Why current pay-or-okay models **violate the GDPR-by-design**

Introduction

In the last couple of months, you may have visited a website or platform where you were given the choice to accept cookies or become a paid subscriber. This so-called **pay-or-okay business model** allows users to either pay for content or services upfront, or agree to provide value in another way, typically by sharing personal data, viewing ads or engaging with promotional content.

As the pay-or-okay model seems to offer a balance between user control and revenue, it has been adopted by quite a number of EU publishers and platforms, especially in digital media. At the same time, the model raises questions about user privacy, data ethics and whether it places an undue burden on consumers to sacrifice privacy for 'free' access – is this privacy for the rich only?

Apart from discussions around ethics and society that publishers may wish to have, there's one concrete question publishers need to ask themselves: **Is this model compliant with EU (e-)privacy regulations?**

In this piece, we answer that question. **We explain why these models fall short of (e-)privacy standards. We also introduce privacy-friendly advertising alternatives already available in the market**. If you're active in the advertising industry and serious about protecting user data and doing lawful and ethical business while still maintaining a profitable model, use this piece to help you rethink your strategy.

This piece is co-written by:

- Opt Out Advertising, a pioneer in consentless advertising, committed to developing and implementing innovative advertising solutions that prioritise and protect individual privacy; and
- De Roos, a leading Dutch law firm that supports companies operating at the intersection of law and technology.

This piece explains:

- What pay-or-okay models are and how they work, including the current underlying programmatic advertising system (real-time bidding, RTB);
- Why – due to the current RTB practice – pay-or-okay models cannot operate in compliance with the GDPR (meaning both the EU GDPR and the UK GDPR) and the EU e-privacy legislation; and
- What privacy friendly online advertising alternatives are available on the market, including Opt Out Advertising's consentless ad server.

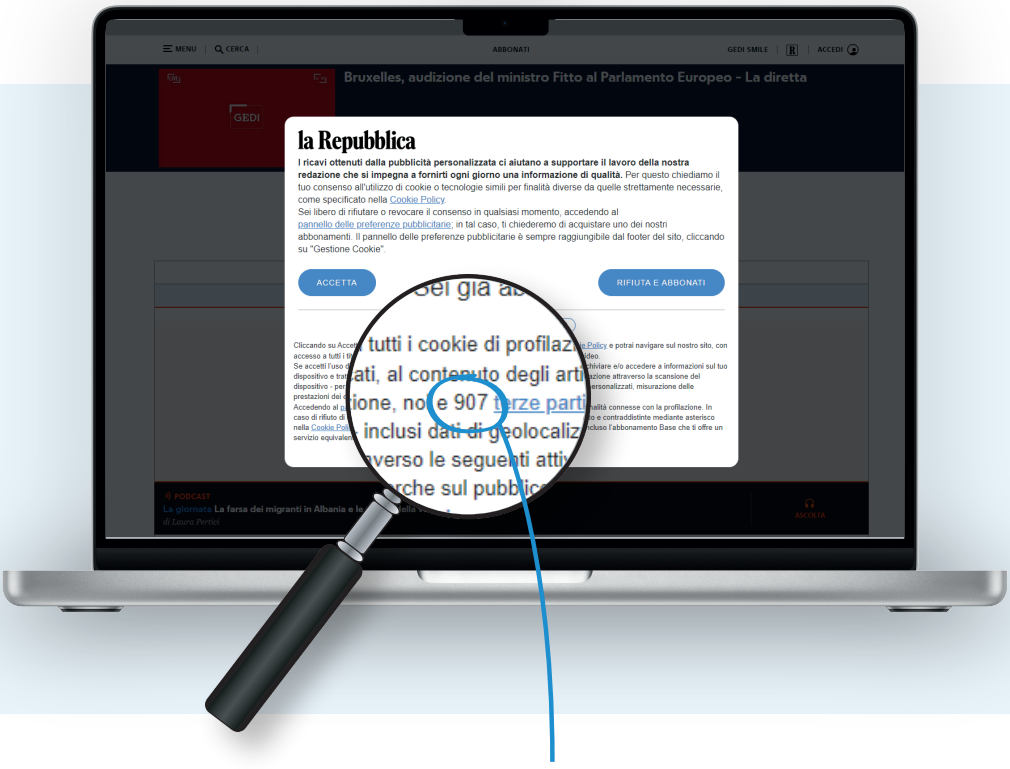
Content

DE ROOS | opt out

1. Current **pay-or-okay** business models

Next to Meta's Facebook and Instagram services, the pay-or-okay business model is widely used amongst **EU online newspapers**.

