Blockchain-Enhanced User Consent for GDPR-Compliant Real-Time Bidding

Cristòfol Daudén-Esmel[1][0000−0002−4607−4035], Jordi Castellà-Roca[1][0000−0002−0037−9888], Alexandre Viejo[1][0000−0003−2342−5100], and Vicenç Torra[2][0000−0002−0368−8037]

[1] Departament d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
{cristofol.dauden,jordi.castella,alexandre.viejo}@urv.cat
[2] Department of Computing Science, Umeå University, Umeå, Sweden
vtorra@cs.umu.se

Abstract. Ensuring Real-Time Bidding compliance with GDPR and the ePrivacy Directive remains challenging. Existing solutions, like the IAB's Transparency and Consent Framework and OpenRTB, lack transparency and fail to secure legally valid user consent. We propose a blockchain-based framework that decentralizes consent management, giving users direct control. The system automates consent handling, provides immutable compliance proof, and includes a smartphone app for users to manage consent per website. Additionally, we introduce a specificity value for IAB Audience Taxonomy elements, helping users assess the privacy impact of sharing data. By enhancing autonomy, transparency, and accountability, our approach strengthens trust in programmatic advertising while maintaining GDPR compliance without disrupting the industry.

Keywords: General Data Protection Regulation (GDPR) · Real Time Bidding (RTB) · Blockchain · User Consent Management

1 Introduction

Every day, millions of users rely on free online services for information, entertainment, and communication. To sustain operations and generate revenue, most of these services rely on display advertising [9, 12, 23]. This model enables service providers (SPs) to monetize their platforms by allowing brands to target audiences through ads.

Programmatic advertising improves traditional display advertising by delivering personalized ads based on user data, including demographics, interests, and online behavior [24]. This approach strategically places ads to maximize engagement and relies heavily on tracking user activities, effectively making consumer data the "product" that fuels the online advertising ecosystem.

While programmatic advertising has gained traction due to its efficiency and targeting accuracy, it has also raised significant privacy concerns. The extensive

collection of user data has sparked debates about the balance between advertising innovation and personal data protection, highlighting tensions between effective marketing and individual privacy rights.

To strengthen data protection rights and regulate personal data processing across various sectors, the European Union introduced the General Data Protection Regulation (GDPR) in 2018 [2]. Although its scope extends beyond online advertising, GDPR has significantly impacted programmatic advertising by granting users greater control over their personal information and enforcing stricter data processing requirements.

To address the compliance challenges posed by GDPR, the *Interactive Advertising Bureau Europe (IAB Europe)*, the leading federation representing the digital advertising industry in Europe [8], developed the *Transparency & Consent Framework (TCF)* [7] to establish a legal foundation for data processing within the programmatic advertising ecosystem. A key objective of the TCF was ensuring GDPR compliance for *real-time bidding (RTB)*, the protocol that enables advertisers to bid for digital ad space in real time. One of the most widely adopted RTB implementations in Europe is OpenRTB [11], a standardized framework that facilitates communication between publishers and advertisers. The TCF was designed to align OpenRTB's personal data processing with GDPR and the ePrivacy Directive [1], positioning it as a compliance solution for the industry.

Despite its goal of facilitating GDPR compliance, the TCF is not an open-access technical standard like those published by public standardization institutions. Instead, organizations must pay an annual membership fee of 1,200 EUR to IAB Europe and comply with a set of strict policies [25]. These policies define the requirements for participation in the framework, mandating that any company involved in personal data processing, such as adtech vendors, advertisers, publishers, and other intermediaries, be listed in a centralized Global Vendor List (GVL) maintained by IAB Europe. Additionally, they regulate how user consent must be obtained, stored, and transmitted, enforcing standardized procedures through Consent Management Platforms (CMPs) that rely on cookies and other tracking mechanisms. Although this structure aims to ensure regulatory compliance, it also restricts flexibility for businesses operating outside the framework, effectively making participation in the TCF a prerequisite for engaging in compliant programmatic advertising.

While the TCF was introduced as a compliance mechanism for GDPR, its restrictive nature and centralized control have drawn criticism. In particular, concerns have been raised about whether it genuinely ensures lawful and fair data processing within the RTB ecosystem. These concerns culminated in February 2022, when the Belgian Data Protection Authority (Belgian DPA) ruled against IAB Europe, questioning the legality of the TCF in the context of real-time bidding [3]. The decision concluded that OpenRTB, as structured under the TCF, violated the GDPR principles due to insufficient legal grounds for data processing and a lack of fairness. This ruling carries significant implications for the future of programmatic advertising in Europe, as it challenges the industry's

reliance on consent-based frameworks and raises broader questions about the legitimacy of current data-driven advertising practices.

1.1 State of the Art

Research on digital advertising has primarily focused on three key areas: i) improving ad targeting and revenue generation from the advertiser's perspective; ii) analyzing the impact of digital ads on users, including consumer behavior, perception, and privacy concerns; and iii) exploring alternative strategies that reduce reliance on personal data while maintaining advertising effectiveness.

The first area, which has been the focus of much of the existing research, explores multiple strategies to enhance ad delivery and personalization. Some studies analyze user behavior through click-through logs to improve ad click-through rates [27, 28], while others examine the broader ad exchange ecosystem, investigating time-dependent patterns in impressions, bids, and conversion rates to refine RTB mechanisms [29]. Additional approaches include recommendation systems that balance ad revenue and user experience [15], dynamic budget allocation strategies that optimize campaign spending [14], and analyses of how website quality influences ad performance and user engagement [21]. Although these studies have advanced targeted advertising and monetization, they rely heavily on extensive user data collection and often require user consent for data processing. However, obtaining meaningful and GDPR-compliant user consent remains a challenge, highlighting the need for alternative privacy-preserving approaches that reduce reliance on personal data.

