How Effective is EU Law in Regulating Personalized Advertising through Real-Time Bidding Ecosystems?

Master's Programme in International Business Law (2 years)
Master's thesis

Author:
Panpan Zhou

Supervisors:
Postdoctoral Researcher, Faculty of Law, Béatrice Schütte
Doctoral Researcher, Faculty of Law, Tahoora Heydari

12.5.2024
Helsinki

Faculty: Faculty of Law
Degree programme: Master of International and Comparative Law (MICL)
Study track: International Business Law (IBL)
Author: Panpan Zhou
Title: How Effective is EU Law in Regulating Personalized Advertising through Real-Time Bidding Ecosystems?
Level: Master's degree
Month and year: May 2024
Number of pages: 67
Keywords: Personalized advertising, Digital advertising, Real-time bidding, Data protection, GDPR, Consent, Transparency

Supervisor or supervisors: Béatrice Schütte, Tahoora Heydari
Where deposited: University of Helsinki
Additional information:
Abstract:

This thesis investigates the intersection of personalized advertising and real-time bidding (RTB) within the European data protection framework, with a focus on evaluating the effectiveness of existing data protection laws. Utilizing a combination of doctrinal research, case studies, and interdisciplinary methodologies, the study explores the mechanisms of personalized advertising and the RTB ecosystems, including the utilization of personal data and the involvement of various stakeholders. The study investigates the interests, roles, and compliance work of key participants in RTB. It identifies the complex nature of RTB ecosystems and the absence of coherent guidelines for clarifying the roles of participants under EU data protection law. This lack of clarity has created legal uncertainty for them in complying with the law. Additionally, this research highlights that the current RTB system falls short of meeting consent criteria, compounded by the unclear legal status of the widely used Transparency and Consent Framework (TCF), leading to uncertainties in ensuring consent within RTB. Moreover, the study finds that current practices heavily rely on partners to collect and transfer data, often based on contractual obligations and shared within the whole ecosystems which are usually inaccessible to users. This lack of transparency hinders users' ability to control their data and exceeds their expectations of data processing. In summary, this thesis adopts a practical perspective, highlighting the inadequacies of the data protection framework in personalized advertising via RTB, emphasizing the need for clear guidelines in the field to ensure compliance. It advocates leveraging industry organizations to bridge the gap between regulations and implementation, as well as fully utilizing technological tools to detect and enhance data protection levels. Although this thesis offers some insights, more comprehensive research is still required for future compliance with data protection laws in the RTB ecosystems.

Table of contents

1 Introduction 6

1.1 Background 6

1.2 Research questions, scope, and delimitations 7

1.3 Methodology 8

1.4 Development of the research 9

1.4.1 Aim and scope 9
1.4.2 Interplay and tensions 10
1.4.3 Primary focus and limitations of existing studies 10
1.4.4 Technical and methodology survey of current research 12
1.4.5 Conclusion 12

2 Personalized advertising and real-time bidding ecosystems 14

2.1 Definition and the mechanisms of personalized advertising 14

2.2 Real-time bidding ecosystems 17

2.3 Data protection challenges 19

2.3.1 Overview of data protection concerns 19
2.3.2 Urgency to clarify the key issues 20

3 Compliance or circumvention? The practices of key stakeholders in the RTB under EU regulations 22

3.1 Understanding 'personal data' under the EU data protection law 22

3.2 The key stakeholders in the RTB ecosystems: interests, roles, and compliance practices 24

3.2.1 Publishers 25
3.2.2 Advertisers 26
3.2.3 AdTech Vendors 27
3.2.4 Consent management platforms 30
3.2.5 Industry association, IAB Europe for example 31

3.3 Challenges in enforcing compliance 34

3.3.1 Complexity of the RTB transaction 34
3.3.2 Lack of coherent interpretation of regulations and detailed guidelines for participants 35
3.3.3 Cross-border issues and jurisdictional challenges 36

4 Effectiveness of EU law in regulating personalized advertising via RTB 37

4.1 Purposes and legal basis in personalized advertising via RTB 37

4.1.1 A survey of purposes and legal basis of data processing in practice 37
4.1.2 Meaning of valid consent 40
4.1.3 How to obtain valid consent? 42
4.1.4 The analysis of the feasibility of the Transparency and Consent Framework after the Belgian DPA's decision on IAB Europe, a case study 44
4.1.5 Examining the viability and dilemmas associated with using legitimate interest as a legal basis 46
4.1.6 Evaluating the efficacy of EU legislation in establishing the legal basis for data processing in RTB 49

4.2 Transparency 49

4.2.1 Understanding transparency in the EU data protection framework 49
4.2.2 Is that possible to meet transparency obligations under EU law in RTB ecosystems? A case study 52
4.2.3 Challenges faced in achieving transparency in data protection law within the RTB 56
4.2.4 Evaluating the effectiveness of the EU data protection framework 59

5 Enhancing the effectiveness of EU Law: opportunities 63

6 Conclusion **66**

Bibliography **68**

List of abbreviations

AdTech: Advertising Technology

AI Act: Artificial Intelligence Act

CJEU: Court of Justice of the European Union

CMP: Consent Management Platform

CNIL: National Commission on Informatics and Liberty

EDAA: European Interactive Digital Advertising Alliance

EDPB: European Data Protection Board (the successor of Art. 29 WP)

DPA: Data Protection Authority

DSA: Digital Service Act

DSPs: Demand Side Platforms

GDPR: General Data Protection Regulation

IAB: Internet Advertising Bureau

ICO: Information Commissioner's Opinion

ICCL: Irish Council for Civil Liberties

NOYB: None of Your Business

OBA: Online behavioural advertising

ROI: Return on Investment

RTB: Real-Time Bidding

SSPs: Supply Side Platforms

TCF: Transparency and Consent Framework

TC String: Transparency and Consent string

Art. 29 WP: Article 29 Working Party (The processor of EDPB)

