matomo which can host the data on your own server and do not pass it on to third parties. According to current assessments of the German Data Protection Conference (DSK), such tools come under the legitimate interest category providing the data is not passed on to third parties.

Request free demo now

Regardless of whether you are just beginning your fact-finding with consent management solutions or are already ready to evaluate potential providers - we are happy to assist! Book a demo now at usercentrics.com/demo or get in touch with us directly to arrange a no-obligation consultation.

We look forward to hearing from you!



About Usercentrics

Compliance & Marketing in Harmony
Munich-based technology company Usercentrics is a market leader in the field of consent management platforms (CMP). The SaaS solution from Usercentrics enables companies to obtain, manage and document consent provided by users on all digital channels such as websites or apps - and achieve high opt-in rates in the process. Since its founding in 2017, the company has grown strongly and now has over 300 enterprise customers including Commerzbank, Fitness First and Telefonica.

Usercentrics GmbH
Sendlinger Straße 7
80331 Munich

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