You either (1) pay a subscription amount, roughly ranging from EUR 1 to EUR 11 per month, or (2) consent to tracking cookies and personalized ads in 'cooperation with our partners'. The amount of partners usually ranges from 100s to almost a 1000, e.g. Der Spiegel (155), Bild.de (279), El País (861) and La Repubblica (907). Interestingly, the main French newspaper (Le Figaro) does not operate with the pay-or-okay model. The same applies to the main Dutch (Telegraaf and Algemeen Dagblad), Polish (Fakt) and Romania (Adevărul) newspapers. However, Dutch weather channel Buienradar (116 advertising partners) does operate a similar pay-or-okay model. [1]

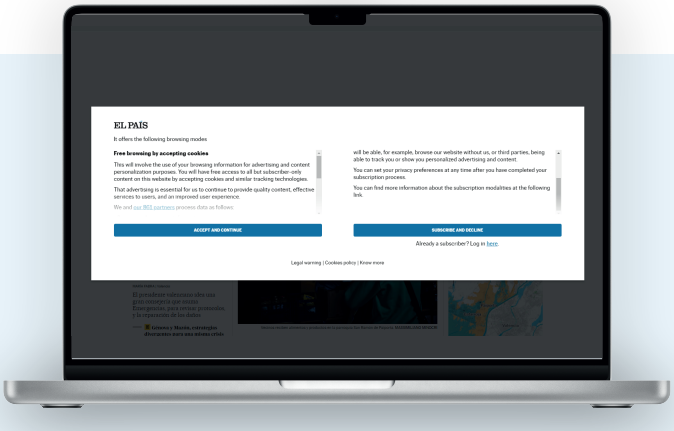


With consent (okay)
you agree to tracking cookies and personalized ads in cooperation with 907 partners

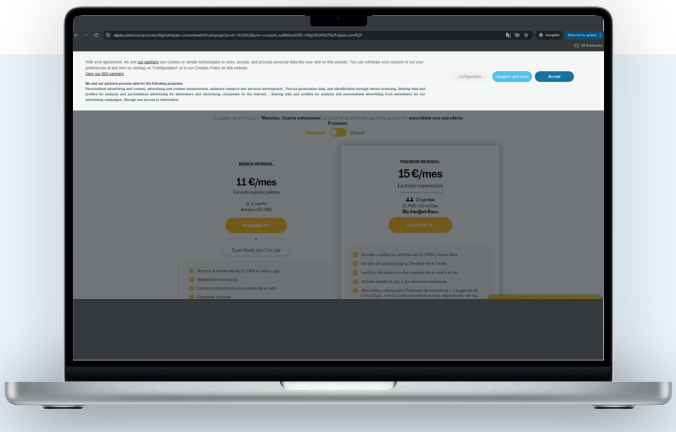
[1] In the UK the use of pay-or-okay models for newspapers is widespread, see for example The Sun, Daily Mail, Mirror, Express and Independent. While the UK still operates a UK GDPR and also e-privacy legislation based on EU law, Brexit means that EU interpretations of these laws are no longer followed. We will therefore leave the UK out of this discussion.

1. Current **pay-or-okay** business models

EL PAÍS



Pay-or-Okay banner at El Pais



Don't want to share your personal data?
Pay €11 per month to read the content

Therefore, smaller publishers might assume they can walk away with a pay-or-okay model without violating (e-)privacy laws.

Pay-or-okay is not new, especially not for online newspapers. In 2018, an Austrian newspaper was the first to operate a cookie-or-pay wall.[2] This makes sense. Print media revenue has declined significantly as readers have shifted to online content. Advertising revenue, which traditionally supported newspapers, has also decreased due to the spread of ad blockers and the dominance of major digital advertising platforms like Google and Facebook, which capture a large share of online advertising euros.