1 Introduction

1.1 Background

Online users have become accustomed to accessing the services of online platforms for free rather than paying directly, with these platforms primarily funded by advertisements. [1] Digital advertising is the field in which advertisers use digital tools and technologies to complete their marketing work, prompting customers to buy their products and services. To maximize ad revenue, they are eager to target individuals who are interested in their offerings, by collecting and profiling personal data they personalized their ads based on users' profiles, which is known as personalized advertising. To reach potential buyers, they need to collaborate with Advertising Technology (AdTech) exchanges and publishers to timely display their ads, in an ecosystem known as Real-time Bidding (RTB) within programmatic advertising. The interdependent relationship between personalized advertising and RTB stands as a cornerstone for digital ads and is heavily relied by digital ads participants.[2] This intricate interplay intertwines online platforms and artificial intelligence models that monetize personal data for digital ads, involving the profiling, tracking, auctioning, and sharing of personal data,[3] shaping advertising methodologies and introducing substantial challenges in personal data protection.[4] In this thesis, I will focus on the main issues raised in this area, analysing them at the intersection of recommender systems and RTB to highlight important data protection issues, then analyse the legal gap between regulations and practices, and provide recommendations for potential improvements.

---

[1] See GfK, 'European Online, An Experience Driven by Advertising' (6 September 2017), 3 <https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf> accessed 27 February 2024; IAB Europe, 'What Would an Internet Without Targeted Ads Look Like' (April 2021) <https://iabeurope.eu/wp-content/uploads/2021/04/IAB-Europe_What-Would-an-Internet-Without-Targeted-Ads-Look-Like_April-2021.pdf> accessed 27 February 2024.

[2] IAB Europe, 'Attitudes to Programmatic Advertising Report' (November 2023), 5, Figure 3 <https://iabeurope.eu/wp-content/uploads/IAB-Europe-Attitudes-to-Programmatic-Advertising-Report-2023-FINAL.pdf> accessed 27 February 2024.

[3] Information Commissioner's Opinion (ICO), 'Data Protection and Privacy Expectations for Online Advertising Proposals' (2021), para 2.

[4] As an illustration example, the German data protection authority investigated revealing that consent mechanisms on media companies' websites are largely ineffective, posing substantial risks for users. The personal data acquired through user tracking is subsequently employed in online marketing, notably within the real-time bidding process, see German SAs, 'Cross-state Audit: Consent on Media Companies' Websites is Mostly Ineffective - Improvements are Needed' (EDPB News, 30 June 2021) <https://edpb.europa.eu/news/national-news/2021/german-sas-cross-state-audit-consent-media-companies-websites-mostly_en> accessed 4 October 2023.

1.2 Research questions, scope, and delimitations

The thesis aims to study the effectiveness of EU law in regulating personalized advertising through the RTB ecosystems. To answer this question, three sub-questions need to be answered:

a. How do key stakeholders in the RTB ecosystems comply with or circumvent EU regulations concerning personalized advertising?

b. To what extent does the current EU law adequately address the data protection concerns arising from the RTB ecosystems in personalized advertising? Especially on the question of adequate legal basis for processing, and transparency requirements.

c. What are the challenges and opportunities for enhancing the effectiveness of EU law in regulating personalized advertising within the RTB ecosystems?

The scope of this thesis is online digital advertising, programmatic advertising, specifically, the intersection of the RTB ecosystems and personalized advertising, which is similar to online behavioural advertising. In this realm, I will focus on the issues related to data protection law, for example, the specific challenges arising from data collection, utilization, transfer, and the flow of data in the ecosystems. Based on this context, I aim to clarify the roles, interests, and compliance work of the main participants in RTB, its adequate legal basis and transparency requirements within it.

Regarding the jurisdiction, the thesis will focus on EU law, which aims to regulate personal data protection, online platforms, and AI models that are related to personal data protection, for instance, the General Data Protection Regulation (GDPR),[5] the Digital Service Act (DSA),[6] and the Artificial Intelligence Act (AI Act) proposal.[7] The objective of this thesis is to conduct comprehensive research on the materials,

[5] 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) [2016] OJ L 119/1.
[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.
[7] European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts [2024] P9_TA(2024)0138 <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf> accessed 28 March 2024.

illustrate the research questions, and bring up new perspectives on data protection in this field.

Since the complexity of recommender systems and the RTB ecosystems, many data protection issues have been raised at this intersection. However, due to the constraints of thesis length, I will focus solely on several key issues for investigation，where the research questions need to be answered. This decision is influenced by the lack of clarity regarding the roles of the main participants in RTB, which leads to uncertainty of compliance work of participants, as well as the lack of examination of the efficiency of consent in the context of RTB in practices, many research studies only justify consent as a proper legal basis but do not delve further. Additionally, the need for transparency, as highlighted in decisions by certain Data Protection Authorities (DPAs), further underscores the importance of prioritizing transparency in this thesis. The thesis aims to follow the newest research in this field, encompassing both legal and technical perspectives.

1.3 Methodology

In this thesis, I will mainly adopt a doctrinal research method, and survey the existing court judgments and statutes[8] in the field of data protection at the intersection of personalized advertising and RTB systems. Sources include EU legislation, case law from the Judgements of the Court of Justice of the European Union (CJEU), binding decisions, opinions, and guidelines from the European Data Protection Board (EDPB) and the Article 29 Working Party (Art. 29 WP); decisions from national supervisory authorities will be studied comprehensively in this thesis. Secondary sources include books, articles, conference papers, theses, comments articles, press, and others.