Regarding the impact of digital advertising on users, research has highlighted significant privacy concerns, particularly related to user tracking, data leakage, and compliance with legal frameworks. Studies have shown that major advertising trackers can identify users with over 99.5% certainty after just 30 search result clicks [10] and that RTB can expose up to 27% of a user's browsing history to bidders [17]. These privacy risks have led to increased scrutiny over the adequacy of user consent in programmatic advertising. While regulatory efforts such as the GDPR and the California Consumer Privacy Act (CCPA) aim to strengthen user rights, research suggests that current consent mechanisms often fail to meet legal standards due to their complexity and lack of transparency [26]. The Belgian Data Protection Authority's ruling against IAB Europe further underscored these issues, concluding that the TCF does not ensure valid GDPR-compliant consent, given the challenges in informing users and managing data controller responsibilities [25]. These challenges call for new privacy-preserving approaches that can ensure compliance while minimizing reliance on personal data.

The third and final area of research examines the risks that digital advertising poses to user privacy and explores alternative approaches that reduce reliance on personal data. Traditional ad-matching schemes, such as the one proposed in [5], initially rely only on webpage content and ad features, avoiding direct user

tracking. This limitation in data collection provides a basic form of privacy protection, as no personal user information is gathered. However, the approach also lacks adaptability since it does not incorporate user feedback. To improve performance, the authors later extend their model by incorporating ad impression and click data, which introduces tracking mechanisms. While this enhances targeting efficiency, it also increases data collection and reduces privacy protection. This transition reflects a common pattern in digital advertising research where efficiency improvements often come at the cost of greater data collection. These challenges highlight the need for GDPR-compliant privacy-preserving solutions that ensure effective advertising while respecting user consent.

In contrast, Provost et al. [18] propose a privacy-friendly approach to audience selection for online brand advertising by leveraging browsing behavior to infer quasi-social networks. Unlike traditional methods that rely on explicit user tracking, this approach constructs an anonymous network based on shared visits to user-generated content pages, such as social networking sites. The framework identifies potential brand audiences by selecting social-network neighbors of users who have previously exhibited brand affinity. A ranking mechanism based on brand proximity ensures that selected audiences show higher brand engagement while preserving user anonymity. The authors demonstrate that this method can effectively target relevant audiences without collecting personal identifiers or content data. However, it does not address broader issues of user consent and transparency, which are central to the objectives of this paper.

Finally, to address GDPR compliance issues in RTB and the TCF following their declaration as non-compliant by European authorities in February 2022, IAB Europe proposed two new initiatives: the *Vendor Compliance Program* and the *Global Accountability Platform*. The Vendor Compliance Program consists of both automated and manual monitoring on end-user devices to identify what information is collected by companies participating in the TCF. On the other hand, the Global Accountability Platform is an audited self-reporting system designed to provide accountability for the movement of RTB data between servers. However, as noted in [19], both initiatives face significant challenges, and the study questions whether the use of the TCF for RTB can be effectively monitored, audited, or secured.

As a result, there is still a need for a non-intrusive solution that ensures legal compliance in digital advertising while preserving the existing paradigm. Rather than replacing the system, targeted modifications should enhance user consent management, data privacy, and GDPR compliance without disrupting the industry.

1.2 Contributions and organization of the paper

This work addresses the challenges of ensuring GDPR and ePrivacy Directive compliance in real-time bidding (RTB) by proposing solutions that align these systems with current legislation. Specifically, we introduce a new framework that ensures compliance within the existing RTB model, focusing on the IAB's Transparency & Consent Framework (TCF) and OpenRTB implementations. At the

core of this approach is user consent, which remains a fundamental requirement for legal compliance and trust in the adtech ecosystem.

Our approach builds on the blockchain-based access control system presented in [6] to decentralize user data collection and consent management. By shifting these processes from the current TCF system to a blockchain framework, our solution enhances transparency, security, and user control over personal data.

By design, this framework empowers users with greater control over their personal data within the adtech ecosystem. Additionally, it provides accessible and immutable evidence, enabling entities involved in the RTB process to verify user consent and demonstrate compliance with legal requirements.

The rest of this paper is organized as follows: Section 2 offers a brief overview of the technologies and concepts used in our contribution. Section 3 elaborates on the new scheme, detailing the design requirements, system architecture, and a high-level description of the protocols employed. Section 4 is dedicated to analyzing the functional, security and privacy aspects of the proposal. Finally, Section 5 presents the concluding remarks.

2 Background

This section provides an overview of the key technologies and concepts used in our contribution.

2.1 Programmatic Advertising and Real Time Bidding

Programmatic advertising [4] automates the purchase and sale of ad space through *Ad Exchanges*. It involves two main entities: *Supply-Side Platforms (SSPs)*, used by publishers to manage and sell ad inventory, and *Demand-Side Platforms (DSPs)*, used by advertisers to automate ad buying and campaign management.

Advertisers define their campaign objectives, target audience, and bid amounts via a DSP, while publishers use an SSP to manage available ad space and pricing. The Ad Exchange serves as a marketplace where SSPs and DSPs interact, with notable examples including Google Ad Exchange, Facebook Ad Exchange, and Microsoft Advertising Ad Exchange. Additionally, *Data Management Platforms (DMPs)* aggregate and analyze user data, enabling advertisers to refine their targeting strategies.

At the core of programmatic advertising is Real-Time Bidding (RTB), where ad inventory is bought and sold in real-time during a web page's loading process. When a user visits a website, an auction occurs within milliseconds, determining which ad will be displayed based on advertisers' pre-targeting criteria.