Also, with individuals becoming more privacy savvy and rejecting more cookies, the introduction of a 'pay' option seemed necessary. Even though, according to research, only 1% of users chooses to pay. when confronted with a choice between paying or 'okaying', this still generates a generous income, with the average subscription price being 200% more that the revenue of cookies.[3]

Recently, the business model has been subject of broad discussion, mostly due to Meta's shift to pay-or-okay. The European Commission already found Meta's model to violate the newly adopted Digital Markets Act (DMA):Meta, while holding a dominant position in the market, forces users to consent. For a similar reason, the European Data Protection Board (EDPB - as a representative of all EU data protection regulators) issued an opinion that Meta, due to its dominant position, should offer a third, free option without data collection for behavioural ads. As smaller publishers are not subject to the DMA and not holding a dominant position in the market, these findings do not equally apply to them. Therefore, smaller publishers might assume they can walk away with a pay-or-okay model without violating (e-)privacy laws.

This assumption is false: The issue with pay-or-okay models is the current working of the 'okay' option. The processing of personal data that takes place when okay is clicked violates the GDPR and e-privacy laws. The introduction of a 'pay' alternative does not take this violation away.

In the next section, we will first explain what kind of personal data processing takes place when you click okay. After that, we explain how this violates the law.

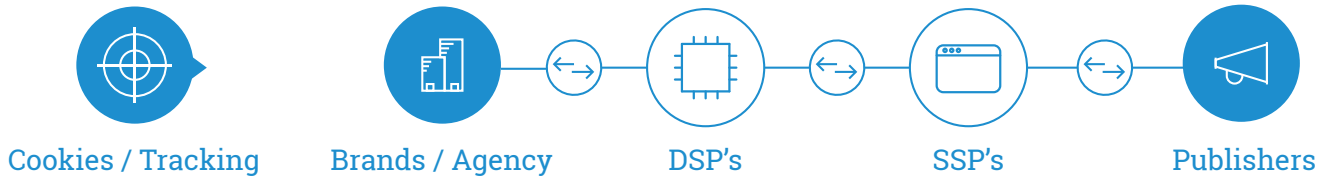
[2] https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.html

[3] See "Pay or Okay": 1,500 € a year for your online privacy? and Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls

2. The technology behind pay-or-okay
What happens when you click 'okay'?

The Real-Time-Bidding-System **(RTB)** is the backbone of the modern online advertising ecosystem. RTB is estimated to be operating behind 80% of websites that use advertising as a source of income and the annual revenue directly attributed to it is likely to lie around $17 billion globally.[4]

RTB allows digital advertising space to be bought and sold in real-time through automated auctions, with millions of specific online user profiles being auctioned daily across a vast network of thousands of adtech companies connected to the system. Each time a user views a webpage which includes RTB-technology, the advertising space on that webpage is automatically filled with an ad targeted at that user.



Once a user clicks on 'okay' in the pay-or-okay banner, the RTB-system starts running. In short, it works as follows:

a) The ad server of the publisher sends an ad request to the supply side platform (SSP) which launches the request in a so-called ad exchange to call for bids. Such bidding request includes various pieces of data including the user's **demographic information (estimated age, gender, location), browsing history, device information, behavioural data (clicks and hover time), the nature of the webpage they are visiting, time of day, IP address and device data.** These often hundreds of data points have been collected through cookies and other technologies, which 'break in' in the communication between the website and the user.

b) The ad exchange is a marketplace where advertisers can bid to have their advertisements published in the advertising space. The ad exchange broadcasts the bid request to multiple of these potential advertisers or their demand-side platforms **(DSPs)**.

c) These parties then evaluate the bid request based on their estimated value of the ad impression and respond with a bid amount that reflects how much they are willing to pay to display their ad to that specific user. They use algorithms to assess the likelihood of the user's interest in their advertisement based on the data provided.

d) The ad exchange selects the highest bidder, and that ad is sent to the website to be loaded into the user's browser, displaying the ad to the user

This entire process, from the user's initial website request to the ad being displayed, happens in real time, typically within 100 milliseconds. After the ad is served, data regarding the ad's performance (clicks, impressions, engagement) is fed back into the RTB eco system for the parties involved to refine their bidding strategies for future ad placements.

The parties mentioned above, e.g. the SSPs, the ad exchange, the DSPs and any ad tech and data companies involved are the 100+ parties as mentioned in the several pay-or-okay statements of the newspapers described in chapter 1.

As you can imagine after reading the RTB-ways-of-working, the RTB system involves large-scale and opaque collecting and sharing of vast amounts of detailed user data between them – this is hardcore online tracking and targeting, across sites, apps and devices.