In addition, an empirical method, specifically, a case study will also be used in this thesis. Using this method to study how laws are understood, and how and why they are applied and misapplied, subverted, complied with, or rejected.[9] The case study will be designed to conduct a cross-sectional analysis between two or more cases.[10] Cases adjudicated by the CJEU and decisions rendered by various national data

[8] Mike McConville and Wing Hong Chui (eds), *Research Methods for Law*, (2nd edn, Edinburgh University Press 2017), 4.
[9] Lisa Webley, 'Stumbling Blocks in Empirical Legal Research: Case Study Research' (2016) Law and Method, 3, para 1.
[10] ibid 12, para 2.

supervisory authorities epitomize the current landscape of conflicts in the RTB and EU Law interpretation. These legal challenges underscore the imperative for interpretation and reveal the disparities between theoretical frameworks, technological advancements, and regulatory measures. The primary focus of the case study will be to assess the adequacy of EU law in addressing data protection concerns stemming from the RTB ecosystems in personalized advertising. The overarching aim is to propose interpretations and provide potential recommendations to bridge these legal gaps, fostering a more robust regulatory framework.

Furthermore, I intend to incorporate an interdisciplinary research approach into this thesis. This approach aims to analyse personalized advertising in RTB from both market and technical perspectives. For instance, it involves investigating the technical aspects of recommendation systems and RTB, AI explainability, technology tools for enhancing transparency and data control, as well as the interplay between data protection law and competition law. Additionally, it delves into the conflict between data monetization and data protection. By doing so, the aim is to deepen understanding of the inherent tensions and to propose potential solutions for addressing challenges within this field.

In this thesis, the AI language models are used in correcting grammar mistakes, improving expressions, giving me some related work recourses and comments on my draft to improve my work. Chat GPT 3.5[11] and Copilot[12] are used in this thesis.

1.4 Development of the research

1.4.1 Aim and scope

This thesis surveys the past decade of research on personalized advertising within RTB, with a particular focus on developments after the implementation of the GDPR. The previous research which is examined includes three main aspects: Firstly, the examination of privacy tensions within recommender systems. Secondly, the exploration of data protection issues within the RTB ecosystems. Lastly, the investigation into technical solutions and strategies designed to enhance data protection in personalized advertising via the RTB ecosystems. This part intends to

[11] Chat GPT 3.5 <https://chat.openai.com/>
[12] Copilot <https://copilot.microsoft.com/>

critically integrate and analyse existing knowledge, offering new perspectives that build upon the foundations laid by previous scholarly works.

1.4.2 Interplay and tensions

From a macroscopical perspective, contemporary research illustrates the dynamic and tense relationships between the development of digital technology, the protection of personal data for data subjects, and regulatory frameworks.[13] The personal data obtained from data subjects form the foundation for recommender systems. Factors such as privacy awareness and the ability to control data significantly influence the utilization and protection of personal data. The advancement of digital technology, exemplified by recommender systems that enhance convenience and efficiency for consumers, simultaneously stimulates consumer desire to make purchases. However, the monetization and excessive use of personal data create tensions between digital technologies and users. Stringent data protection regulations provide safeguards for data subjects but concurrently impose restrictions and legal uncertainties for digital technology businesses.

The dynamic interplay among various stakeholders poses numerous challenges to establishing and maintaining an effective data protection framework. While current studies establish a research framework for new researchers within a broader scope, they fall short of presenting detailed solutions for the fundamental conflicts in this field.

1.4.3 Primary focus and limitations of existing studies

From a microscopic viewpoint, the ongoing research discusses numerous issues within legal practices, many of which require urgent clarification. For instance, a set of questions has arisen following the Belgian DPA's decision on Internet Advertising Bureau Europe (IAB Europe),[14] encompassing the roles, duties, and responsibilities of different participants in RTB ecosystems, if the Transparency and Consent string (TC String) in RTB can be regarded as personal data, and whether current practices in the RTB ecosystems comply with transparency, accountability, and legal transfer requirements in the EU legal framework. Some questions have been answered by the

[13] Sara Quach and others, 'Digital Technologies: Tensions in Privacy and Data' (2022) 50 J. of the Acad. Mark. Sci, 1299 <https://doi.org/10.1007/s11747-022-00845-y> accessed 17 January 2024.
[14] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377.

CJEU, some still need detailed assessment by referring court.[15] While this case might prompt adjustments to data protection strategies, it may not resolve the contentious and irreconcilable contradiction between the two sides.

There is agreement that this case represents a milestone capable of reshaping the entire landscape of online advertising. Some argue that complying with the Belgian DPA's requests in the RTB ecosystems is unrealistic or even impossible.[16] The adequate legal basis for processing data in this field remains a prominent subject of debate.[17] Numerous studies have scrutinized the feasibility of utilizing legitimate interests, contractual necessity or consent for data processing, with a prevailing argument that, in the RTB ecosystems, only consent, as a more stringent legal basis, can be employed in this context.[18] However, there is also researcher contends that even consent is likely invalid under EU law.[19] This raises questions about is possible to gain valid consent and how within the RTB. Is it plausible to consider legitimate interest as a legal basis for processing personalized advertising? Are there gaps between legal propositions and practical implementations?