The RTB process, illustrated in Figure 1, follows these steps:

1. Advertisers specify campaign details, including ads, target profiles, and bid amounts via DSPs.
2. A user visits a publisher's website, which has reserved ad space for programmatic sales.

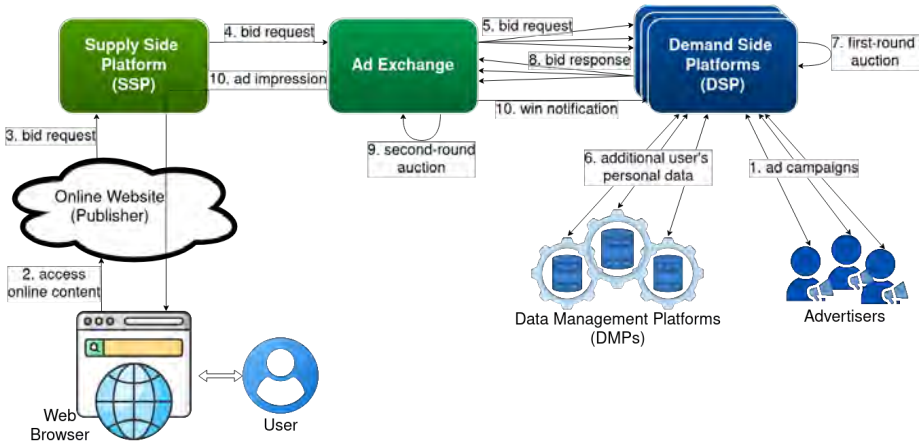


Fig. 1. Programmatic Advertising Scheme

3. The publisher sends a bid request to the SSP, including page details and user data.
4. The SSP forwards the request to the Ad Exchange.
5. The Ad Exchange relays the bid request to the connected DSPs.
6. DMPs may attach additional user-related metadata to the bid request sent to the RTB system. Then, the DSPs retrieve this additional user information and analyze the bid request.
7. Each DSP conducts an internal auction among relevant ad campaigns.
8. DSPs submit bids, specifying the amount and ad content.
9. The Ad Exchange selects the highest bid and runs a second-price auction, where the highest bidder pays slightly above the second-highest bid.
10. The winning ad is sent to the SSP and displayed on the publisher's webpage.

2.2 Pricing model

The primary pricing model in real-time display advertising is CPM (Cost Per Thousand Impressions), where advertisers pay per 1,000 ad displays. Alternative models include CPC (Cost Per Click), charging per ad click, and CPA (Cost Per Acquisition), where payment occurs only after a user completes a specific action [22].

2.3 User consent in IAB's Europe OpenRTB

In Programmatic Advertising, the IAB's TCF embeds user consent into OpenRTB bid requests [11], enabling DSPs and adtech vendors to verify consent before processing personal data for targeted ads. The bid request also includes user data for targeting and measurement.

Consent is stored as a Base64 string generated by the *Consent Management Platform (CMP)*, indicating: i) approved processing purposes, ii) authorized vendors, iii) legal basis (e.g., consent or legitimate interest), and iv) permitted data uses (e.g., personalized ads, analytics).

Upon receiving a bid request, DSPs and vendors check the consent string to determine processing permissions. If restrictions apply, they must exclude certain data or refrain from bidding. Advertisers must ensure compliance with a valid legal basis.

Despite these measures, OpenRTB fails to meet legal requirements (Section 1.1) due to insufficient transparency and user control. Additionally, bid requests expose user data—such as location, device details, and browsing history—raising privacy concerns over how this information is handled and shared.

2.4 Audience Taxonomy

Traditionally, data vendors, DMPs, and analytics providers have used custom taxonomies to segment audiences, leading to inconsistencies in data descriptions. Variability arises from diverse segmentation approaches, including demographic, interest-based, purchase intent, and psychographic classifications, making data comparability challenging.

To address this, the IAB Tech Lab introduced Audience Taxonomy 1.0[3], a standardized framework for labeling audience segments across different providers. This taxonomy ensures consistent classification of both first-party and third-party audience data. In this work, we analyze and adopt this taxonomy to define user profiles.

3 Proposal

In this section, we present the proposed solution for ensuring GDPR compliance in RTB while maintaining transparency and user control. First, we define the requirements that the system must meet to align RTB practices with privacy regulations. Next, we describe the system architecture, explaining how blockchain technology and a browser plug-in enable decentralized consent management. Finally, we detail the three-phase workflow of the framework: Configuration, where users define their privacy preferences; Web Browsing & Consent Enforcement, where consent is automatically applied during online activity; and Consent Management & Data Accountability, which allows users and regulatory authorities to monitor and verify data usage.

3.1 Requirements

In order to reconcile the TCF and RTB systems with GDPR, the following requirements must be fulfilled:

[3] Audience Taxonomy: `https://iabtechlab.com/standards/audience-taxonomy/`

R1 User consent must be explicit, informed, and freely given, ensuring clarity in purpose, data usage, and user choice without implicit assumptions or misleading design.

R2 The integrity and authenticity of consents must be preserved.

R3 Users must be able to access, erase, and withdraw consent as easily as they give it.

R4 Users should have accessible records of visited publishers and involved trackers.

R5 Compliance with user preferences must be enforced across the adtech ecosystem.