[4] https://www.thebusinessresearchcompany.com/report/real-time-bidding-rtb-global-market-report

3. E-privacy consent and GDPR principles

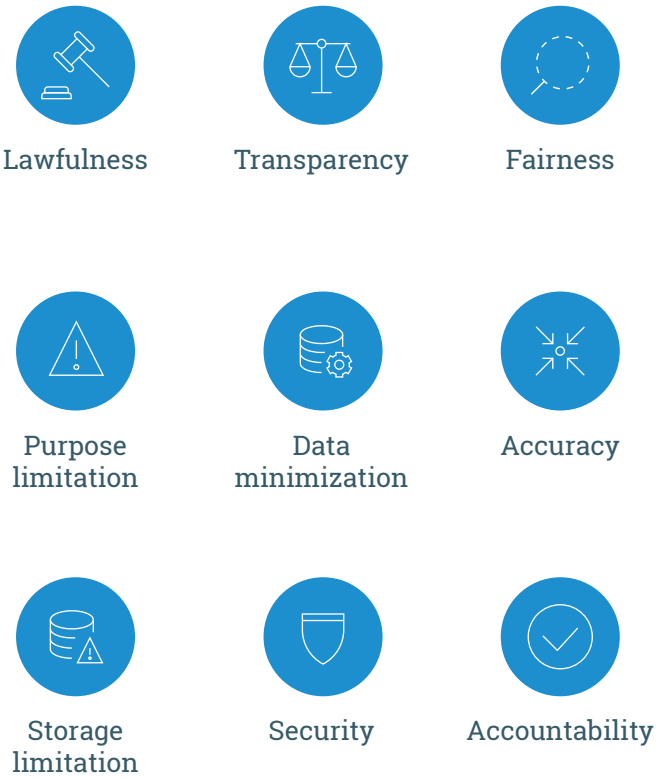
EU e-privacy laws

aim to guard the secrecy of online correspondence. You do not have to expect that your letter is being opened by the mailman or another party involved in the delivery of your mail communication. This principle of secrecy also applies in the online world. E-privacy laws allow for exemptions to this rule, e.g. where interception is required for the functionality of a website or when GDPR-style consent is obtained. As cookies and similar technologies used for online advertising intercept communications (i.e. break confidentiality) while not being required for the functioning of a website, consent is required to comply with e-privacy laws. The obligation to get such appropriate consent sits with the publisher.

The GDPR

is a principle based regulation, making so-called 'controllers' of personal data accountable for compliance. Controllers are the parties that have a decision-making power over the 'why' and 'how' of data processing. You can assume that the majority of the RTB partners are controllers of the personal data they receive in their role as participant in the RTB system as most have their own business purposes for building, sharing or analysing online user profiles.

The GDPR principles which we will describe below: lawfulness, transparency and fairness, purpose limitation, data minimization, accuracy, storage limitation, security and accountability.



Lawfulness

Parties active in online advertising work with consent as a tool for compliance. In theory, this should kill two birds with one stone – valid GDPR consent allows for breaching the secrecy of e-communication as described above and also provides for the GDPR required lawful ground. For such consent to be valid (i.e. 'lawful'), it should be, amongst others, 'specific' and 'informed'. This is the first violation: the one-click consent for multi-purpose, multi-party, multi-data, hyper-technological processing can never achieve this GDPR threshold. As such, the GDPR required lawful ground is missing, as is an e-privacy exemption to intercept online behaviour and other communications. This is the core reason why RTB and thus the current version of pay-or-okay violates the laws.

NB: The main point of the scrutiny around Meta's pay-or-okay model also focusses on consent, and then mostly around the other GDPR requirement for valid consent, which should be 'freely given'. Do you feel sufficiently free to choose between your data being used by Meta for personalized advertising in your feed vs. paying EUR 4,99/month? The European Data Protection Board suggests for Meta a third option to choose – free and without data sharing. But even then our point remains: Clicking consent does not achieve GDPR compliance on the lawfulness requirement, as the user is in no way in the position to understand what happens when they click consent.