While current research continually introduces recommendations, the lack of a comprehensive data protection strategy integrated with technical measures results in substantial gaps between theory and practice, for example, the process of achieving visualization and reference code from the legal side for the technical side remains unanswered in current research.[20]

Discussions on transparency are prevalent in research, particularly concerning the data source, sharing, and profiling of personal data in the context of RTB. The previous studies argue that transparency is not possible, because it is difficult to

---

[15] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214.
[16] Michael Veale and others 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?' (2022) TechReg 12, 22 < https://ssrn.com/abstract=4206059>accessed 17 January 2024.
[17] Célestin Matte and others 'Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?' (In proceedings of Privacy Technologies and Policy: 8th Annual Privacy Forum, Lisbon, October 2020) <https://doi.org/10.1007/978-3-030-55196-4_10> accessed 17 January 2024.
[18] Chaoqun Li, 'Analysis of the Advertising Technology Industry's Compliance with the General Data Protection Regulation: A Case Study of the CNIL Investigation of the French Advertising Technology Giant Criteo' (Master's thesis, Technische Universität Dresden 2022), 24-43 <http://dx.doi.org/10.2139/ssrn.4307210> accessed 17 January 2024.
[19] Konrad Kollnig, 'Priorities for More Effective Tech Regulation' (2023) 1 ArXiv Computers and Society, 2 < https://doi.org/10.48550/arXiv.2302.13950> accessed 17 January 2024.
[20] ibid 6.

provide comprehensive information, lack of clarity about the processing, ambiguity about the data sharing activities. [21]

1.4.4 Technical and methodology survey of current research

From the technical aspect, incorporating privacy considerations or designing with privacy in mind emerges as a crucial subject in practice. Current research addresses various technical protection strategies, essential technical methods for privacy protection within recommending systems,[22] the diverse ways in which personal data is utilized by participants in RTB, the influence of personal data on bidding strategies, the feasibility and costs associated with re-identification,[23] and technological advancements aimed at enhancing personal data protection. Nevertheless, there is a noticeable absence of interdisciplinary consideration, such as aligning privacy design or existing data protection technologies with the latest requirements from EU law.

From a methodological perspective, previous relevant studies have predominantly employed literature analysis, empirical research, survey studies, and case studies, with only a few considering interdisciplinary research methods. I believe that in this research field, it is crucial to fully consider legal practices, such as technological implementations, impact and incentives to the businesses, and enforcement of the EU law, rather than merely constructing castles with perfect legal expressions in the air. Therefore, starting from legal cases, it is essential to identify contradictions in judicial practices and engage in thoughtful considerations from both interdisciplinary and multiple stakeholders' perspectives.

1.4.5 Conclusion

In summary, previous studies have laid a solid foundation and framework for further research in this thesis, offering insights into the analysis of various participants from a legal perspective, the clarification of key research issues, and the consideration of methodology. However, current research still lacks a thorough and comprehensive

---

[21] Gabriela Davoli, 'Is Winter Coming for Online Behavioural Advertising? The Future of Targeted Advertising in the EU' (Master's thesis, Tilburg University 2023), 34, para2.
[22] Cong Wang and others, 'Toward Privacy-Preserving Personalized Recommendation Services' (2018) 4(1) Engineering 21<https://doi.org/10.1016/j.eng.2018.02.005> accessed 17 January 2024.
[23] Keen Sung and others, 'Re-Identification of Mobile Devices Using Real-Time Bidding Advertising Networks' (In Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, Association for Computing Machinery, New York, Article 48, 2020) <https://doi.org/10.1145/3372224.3419205> accessed 17 January 2024.

analysis of the utilization and protection of personal information in personalized advertising via RTB ecosystems. This deficiency is particularly evident in the data profiling, attention to data flows, the analysis of roles and obligations of various participants, and the multi-perspective analysis within the current legal framework. In the upcoming chapter, we will study the personalized advertising and real-time bidding ecosystems, aiming to clarify the technical aspects that are essential for legal analysis.

2 Personalized advertising and real-time bidding ecosystems

The intersection between personalized advertising and RTB holds significant importance for digital ads. Prior to conducting a thorough analysis, it is crucial to gain a comprehensive understanding of their functionalities, the involved stakeholders, and the interdisciplinary aspects associated with them. This section aims to introduce the intricacies of personalized advertising, the operational processes of RTB, and the distinctive challenges within this domain.

2.1 Definition and the mechanisms of personalized advertising

Personalized advertising, similar to online behavioural advertising, [24] utilizes a wide range of personal data to deliver tailored advertisements to users. These ads are widely deployed[25] on online platforms and play a vital role by emphasizing the monetization of personal data, optimizing conversion rates, minimizing costs, increasing advertising revenue, and enhancing users' experiences. Personalized advertising customizes ads and predicts users' preferences based on data analysis and digital technologies. In this situation, effectively and comprehensively capturing and profiling personal data is important since businesses aim to avoid spending on users who are not interested in their products or services.

[24] In this thesis, I opt to use the term 'personalized advertising' rather than 'online behavioral advertising' (OBA), because later one is primarily centers on users' online activities such as searches, clicks, visits, and others. However, it should be noted that in certain studies, the definitions of these two terms may overlap. For example, the OBA is defined as 'Advertisers are increasingly monitoring people's online behavior and using the information collected to show people individually targeted advertisements' 'Such data can include websites visited, articles read, and videos watched, as well as everything' After becoming widely used, this definition expanded to include the use of static user information. To be more specific, I've chosen to use 'personalized advertising.' see Sophie C. Boerman and others, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) J. Advert 363, 363.

[25] For example, Google collects personal data to provide personalized services, including content and ads. Amazon use personal information to recommend feature, products, and services that might be of interest to users, identify uses' preferences, and personalized their experience. Instagram uses the information they collect to provide users with a personalized experience, including advertising.