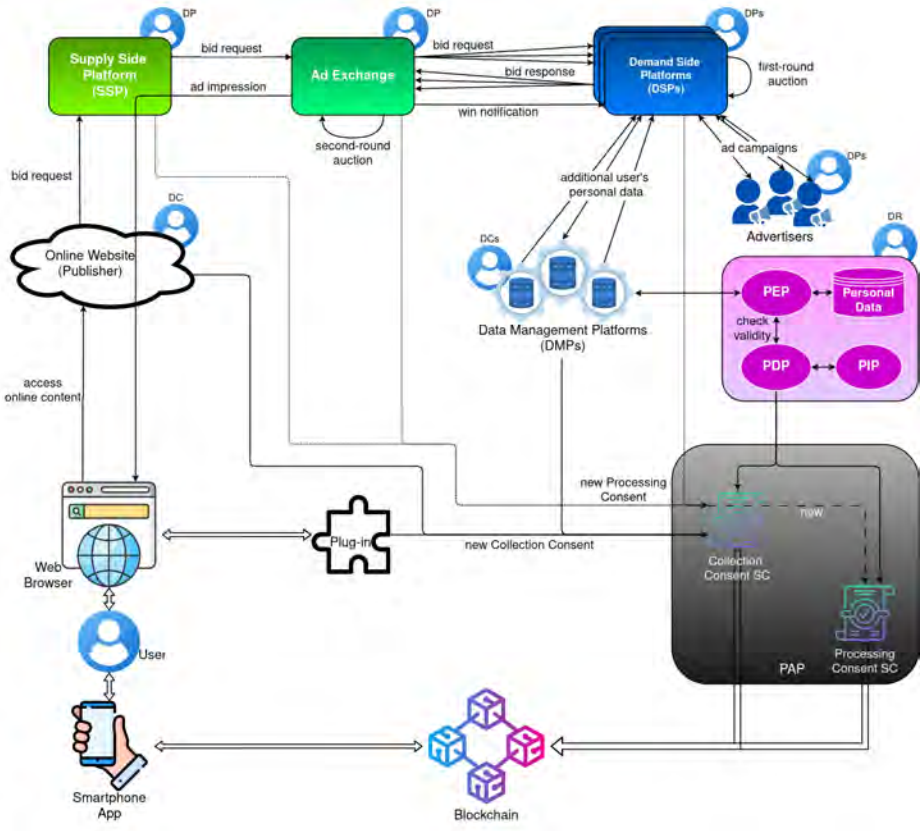


Fig. 2. Proposal Overview

3.2 System architecture

To meet the legal requirements of OpenRTB, our solution decentralizes GDPR compliance verification and data management by leveraging a blockchain network, following the scheme in [6]. By storing user consents on-chain, we provide both users and adtech entities with immutable proof of granted permissions for data processing.

Figure 2 presents an overview of the system, where the browser extension (plug-in) plays a key role in consent management, serving as the user's access point. The plug-in, integrated into the OpenRTB model, ensures compliance without modifying the existing ecosystem. Once configured, it automates consent management based on the user's preferences, transparently handling data collection and processing. Additionally, it records visited sites and displayed ads for user review.

Under GDPR, adtech entities process personal data in two primary roles: Data Controllers (DCs), which determine the purpose and means of data processing, and Data Processors (DPs), which process data on behalf of a DC. In this context, Publishers and Data Management Platforms (DMPs) act as DCs because they collect and provide users' personal data for profiling in ad campaigns. Conversely, SSPs, DSPs, Ad Exchanges, and Advertisers function as DPs since they process this data during the advertising process. Additionally, the role of Data Recipient (DR) refers to the entity responsible for storing users' collected data. A DMP can also act as a DR if it directly stores the data. However, if storage is outsourced to a third party, then that third party assumes the role of DR.

Following [6], our system distinguishes between:

- *Data-Collection Consent:* Agreement between a user and a DC, specifying conditions for data collection in exchange for web content access.
- *Data-Processing Consent:* Agreement between a DP, DC, and user, outlining conditions under which the DP processes user data collected by the DC.

Additionally, a smartphone application provides users with a centralized interface to monitor, modify, and revoke consents in real-time. It also enables users to request data deletion, ensuring full control over their personal information in compliance with GDPR.

The system follows a three-phase workflow:

1. *Configuration:* Users define their privacy preferences, specifying which data can be collected and how it can be processed.
2. *Web Browsing & Consent Enforcement:* As users navigate the web, consent is automatically applied, and the RTB process operates within the predefined privacy settings.
3. *Consent Management & Data Accountability:* Users can monitor their consent history, track displayed ads, modify permissions, and request data deletion as needed.

3.3 Phase-1: Configuration

During the initial configuration, the user installs the plug-in, which enables control over personal data sharing with adtech entities. As part of this setup, the user specifies: i) the types of data she is willing to share; ii) the processing purposes she consents to by default; and iii) whitelisted or blacklisted vendors from the IAB Global Vendor List.

If a new entity, not previously approved, seeks access to user data for a specific purpose, it must first request explicit manual consent.

To help users assess their privacy exposure, the plug-in evaluates the worst-case scenario profile that could be constructed from the selected data. It then generates a privacy risk score ranging from 0 to 1, offering a clear, quantifiable measure of potential data exposure.

Since adtech entities use user profiling to categorize audiences for targeted advertising, understanding how shared data influences profiling is essential. The proposed system leverages this information to compute exposure levels, helping users make informed privacy decisions. The next subsections detail how user interests are structured, how the specificity of shared data is measured, and how this data is processed within the system to assess potential privacy risks.

User Profiling in Programmatic Advertising. User profiles in programmatic advertising are structured as topic distributions that reflect interests derived from browsing behavior. These profiles are built using elements such as keywords, website titles, and metadata, mapped to IAB's Audience Taxonomy (Section 2.4).

Our approach, based on Information Theory, measures the specificity of each taxonomy element using Inverse Document Frequency (IDF) [13]. The web, as the largest publicly available corpus of human knowledge, serves as a reference point to estimate the relative rarity of terms. The frequency with which a term appears across indexed web pages determines its specificity—less frequent terms provide more precise insights into user interests, while widely used terms offer broader categorizations [20].