3. E-privacy consent and GDPR principles

Transparency

Controllers should also be transparent to individuals about data processing, meaning that any information and communication relating to the processing of personal data should be easily accessible and easy to understand through the use of clear and plain language. **This includes information on the identity of the controller and the purposes of the processing and 'further information to ensure fair and transparent processing in respect of the natural persons concerned'.**

For targeted advertising through the RTB model, transparency is usually aimed for by including links to the privacy notices of all parties involved in the consent statement. With the 100s of 'partners' involved in RTB – expecting users to navigate these partners 100'+ privacy notices is unrealistic and therefore also violates the GDPR's transparency principle, which requires clear, simple, and easily accessible information.[5]

Control over personal data is a purpose of the transparency principle of the GDPR: If you know what personal data is processed by whom and for what purpose, you can ask questions and have your data adjusted or deleted where necessary or appropriate. By design, through the 100s of data points and parties involved, the current RTB system fails to provide for such user control.

Fairness

Given the complexity of RTB, achieving true GDPR transparency and control is probably never really possible. The question is whether it is fair that this 'problem' currently rests with individual users and not with the business making millions on user data.

This unfairness is actually also a GDPR violation in itself, as fairness is a GDPR principle. Under the GDPR, fairness means that personal data should processed in a way that respects the rights and expectations of users without harmful or disproportionate impact. Such fairness should ensure that users are not misled or coerced and that their data is handled in ways that they would reasonably expect. As described above, unfairness is designed into the current RTB system. This is also shown by the imbalance between the fact that intimate profiles of individual users are floating around uncontrollably through the RTB system, and the ignorant user is presented with an ad which has the highest change of click and buy. This is not a fair deal. Of course, publishers have a right to be paid for their newspaper content and such price can be set by different factors which may not always feel fair. However, when such business practice violate the GDPR and thus the right of privacy, this unfairness becomes unlawful.

Specifically for RTB, IAB Europe (the European trade association for the digital advertising and marketing ecosystem) established the Transparency and Consent Framework (TCF) containing the technical and organizational measures for managing e-privacy (consent) and GDPR (consent and transparency) requirements. Through the TCF framework, user consents are managed, adtech companies 'whitelisted' and purposes of use and links to the privacy notices published. While addressing some technological complexities in the RTB framework around consent and transparency, the TCF does not fundamentally solve any of the issues addressed in this memo. **No valid consent, no meaningful transparency and no fair processing is achieved.**

The other six GDPR principles

Valid consent would have largely solved compliance with e-privacy laws and the first principle of the GDPR. However, the end-to-end data processing that takes place within the RTB ecosystem needs to comply with the other principles of the GDPR as well. These include: **purpose limitation, data minimisation, accuracy, storage limitation, security and accountability.**

Purpose limitation means that user's personal data can be processed for specific, explicit and legitimate purposes only. Further processing for other purposes is only allowed when this is 'compatible' with the first purpose. While the TCF lists standard purposes for processing, and therefore takes an aim at complying with the 'specific' and 'explicit' purposes, there is no control over the personal data that is further processed by parties connected to the TCF. Also, the purposes as described in the TCF are in our view insufficiently informative. How specific and explicit is the description for the purpose 'Store and/or access information on a device' (TCF Purpose 1), 'Create profiles for personalised advertising' (TCF Purpose 3) or 'Understand audiences through statistics or combinations of data from different

[5] In 2008, researchers estimated that reading privacy notices of all the websites you visit in a year would take more than a week of non-stop reading or more than half an hour every day, what happens when you add the 100s of privacy notices of the website that you do not visit, but that do know about you through RTB. In relation to comprehensibility of online privacy notices, also a GDPR requirement to achieve transparency, this New York Times article is hilarious.

3. E-privacy consent and GDPR principles

sources' (TCF Purpose 9), especially when you take into account the number of data points and parties involved?

The **data minimisation principle** requires controllers to only collect personal data that is adequate, relevant and necessary for its specific purposes. It is up to the participants in the RTB ecosystem to ensure that the data they collect is necessary for the purpose they have (i.e. – their specific, explicit and legitimate purposes). It is up to the partners in the RTB system to decide why the 100s of data points collected are adequate, relevant and necessary. This seems like an herculean exercise given the number of data points and purposes, and in our view undoable – the absence GDPR requirements such as lawfulness and fairness makes it impossible to nevertheless comply with this data minimisation principle.
The parties in the RTB ecosystem should ensure processing of accurate personal data. **Accuracy** is not always the most important or clear GDPR principle – it gets more serious once the consequences of inaccurate data are tangible for the individuals involved. When you look at it from a far, the worst that can happen with inaccurate data with RTB is that you get an advertisement of a product or service which you are in no way interested in. That doesn't sound too bad. However, intimate profiles collected and further enriched through RTB are creepy, whether inaccurate or not (for example: receiving pregnancy related ads when you reach a certain age). It is up to the participants in the RTB ecosystem to ensure that they achieve an acceptable level of accuracy.