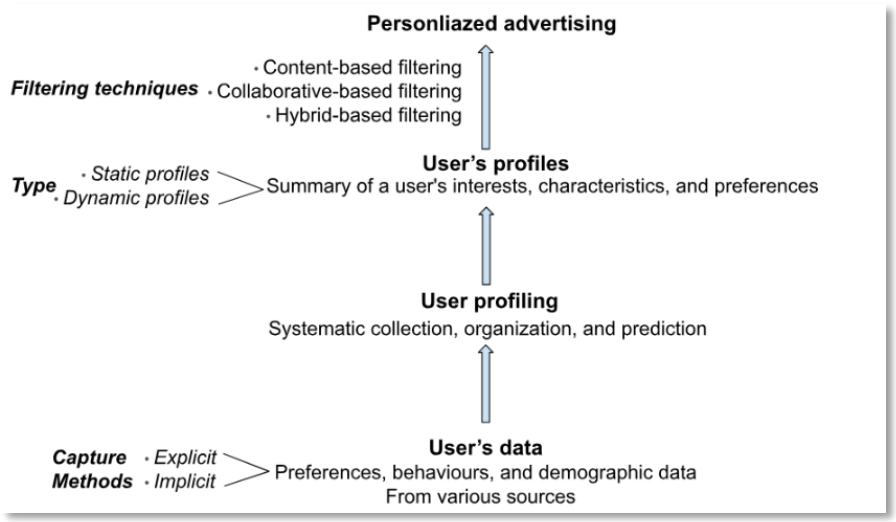

Figure 1: the mechanisms of personalized advertising

Personalized advertising (the mechanisms see figure 1) relies heavily on profiling, which enables the promotion of tailored products and services to users based on their preferences, behaviours, and demographic data. A user profile serves as a concise summary of a user's interests, characteristics, and preferences.[26] User profiling involves the systematic collection, organization, and prediction of this profile. There are two main types of user profiles: static profiles, which are permanent attributes, that are actively provided by the user and changed manually in the user's database.[27] Dynamic profiles, also known as behavioural or adaptive profiles, are typically predicted or captured by the system through interactive user-content activities.[28] Since in the former situation, not many users would like to keep a higher quality and also update their information timely, so the latter one is even commonly used in practice.[29]

User profiling encompasses various approaches, including behavioural modeling and interest modeling. These approaches utilize user preference data such as likes, shares,

[26] Sara Ouaftouh and others, 'A User Dimension-Based Classification' (10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, Morocco,2015) 1, 2 <DOI: 10.1109/SITA.2015.7358378> accessed 18 January 2024.
[27] Elma Avdagić-Golub and others, 'Profiling Contact Center Customers for Optimization of Call Routing Using Data Mining Techniques' (20th International Symposium INFOTEH-JAHORINA,2021)1, 2 <DOI: 10.1109/INFOTEH51037.2021.9400671> accessed 18 January 2024.
[28] Christopher Ifeanyi Eke and others, 'A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions' (2019) 7 in IEEE Access 144907, 144910 <DOI: 10.1109/ACCESS.2019.2944243> accessed 18 January 2024.
[29] Sara Ouaftouh and others, 'A User Dimension-Based Classification' (10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, Morocco,2015)1, 2 <DOI: 10.1109/SITA.2015.7358378> accessed 18 January 2024.

search history, and attention data. Additionally, user profiling can be based on user intentions. The process involves understanding and categorizing user behaviours to enhance the effectiveness of personalized advertising.

The profiling process typically commences with the collection of personal data, utilizing both explicit and implicit methods to capture user information, the former usually needs users' effort and puts them in a conscious situation, latter is processed automatically,[30] These approaches heavily rely on machine learning and have distinct implications for privacy. Following the acquisition of personal data and the establishment of user behavioural and interest profiles, the next steps involve optimizing the data by rectifying inaccuracies and providing more effective recommendations. This optimization process is followed by feature extraction, employing various technologies in data modeling and profiling.[31]

Filtering techniques, such as content-based filtering, collaborative-based filtering, and hybrid-based filtering, play a crucial role in refining and enhancing the profiling process. Content-based filtering categorizes users into groups, analyses their profiles, and delivers tailored ads based on the similarity of users. Collaborative-based filtering is based on the interactions between users and features and characteristics of items, where users' preferences, behaviour data can be used.[32]

User profiling plays a pivotal role in personalized advertising. Clearly defining the concept and process of data profiling is essential to understanding the utilization of personal data in complex personalized advertising systems. Contemporary user profiling methods are diverse, automated, and complex. Throughout the entire process, various information and personal data are captured and leveraged to enhance user profiles, leading to more accurate personalized recommendations.

However, several challenges related to data protection arise along with personalized advertising. Firstly, establishing a valid legal basis for user profiling poses a challenge, especially when data is not directly obtained from users. Secondly,

---

[30] Bo Zhang and others, 'Privacy Concerns in Online Recommender Systems: Influences of Control and User Data Input' (In Proceedings of the Tenth USENIX Conference on Usable Privacy and Security (SOUPS '14). USENIX Association, USA, 2014) 159, 159.
[31] Christopher Ifeanyi Eke and others, 'A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions' (2019) 7 IEEE Access144907, 144910 <DOI: 10.1109/ACCESS.2019.2944243> accessed 18 January 2024.
[32] Cong Wang and others, 'Toward Privacy-Preserving Personalized Recommendation Services' (2018) 4(1) Engineering 21, 21, para 2 <https://doi.org/10.1016/j.eng.2018.02.005> accessed 18 January 2024.

advanced technologies may be deployed to re-identify or deduce user's personal data to use in the process even when not provided directly. Thirdly, meeting the transparent requirement for data minimization is also a significant challenge in this context. We will delve into details later on.