For example, general terms such as "health" appear frequently across web content, making them less specific and revealing only broad user interests. In contrast, rare terms such as "lung cancer" occur far less often, making them more specific and offering deeper insights into user preferences.

To compute specificity, we analyze the hits (H) from web search engines. The IDF value for a term k is calculated as:

$$IDF(k) = -log(\frac{HC(k)}{total_webs}) \tag{1}$$

where $HC(k)$ is the number of search results for term k ($HC(k) = |H(k)|$), and $total_webs$ is the estimated number of indexed websites (e.g., 400 billion in Google[4]).

[4] Google's Index Size Revealed, 400 Billion Docs: `https://zyppy.com/seo/google-index-size/`

To normalize specificity across different taxonomy levels, we define the Specificity (SP) metric as:

$$SP(k) = \frac{IDF(k)}{-log(\frac{1}{total_webs})} = \frac{-log(\frac{HC(k)}{total_webs})}{-log(\frac{1}{total_webs})} \tag{2}$$

This normalization ensures that specificity values remain within a consistent range, making it possible to compare different taxonomy elements effectively.

Hierarchy-Based Adjustments. The taxonomy used in this work follows a hierarchical structure, where higher-level categories are more general and lower-level categories are more specific. Consequently, the specificity of a non-leaf category depends on its own frequency as well as the aggregated contributions of its subcategories.

Since we are using hit counts to measure specificity, the HC value of a non-leaf category must be adjusted to reflect its overall presence in search results. Ideally, this would involve computing the union of unique search hits from all its subcategories along with its own hits:

$$HC(k) = \left| \left[\bigcup_{k' \in sonsOf(k)} H(k') \right] \cup H(k) \right| \tag{3}$$

However, accurately computing this union is computationally infeasible, as search results often overlap across subcategories or redirect to identical web content. To approximate this value efficiently, we define the adjusted hit count of a non-leaf category as:

$$HC(k) = |H(k)| + \max_{k' \in sonsOf(k)} |H(k')| \tag{4}$$

which follows the assumption:

$$HC(k) = \left| \left[\bigcup_{k' \in sonsOf(k)} H(k') \right] \cup H(k) \right| \geq \max_{k' \in sonsOf(k)} |H(k')| \tag{5}$$

This approximation ensures that higher-level categories retain a meaningful specificity score while remaining computationally efficient. The adjusted HC values are then used to compute IDF, ensuring that hierarchical dependencies are accounted for in the final specificity calculation.

Privacy Awareness and Exposure Calculation

The plug-in uses this specificity metric to help users assess their profile exposure when selecting allowed data categories. Once a user defines a personalized subset (P), their overall profile specificity (SP') is recursively computed:

$$SP'(k) = \begin{cases} \sum_{k' \in sonsOf(k) \cap P} SP'(k'), & \text{if } NOT \text{ areLeafs}(sonsOf(k)) \\ \sum_{k' \in sonsOf(k) \cap P} SP(k'), & \text{if areLeafs}(sonsOf(k)) \wedge \\ & |sonsOf(k) \cap P| < |sonsOf(k)| \\ SP(k), & \text{if areLeafs}(sonsOf(k)) \wedge \\ & |sonsOf(k) \cap P| = |sonsOf(k)| \vee \\ & |sonsOf(k) \cap P| = 0 \end{cases} \quad (6)$$

The final value is normalized between 0 and 1, enabling users to understand their privacy exposure level before consenting to data sharing.

3.4 Phase-2: Web Browsing & Consent Enforcement

When a user accesses a website with ad slots served through programmatic advertising, the publisher must obtain user consent before collecting and transmitting personal data to adtech entities.

In the proposed solution, instead of requiring the user to manually accept the publisher's terms via a TCF pop-up, the plug-in automatically provides the publisher with the user's preset privacy preferences. If the publisher agrees to these conditions, the plug-in generates a *Data-Collection Consent*, granting the user access to the content while allowing the publisher to collect personal data.

To share collected data with other RTB entities (DSPs, Ad Exchanges, and SSPs), the publisher must establish a *Data-Processing Consent* for each. If an entity is whitelisted in the plug-in's IAB Global Vendor List, the publisher generates the corresponding consent automatically. Otherwise, the publisher must request explicit user consent through the plug-in's API.

Both *Data-Collection* and *Data-Processing Consents* are encoded as Smart Contracts (SCs) on the Blockchain [6]. The plug-in manages all consents on behalf of the user, ensuring compliance. These SC references replace the TCF's TC string, which has been deemed non-compliant with current legislation.

Additionally, SSPs may enrich user data using Data Management Platforms (DMPs). In such cases, DMPs must have pre-obtained user consent to lawfully collect data, and SSPs must establish a *Data-Processing Consent* before using it, as detailed in [6].

Once all necessary consents are in place, the RTB protocol proceeds without modification, except when an SSP requests additional user data beyond what is included in the bid request. In this scenario, the SSP must verify a valid *Data-Processing Consent* between the user and the DMP supplying the data. The DMP, in turn, uses the proposed XACML extension to confirm consent validity before requesting the Data Recipient (DR) to provide the user's stored personal data.

Throughout this process, the plug-in records bid impressions for all displayed ads. The logged data includes: i) the winning advertiser's ID; ii) the user data

shared by the publisher; iii) the amount paid for the impression; and iv) the reference to the Data-Collection Consent between the user and the publisher.

3.5 Phase-3: Consent Management & Data Accountability

During this phase, users can access and manage all generated consents, monitoring which entities collect and process their personal data and for what purposes. They can also modify or revoke these consents through a smartphone application, which interacts with Smart Contracts deployed on the Blockchain to ensure transparency and enforcement.