The GDPR's **storage limitation principle** requires controllers to keep personal data only for as long as necessary for their purposes. E-privacy also has a role here, as the retention period of the cookie needs to be included in the information provided to users. This often absent or set on indefinite. Where such cookie retention periods are included, these seem usually far too long (e.g. 3 or 10 years), especially in light of the purpose (targeted advertising). And this only applies to cookies and other technologies placed on the user's device. What happens to the data floating through RTB? How long is this retained? The TCF also doesn't help here, as it simply requires participating adtech companies to put in place 'reasonable retention periods', without any further guidance.

That RTB obviously violates the **confidentiality, integrity and availability – or in short – security principle** is already clearly described by the Irish Council for Civil Liberties.[6] In short: "RTB is the biggest data breach ever occurred". The TCF doesn't solve this problem as IAB Europe is not in a position to technically limit the way data is used after it starts flowing within the RTB-framework. The failure of supervisory authorities to adequately respond to complaints in this regard, does not take this violation away.

Accountability is the GDPR's final 'principle', requiring organizations to consciously take measures to comply with the GDPR based on their adequate knowledge of the data processing activities and the risks associated with such processing. Accountability also includes documentation – you need to be able to demonstrate that you comply. The problem with RTB is that – due to the massive web of companies connected to it – no company can ever be truly held accountable. For example: it is undoable to validate consents across the network, ensure sufficient security of all vendors or audit data retention. There is no single organisation in control or responsible of the whole RTB system (also not the IAB, despite their role). Again, the question is – on whose shoulders rests this problem?

RTB is already under scrutiny

This article does not describe a stand-alone opinion and there is hope for privacy compliant online advertising. RTB is facing increased scrutiny to meet key e-privacy and GDPR requirements including valid consent and transparency. The TCF is criticized in RTB's slipstream. While both RTB and the TCF have been the subject of several actions by individuals, regulators, consumer groups and NGOs, the most significant is the ongoing enforcement of the Belgian data protection authority against IAB Europe (link). A final decision by the Belgian Market Court is expected in one or two years.

In the meantime, specific RTB vendors have been called to action as well - for example Criteo and Microsoft which were both ordered by the Dutch court to obtain valid consents. Criteo also received a EUR 40 million fine from the French Data Protection Authority.

[6] https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf#page=9

3. E-privacy consent and GDPR principles

Conclusion

With the above, we hope to have taken away the understanding that pay-or-okay models can operate legally. To recap:

1. Pay-or-okay in itselfdoes not violate the GDPR and e-privacy laws.
2. However, behind the 'okay'-option, RTB is currently operating. This enables advertisers to compensate for their missed income via paid subscriptions.
3. RTB violates GDPR-by-design and pay-or-okay-models provide no solution for this violation.

The question is **what are the alternatives?**

4. Which **privacy-friendly advertising models** are available on the market?

Despite recent news about Google retaining third-party cookies, advertisers and media agencies might wrongly assume that the debate over cookies has been resolved. However, this is not the case as informed consent is still required, even when third-party cookies are used.

As **privacy awareness is growing among users**, privacy-compliant advertising is not just possible, but increasingly necessary, and several alternative models are already being successfully implemented.

One of the most effective alternatives is a **consentless advertising** ecosystem that completely removes the need for personal data, cookies and other personal identifiers. By adopting systems that rely on non-personal data and contextual targeting rather than behavioural profiling, publishers can still monetise their content while adhering to existing and developing privacy standards.

How can the Opt Out platform help publishers serve ads in a privacy-focused way?

Opt Out Advertising's unique, self-service ad server delivers compliant, effective advertising in a fully privacy-focused manner, ensuring that publishers are in total compliance with GDPR and e-privacy regulations, both now and in the future.