2.2 Real-time bidding ecosystems

RTB is one of the mechanisms used in online programmatic advertising.[33] It is a transactional method that facilitates the buying and selling of online ad space within milliseconds. RTB is a dynamic process in which advertisers present personalized ads on the publisher's website driven by the bid request that includes various user data.

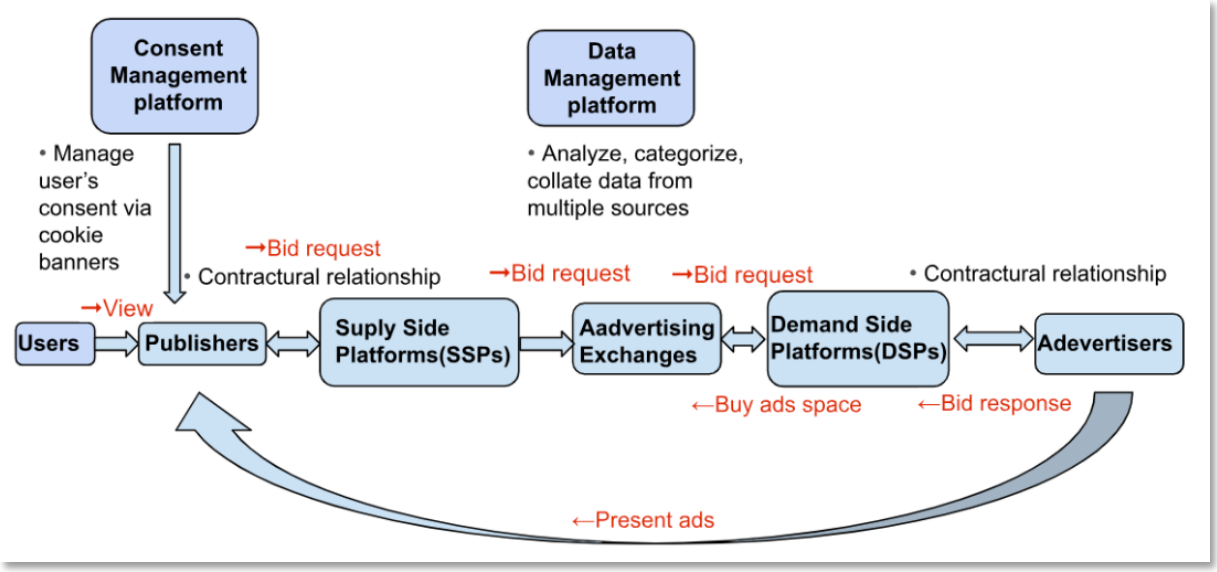

Figure 2: the RTB process (Michael Veale and Frederik Zuiderveen Borgesius).[34]

This process (see Figure 2: The RTB process) initiates when a user visits the publisher's website, the user's view or impression, where online ad space is available for sale. Publishers collect user's consent and preferences with the cookie banners

[33] Programmatic advertising is defined as 'Programmatic ad campaigns automatically follow certain rules decided ahead of time by the managers or campaign decision makers, as advertising space is created in real-time by consumers' actions such as visiting a website.' The biggest difference between it and traditional ads is lying in the degree of automation of advertising delivery technology, it may include RTB as well as other methods such as private marketplace (PMP) deals and programmatic guaranteed. To enhance precision, this thesis will exclusively utilize the term 'RTB'. Definition see Dylan Cooper and others, 'Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising' (2021) JCM 8, paras 2-3<http://dx.doi.org/10.2139/ssrn.4012936> accessed 18 March 2024. Categories of Programmatic Advertising see Jiří Maršál, 'Legal Aspects of Online Behavioural Advertising' (Master's thesis, Univerzita Karlova 2022), 14, para 2.

[34] Michael Veale, Frederik Zuiderveen Borgesius, 'Adtech and Real-time Bidding under European Data Protection law' (2022) 23 GLJ 226, 232, figure 1, <DOI:10.1017/glj.2022.18> accessed 3 March 2024.

provided by CMPs. Publishers with the assistance of Supply Side Platforms (SSPs), send ad bid requests, that include various personal data to advertising exchanges, also called AdTech vendors, which facilitates the auction deal between SSPs and Demand Side Platforms (DSPs). The AdTech vendors then dispatch bid requests to various potential DSPs. Subsequently, the DSPs help advertisers purchase ad space by utilizing the user's data contained in the bid request and the parameters they set for auction, ensuring they can effectively present ads to the most relevant audience of advertisers. Ultimately, the winning bidder among advertisers gets the opportunity to present their ads on publishers' websites, reaching the targeted users.[35] [36] [37] Data management platforms may be used in the ecosystems to collect, organize, analyse large volumes of data from various sources, to create extensive user profiles and to improve the efficacy of targeting.

Various participants are involved in this process, and the entire process unfolds within milliseconds. In practice, the whole process could be more complex due to the multifaceted role of the company and the contracultural relations between them, as well as multiple sources of personal data and the utilization of various digital technologies.