For data accountability, the plug-in records all displayed ads as the user browses the web. This enables users to verify whether advertisers had proper consent to use their data for targeted advertising.

Additionally, Supervisory Authorities can audit these records at any time to ensure adtech entities comply with legal requirements and operate within GDPR regulations.

4 Discussion

Section 3.1 defined key GDPR compliance requirements. This section evaluates their fulfillment through four propositions, each backed by supporting claims.

4.1 Proposition-1: User consent for data collection and processing is explicit, informed, and specific to user preferences

Upon installing the plug-in, users set their privacy preferences and assess their data exposure. These preferences generate a *Data-Collection Consent* when accessing services that request personal data for ads. A *Data-Processing Consent* ensures additional entities (e.g., SSPs, DSPs, Ad Exchanges) obtain explicit user authorization before accessing the data.

This proposition directly supports requirement R1, which mandates that consent be explicit, informed, and freely given. It is validated through the following claims:

Claim 1 *User consent preferences are explicitly defined during the plug-in setup.*

Proof. Upon installation, the plug-in requires users to configure their privacy settings via a user-friendly interface. Users specify: i) which personal data categories may be collected; ii) the duration for which data may be retained; and iii) which vendors from the IAB's Global Vendor List are pre-approved for data processing. Additionally, the plug-in provides transparency by evaluating and displaying the specificity of selected data categories, helping users understand their potential exposure based on the methodology in Section 3.3.

Claim 2 *A new Data-Collection Consent is generated whenever a user accesses an online service that collects personal data for advertising purposes.*

Proof. When a user visits a website that requires personal data for ad targeting, the plug-in ensures that the publisher adheres to the user's predefined privacy preferences. If the publisher agrees to these conditions, the plug-in generates a *Data-Collection Consent* contract between the user and the publisher. This contract specifies: i) the types of personal data the publisher may collect; ii) the retention period; and iii) the identity of the DR responsible for storing the collected data. This contract serves as explicit proof that the user has consented to data collection under the specified conditions.

Claim 3 *A new Data-Processing Consent is created whenever an additional entity requests to process user data collected by the publisher.*

Proof. If an SSP, DSP, Ad Exchange, or advertiser requests access to user data collected by the publisher, a *Data-Processing Consent* contract must be established. This contract specifies: i) the subset of personal data requested; ii) the processing purpose; and iii) the duration for which the data will be processed. The consent is linked to the original *Data-Collection Consent* to ensure that data usage remains traceable and compliant with user preferences.

Claim 4 *Data-processing consent requires explicit or implicit user approval.*

Proof. When a publisher creates a *Data-Processing Consen*t request for an entity, the plug-in checks whether the entity is whitelisted and whether the requested data aligns with the user's predefined preferences. If both conditions are met, the consent is automatically validated. Otherwise, the user must manually approve or reject the request through a notification generated by the plug-in. This ensures that no personal data is shared beyond the user's explicit authorization.

4.2 Proposition-2: Generated Consents Maintain Integrity and Authenticity Throughout Their Lifecycle

The *Data-Collection* and *Data-Processing Consents* referenced in Claims 2 and 3 are stored as Smart Contracts on a public blockchain. Public blockchains are inherently tamper-resistant, ensuring transparency, integrity, and authenticity. Additionally, users interact with these contracts through asymmetric cryptographic key pairs, reinforcing security and non-repudiation.

This proposition directly supports requirement R2, which mandates that the integrity and authenticity of consents must be preserved. It is validated by the following claim:

Claim 5 *All Data-Collection and Data-Processing Consents established between the involved parties are securely stored on a public blockchain using immutable smart contracts.*

Proof. In the proposed system, *Collection Consent Smart Contracts* and *Processing Consent Smart Contracts* encode the respective agreements. Once deployed on the blockchain, these contracts inherit its immutability, authenticity, integrity, and irreversibility properties, ensuring that consents cannot be altered or forged [16].

4.3 Proposition-3: Users retain full control over their consents and GDPR rights

The proposed system allows users to manage consents via smart contracts, enabling them to: i) access their data; ii) request deletion; iii) control data collection and processing; iv) revoke consent anytime. As stated in Claim 5, consents are stored in Smart Contracts, providing users with methods to exercise their rights. The DR enforces access control through an XACML extension, verifying permissions recorded on the blockchain. *Collection-Consent Smart Contracts* encode agreements between users (data owners) and publishers (data collectors), ensuring secure and transparent access.

This proposition supports requirement R3, ensuring users can easily access, delete, and withdraw consent. The following claims support this:

Claim 6 *Smart contracts enable user rights management.*

Proof. The *Collection and Processing Consent Smart Contract*s implement methods that allow users to: i) revoke a *Data-Collection* or *Data-Processing Consent* (i.e., revokeConsent()); ii) modify which personal data can be collected or processed (i.e., modifyData()); and iii) request the DC to erase stored data (i.e., eraseData()).

Claim 7 *The DR enforces access control to user data through the XACML extension.*

Proof. The DR regulates access to user data using an XACML extension, ensuring compliance with granted permissions. The blockchain functions as the Policy Administration Point (PAP), maintaining access rights immutably. When a request is made: i) the Policy Enforcement Point (PEP) forwards it to the Policy Decision Point (PDP) for validation; ii) the PDP retrieves the corresponding *Collection-Consent SC* from the blockchain, verifies the user's public key (PK_{user}), and determines whether the requesting entity has the necessary permissions. This process guarantees that data access is only granted in accordance with the user's established consent.