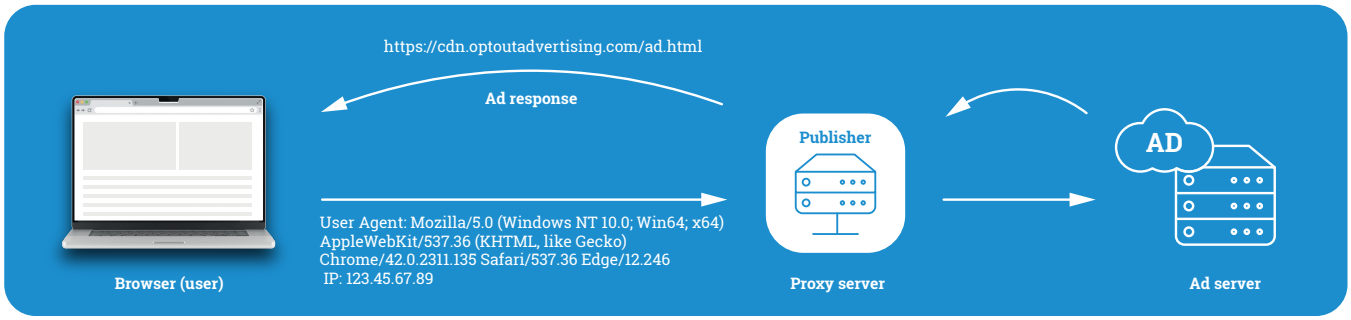
Our platform's contextual targeting solution enhances consentless advertising on a website by aligning relevant ads with the content visitors are viewing. Rather than tracking individual users across the web, **contextual targeting** focuses on delivering ads based on a page's content, the device being used or other non-identifiable characteristics (such as the time of day or weather conditions). This strategy ensures that ads complement the user experience rather than disrupting it, and that non-consenting users can be effectively engaged in a privacy-first environment.

Publishers can drive substantial revenue growth by monetising consentless inventory – ad space where visitors decline tracking. By tapping into this under-utilised inventory, the Opt Out ad server can help publishers reach their entire audience and **boost overall revenue by up to 20%**, matching the average percentage of users who opt out of tracking. This enables them to capture valuable revenue opportunities while prioritising user privacy.
Our solution also enables advertisers to bid for ad

4. Which **privacy-friendly advertising models** are available on the market?

spaces in real-time, just as they do with RTB, but without access to personal user data. The ad server does not store any personal data, but sends a creative back to the browser in the ad response, where the creative is then checked and cleaned of any cookies or identifiers.

Not only are large publishers benefitting, but smaller publishers are also leveraging privacy-enhancing technologies (PETs), such as the Opt Out ad server, to effectively deliver ads without collecting personal data.



Advertisers can instead rely on signals such as page content, ad placement and non-personal triggers to ensure their ads are contextually relevant to their audience. This not only ensures compliance with privacy regulations but also improves the user experience by reducing page load times and preventing the overwhelming amount of ad requests that come with RTB.

Consentless advertising has proven to be effective

Large publishers such as Immediate Media, The Guardian, and the Dutch Public Broadcasting (NPO) have adopted consentless advertising models, providing competitive and valuable ad spaces without relying on tracking cookies or identifiers.

This approach has proven highly effective. For example, after NPO eliminated the use of personal data for advertising in 2020, it achieved a revenue surge of 61% to 76% in the initial months compared to the same period in 2019 when it still used some consented inventory.

This success highlights the potential of an advertising model that prioritizes user privacy.

From an advertisers' perspective, a privacy-first approach unlocks new opportunities to engage with a distinct, privacy-conscious audience. **Early campaigns have demonstrated that this audience segment is highly valuable, even when personal data is not used**. In a regional newspaper campaign, a comparison between traditional real-time bidding (RTB) networks and a consentless strategy revealed remarkable results. The time spent on the page tripled compared to similar commitments on consented traditional networks.

Additionally, the quality of traffic from consentless inventory was superior, resulting in a 15% increase in subscriptions. Consistent positive outcomes have been observed across multiple campaigns, further validating the effectiveness of a privacy-first approach.

As demonstrated by pioneers in the field, there is a clear path forward.

The Opt Out platform allows advertisers to buy media in a privacy-first manner, optimizing ad campaigns without the use of personal data while achieving similar performance metrics as data-driven campaigns.

5. **Whats next?**

To close of - the EDPB has called out an industry stakeholder consultation on pay-or-okay models on November 18, requesting industry views. We will use this opportunity to put forward the notion that the EDPB should apply the law properly: requiring the advertising industry to change its business model to bring it in line with the GDPR and e-privacy rules.

Are you active in the advertising industry and want to know more about privacy savvy advertising business models or are you seeking for legal advice?

Do not hesitate to reach out!

DE ROOS | opt out