The ad bid request contains various data, and it can also be enriched in the whole process by combining data from different sources, Usually, an ad bid request could include the following information: 'a unique identifier for the bid request, the user's IP address, cookies IDs, user IDs, a user-agent string identifying the user's browser and device type, the user's location, the user's time zone, the detected language of the user's system, the device type, other information could include referring sites, user journey on the side, mouse cursor movement for example, events' and so on. [38]

In addition, the bid request is delivered to various participants in the whole process, it will be sent to one or several ad exchange companies, and then they will send the

[35] Kristin Benedikt, 'Belgian Data Protection Authority Ruling - Online Advertising on the Brink of Extinction?' (2022) 8(1) European Data Protection Law Review 85-89, 85, <https://doi.org/10.21552/edpl/2022/1/13> accessed 29 January 2024.
[36] ICO, 'Update Report into AdTech and Real Time Bidding' (2019), 10.
[37] Gabriela Davoli, 'Is Winter Coming for Online Behavioural Advertising? The Future of Targeted Advertising in the EU' (Master's thesis, Tilburg University 2023), 21, figure 1.
[38] ICO, 'Update Report into AdTech and Real Time Bidding' (2019), 12.

bid request to a large number of DSPs that represent potential advertisers.[39] In this process, DSPs can obtain a lot of personal data at a low cost. User profiling is very common in whole ecosystems and various of technologies are used, for example, machine learning and AI models, which allow the system to become more efficient and automatic.

To ensure the effective operation of RTB, the RTB protocol, established as an industry standard, facilitates efficient communication among participants. These technical specifications precisely detail the data exchanged between parties and the mechanisms governing this exchange during transactions.[40] Two leading protocols are commonly used in industry, one IAB's 'Open RTB' and IAB Europe's 'Transparency and Consent Framework'(TCF), another is Google's 'Authorized Buyers' framework. [41]

2.3 Data protection challenges

Online advertising strives to personalize the selection and delivery of ads to the right potential customers(personalization) at the right time(real-time),[42] involving user profiling and the participation of multiple entities, as demonstrated in the previous section. This brings special data protection challenges in this intersection area. Identifying the challenges is an important step to clarify the legal gaps and explore potential opportunities for enhancing the effectiveness of the EU data protection framework.

2.3.1 Overview of data protection concerns

Personalized advertising through RTB ecosystems poses risks to data protection. The request for effectiveness and data monetization within the ecosystems often overlooks data protection, which needs additional oversight. In the RTB ecosystems, various participants handle data collection, sharing, identification, and utilization. Users' profiles may be shared with economic vulnerabilities and irresponsible third

[39] Johnny Ryan and Cristiana Santos, 'An Unending Data Breach Immune to Audit? Can the TCF and RTB be Reconciled with the GDPR?' (2022) Irish Council for Civil Liberties (ICCL)Research Paper, 7 <https://ssrn.com/abstract=4064729> accessed 22 January 2024.
[40] Jiří Maršál, 'Legal Aspects of Online Behavioural Advertising' (Master's thesis, Univerzita Karlova 2022), 20, para 4.
[41] ICO, 'Update report into AdTech and Real Time Bidding' (2019), 14.
[42] José Antonio Estrada Jiménez, 'Privacy in Online Advertising Platforms' (DPhil thesis, Universitat Politècnica de Catalunya 2020), 64, para 1<https://upcommons.upc.edu/bitstream/handle/2117/330390/TJAEJ1de1.pdf> accessed 22 January 2024.

parties, for example, all potential DSPs in the RTB, which brings data leakage and cross-border transfer risks, just like the Irish Council for Civil Liberties (ICCL) worried about 'confirming there are no technical measures to limit what companies can do with people's data, nor who they might pass it on to'. [43]

Moreover, tracking and profiling technologies like cookies, fingerprinting, pixel syncs and others, while enhancing the ecosystems, can also lead to the entire system being challenging to control, cognitively burdensome, and opaque to users, which may make users feel they are continuously monitored and also raise transparency concerns. In this field, the processing of sensitive categories of personal data, such as health information or financial data, is also possible, which raises concerns regarding the potential for discrimination or exploitation. And since the characteristics of the ecosystems, ensuring adequate legal basis that meets data protection laws is also challenging.

2.3.2 Urgency to clarify the key issues

In this dynamic ecosystem, various participants interact with each other, relying on one another to transfer user data and complete the RTB process. However, there is a lack of clarity regarding the roles of different participants, leading to uncertainty about their obligations and allocation. It is crucial to clarify these roles in this field.

According to Article 8 of the Fundamental Rights of the European Union, personal data 'must be processed fairly for specified purposes and on the basis of lawful grounds'.[44] Article 5(1)(b) of the GDPR establishes a 'purpose limitation' for data processing, which indicates that data should be collected for specific, explicit, and legitimate purposes and should not be processed further that is inconsistent with those purposes. [45] So, the legal basis should be relevant to and supportive of the specific purposes for which the data is processed. In personalized advertising practices, some companies are eager to use legitimate interests as the legal basis for

[43] ICCL, 'ICCL Lawsuit Takes Aim at Google, Facebook, Amazon, Twitter and the Entire Online Advertising Industry' (2021), para 5 < https://www.iccl.ie/news/press-announcement-rtb-lawsuit/> accessed 8 February 2024.
[44] Célestin Matte and others, 'Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?' (In proceedings of Privacy Technologies and Policy: 8th Annual Privacy Forum, Lisbon, October 2020), 2, para 1 <https://doi.org/10.1007/978-3-030-55196-4_10> accessed 17 January 2024.
[45] The GDPR, art 5(1)(b).

processing,[46] which could be supported by recital 47 of the GDPR, stating that direct marketing is a legitimate interest for processing. However, according to EU law and data protection research studies, only consent can be justified as the legal basis for data processing in personalized advertising through RTB.[47] This creates a gap between regulations and practices, and it is also debatable whether even consent in practice can meet the requirements set by EU data protection law. Therefore, this thesis will delve into this aspect, particularly focusing on the disparity between EU law and practices after the invalidation of TCF by Belgian's DPA on TCF.

Transparency and user control are essential aspects of RTB. The intricate nature of RTB and the extensive use of data often encourage risky data processing practices within ecosystems, resulting in a lack of transparency for data subjects. This issue requires further clarification and addressing within RTB.