4.4 Proposition-4: Users have direct access to their consents and ad tracking records

The proposed system allows users to review and manage all granted consents and collected data via the smartphone app (Claims 2, 3 and 7), ensuring compliance with their rights (Claim 6). Additionally, the plug-in logs ad impressions,

summarizing displayed ads, involved entities, and personal data used for targeting. This transparency enables users to monitor data usage and detect potential misuse. If unauthorized processing is suspected, they can request an audit with a Supervisory Authority under GDPR.

This proposition supports requirements R6 and R7 by ensuring users have access to records of visited publishers, trackers, and adherence to their preferences across the adtech ecosystem. It is supported by the previous claims as well as the following:

Claim 8 *The Plug-in Captures All Bid Impressions and Related RTB Data.*

Proof. When a user visits a website displaying ads via RTB, the plug-in records bid impressions and associated data, including the advertiser, participating entities, ad category, and user data used in the selection process. This information is summarized and made accessible through the plug-in's interface, allowing users to review ad delivery details in a clear and structured manner.

5 Conclusions

This paper tackles GDPR and ePrivacy compliance in Real-Time Bidding (RTB) by decentralizing user consent management with blockchain. The proposed framework aligns IAB's TCF and OpenRTB with legal requirements, giving users direct control over their data while providing immutable proof for compliance.

A browser plug-in automates consent management based on user preferences, ensuring seamless browsing and transparency in data processing. A smartphone app allows users to monitor, modify, and revoke consents, while a specificity value in the IAB Audience Taxonomy helps assess privacy risks of shared data.

Future work includes implementing the solution, enforcing compliance without external audits, and evaluating usability, security, and economic feasibility across blockchain architectures.

Acknowledgments. This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation; and by the project Privacy-aware secure explainable data-driven models in federated learning (VR 2023-05531). Furthermore, this research is also supported by the project "HERMES" funded by the European Union NextGenerationEU/PRTR via INCIBE; by project PID2021-125962OB-C32 "SECURING/DATA" funded by MCIN/AEI/10.13039/501100011033/ FEDER, UE, and by the grant 2021SGR 00115 from the Government of Catalonia. The first author is also supported by the Spanish Government under an FPU grant (ref. FPU20/03254).

References

1. Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the

electronic communications sector (directive on privacy and electronic communications). Official Journal of the European Union **L 201**, 37–47 (2002), published 31 July 2002
2. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance). Official Journal of the European Union L 119 **59**, 1–88 (5 2016)
3. Authority, B.D.P.: Iab europe held responsible for a mechanism that infringes the gdpr. https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr (2022), accessed: 2024-11-26
4. Busch, O.: The programmatic advertising principle. In: Programmatic advertising: The successful transformation to automated, data-driven marketing in real-time, pp. 3–15. Springer (2015)
5. Chakrabarti, D., Agarwal, D., Josifovski, V.: Contextual advertising by combining relevance with click feedback. In: Proceedings of the 17th International Conference on World Wide Web. p. 417–426. WWW '08, Association for Computing Machinery, New York, NY, USA (2008)
6. Daudén-Esmel, C., Castellà-Roca, J., Viejo, A.: Blockchain-based access control system for efficient and gdpr-compliant personal data management. Computer Communications **214**, 67–87 (2024)
7. Europe, I.: Iab transparency and consent framework. https://iabeurope.eu/transparency-consent-framework/ (2020), accessed: 2024-11-26
8. Europe, I.: Iab europe adex benchmark 2022 report. https://iabeurope.eu/wp-content/uploads/2023/07/IAB-Europe_AdEx-Benchmark-2022_REPORT-1.pdf (2023), accessed: 2024-11-26
9. Everywhere, K.: 64 game-changing display advertising stats you need to know. https://keywordseverywhere.com/blog/display-advertising-stats/ (2024), accessed: 2024-11-29
10. Gomer, R., Rodrigues, E.M., Milic-Frayling, N., Schraefel, M.: Network analysis of third party tracking: User exposure to tracking cookies through search. In: 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT). vol. 1, pp. 549–556 (2013)
11. Group, P.S.C.W.: Openrtb version 2.6. https://iabtechlab.com/standards/openrtb/ (2022)
12. IAB: 2023 u.s. digital advertising industry hits new record. https://www.iab.com/news/2023-u-s-digital-advertising-industry-hits-new-record-according-to-iabs-annual-internet-advertising-revenue-report/ (2023), accessed: 2024-11-29
13. Jain, A.: Tf-idf in nlp: Term frequency-inverse document frequency. Medium (2024), accessed: 2024-10-05
14. Liu, M., Yue, W., Qiu, L., Li, J.: An effective budget management framework for real-time bidding in online advertising. IEEE Access **8**, 131107–131118 (2020)
15. Malthouse, E.C., Hessary, Y.K., Vakeel, K.A., Burke, R., Fudurić, M.: An algorithm for allocating sponsored recommendations and content: Unifying programmatic advertising and recommender systems. Journal of Advertising **48**(4), 366–379 (2019)
16. Mohanta, B., Panda, S., Jena, D.: An overview of smart contract and use cases in blockchain technology. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (10 2018)

17. Olejnik, L., Minh-Dung, T., Castelluccia, C.: Selling off privacy at auction. In: Network and Distributed System Security Symposium (NDSS) (2014)
18. Provost, F., Dalessandro, B., Hook, R., Zhang, X., Murray, A.: Audience selection for on-line brand advertising: privacy-friendly social network targeting. In: Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. p. 707–716. KDD '09, Association for Computing Machinery, New York, NY, USA (2009)
19. Ryan, J., Santos, C.: An unending data breach immune to audit? can the tcf and rtb be reconciled with the gdpr? SSRN (March 23 2022)
20. Sanchez, D., Batet, M., Viejo, A.: Automatic general-purpose sanitization of textual documents. IEEE Transactions on Information Forensics and Security **8**(6), 853–862 (2013)
21. Shehu, E., Abou Nabout, N., Clement, M.: The risk of programmatic advertising: Effects of website quality on advertising effectiveness. International Journal of Research in Marketing **38**(3), 663–677 (2021)
22. Start.io: Advertising pricing models. https://www.start.io/glossary/advertising-pricing-models (2025), accessed: 2025-01-29
23. Statista: Digital display advertising spending worldwide from 2022 to 2026. https://www.statista.com/statistics/235710/display-ad-spend-worldwide/ (2023), accessed: 2024-11-29
24. Statista: Programmatic advertising worldwide - statistics & facts. https://www.statista.com/topics/2498/programmatic-advertising/ (2023), accessed: 2024-11-29
25. Veale, M., Nouwens, M., Santos, C.: Impossible asks: can the transparency and consent framework ever authorise real-time bidding after the belgian dpa decision? Technology and Regulation pp. 12–22 (2022)
26. Veale, M., Zuiderveen Borgesius, F.: Adtech and real-time bidding under european data protection law. German Law Journal **23**(2), 226–256 (2022)
27. Wu, X., Yan, J., Liu, N., Yan, S., Chen, Y., Chen, Z.: Probabilistic latent semantic user segmentation for behavioral targeted advertising. In: Proceedings of the Third International Workshop on Data Mining and Audience Intelligence for Advertising. p. 10–17. ADKDD '09, Association for Computing Machinery, New York, NY, USA (2009)
28. Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y., Chen, Z.: How much can behavioral targeting help online advertising? In: Proceedings of the 18th International Conference on World Wide Web. p. 261–270. WWW '09, Association for Computing Machinery, New York, NY, USA (2009)
29. Yuan, S., Wang, J., Zhao, X.: Real-time bidding for online advertising: measurement and analysis. In: Proceedings of the Seventh International Workshop on Data Mining for Online Advertising. ADKDD '13, Association for Computing Machinery, New York, NY, USA (2013)

Appendix

The Taxonomy used in the work for user profile definition (IAB Tech Lab's Audience Taxonomy) has a total amount of 496 values under the *Interests* segment. These are organized in an architectural structure as can be seen in Figure 3. In this figure, each node represents an element of the taxonomy and the color and size of the nodes indicate their height and their specificity. In order to calculate this specificity, first, we have performed a search of the different values on the Google search engine and then, we have applied the equation defined in Section 3.3 (Equation 6). See Figure 4, for a zoom of the branches *Academic Interests* and *Healthy Living* for a more detailed example of the labels.

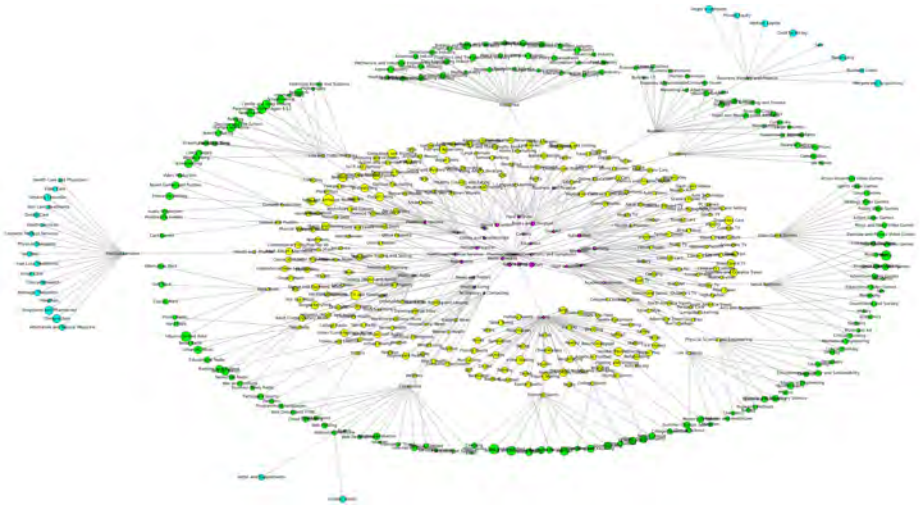


Fig. 3. Interests segment of the IAB Tech Lab's Audience Taxonomy

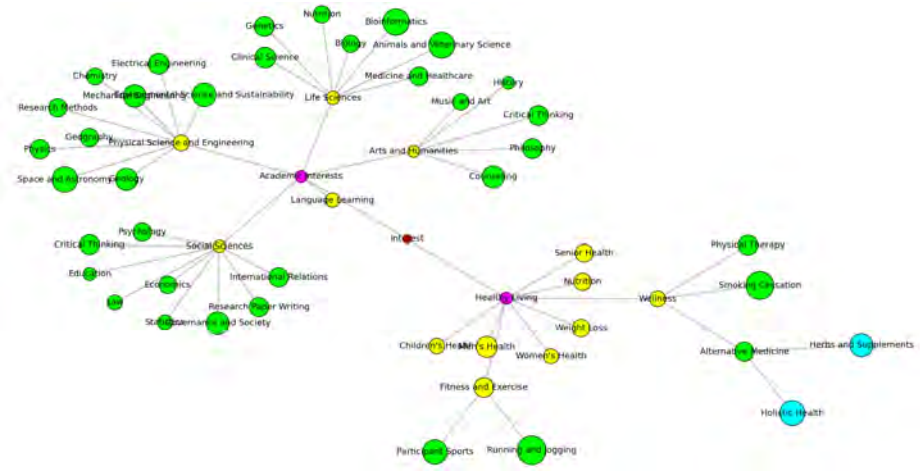


Fig. 4. Subset of Interests segment of the IAB Tech Lab's Audience Taxonomy