The transparency requirement is a fundamental aspect throughout the entire GDPR. Opacity in RTB introduces risks, especially when personal data is obtained from multiple sources, coupled with vague and deceptive expressions of purposes and legal bases. This may hinder data subjects from recognizing and exercising their rights. So, clarifying the gap between data protection laws and legal practices, and identifying possibilities and potential areas that need to be supplemented, is the prerequisite and foundation for achieving transparency. It is also an important aspect that this thesis aims to investigate.

Once we examine how personalized advertising and real-time bidding systems work, particularly who the main players are, it is crucial to explore their roles, interests, and how they interact and comply with EU data protection law, which we will elaborate in next chapter. Understanding these factors is vital for digging into the details of how effective EU laws are in this area.

---

[46] Italian SA, 'TikTok: Italian SA Warns Against 'Personalized' Ads Based on Legitimate Interest' (EDPB News, 15 July 2022) <https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads-based-legitimate-interest_en> accessed 6 October 2023.

[47] ICO, 'Update Report into AdTech and Real Time bidding' (2019), 18, para 3; Chaoqun Li, 'Analysis of the Advertising Technology Industry's Compliance with the General Data Protection Regulation: a Case Study of the CNIL Investigation of the French Advertising Technology Giant Criteo' (Master's thesis, Technische Universität Dresden 2022), 44 <http://dx.doi.org/10.2139/ssrn.4307210> accessed 17 January 2024.

3 Compliance or circumvention? The practices of key stakeholders in the RTB under EU regulations

This chapter aims to explore the legal practices of key stakeholders in the RTB ecosystems. It begins by affirming that their activities fall within the realm of data protection laws, then delves into the compliance efforts of select companies as examples. It will examine their roles, interests, and impact on data protection, as well as the challenges they face in complying with data protection laws. The chapter will provide a solid foundation for examining the effectiveness of EU law in legal practice.

3.1 Understanding 'personal data' under the EU data protection law

Within the context of personalized advertising through RTB, a critical area of exploration involves defining personal data since the advances in the technology of the big data era make it difficult to adequately make the distinction between data and personal data.[48] Questions arise concerning the classification of data as anonymous, pseudonymous, or identifiable, each carrying unique implications within the GDPR's protection framework. This classification serves as the initial step in delineating the respective roles of different participants in RTB, as they are only considered controllers or processors when involved in determining or processing personal data.

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person…directly or indirectly…'. [49] Pseudonymous information, which can be considered information about an identifiable natural person, is included in the scope of personal data under the GDPR, whereas anonymous information is excluded.[50] Understanding 'identifiable' becomes an important step of understanding 'personal data'.

In online ad scenarios, various identifiers are deployed to facilitate tracking and personalized advertising.[51] Although companies may argue that they are processing anonymous personal data, which is not in the scope of the data protection law and the

[48] Jeffrey Bholasing, 'How Technological Advances in the Big Data Era Make It Impossible to Define the 'Personal' in GDPR's 'Personal Data' (2022) 8(3) EDPL 346 < https://doi.org/10.21552/edpl/2022/3/5> accessed 17 January 2024.
[49] The GDPR, art 4(1).
[50] The GDPR, recital 26.
[51] For example, Criteo utilizes a range of identifiers for its services, such as the Identifier of a Criteo cookie, advertising ID, Exchange platform cookie ID, Cross-device ID, and others. See Criteo, 'How We Use Your Data: The Categories of Data Used in the Context of Our Services' (11 March 2022) <https://www.criteo.com/privacy/how-we-use-your-data/> accessed 19 March 2024.

risk of reidentifying risks is limited.[52] However, I think personalized advertising via RTB, identifiers, and many other data together can be regarded as personal data under the GDPR 4(1) for several reasons.

Firstly, identifiers are typically created to access a wide range of user information linked to the identifier, including identity, behavior, and deductive details. Companies can reasonably identify individuals, distinguish them from others, and consequently prompt personalized ads to individuals they select;[53] Secondy, the aggregation of all this information can unveil comprehensive aspects of a person's life, including age, gender, and consumption patterns, making the processing both extensive and intrusive.[54] Even in bid requests, when they sometimes do not contain explicit identifiers, a user's identity can also be revealed because of data aggregation or special characteristics of the user.[55]

Regarding the understanding of 'personal data' in online advertising, the CJEU's judgment provides more detailed clarification, especially on TC String. The TC String is a string that stores encoded user preferences, composed of a combination of letters and characters.[56] This string will be shared among participants in the Open RTB so that they can easily determine what users have consented to and objected to.[57]

The CJEU rules that the TC String shall be regarded as personal data even if it does not contain any information that can directly identify the data subjects because the TC string itself can be regarded as information 'relating to [a] ... natural person' under Article 4(1) of the GDPR.[58] When it is combined with other information, for example, the user's IP address or other identifiers, even if other information is not accessible to IAB Europe, the creator of the TC String, it does not exclude the TC String itself from being regarded as personal data under the GDPR.[59] This is because

---

[52] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), para 35.
[53] ibid, paras 160-161.
[54] ibid, paras 160-161.
[55] Jiří Maršál, 'Legal Aspects of Online Behavioural Advertising' (Master's thesis, Univerzita Karlova 2022), 57, para 2.
[56] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214, para 25.
[57] Gegevensbeschermingsautoriteit, 'The Belgium DPA to Restore Order to the Online Advertising Industry: IAB Europe Held Responsible for a Mechanism That Infringes the GDPR' (2 February 2022), para 4 <https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr> accessed 20 March 2024.
[58] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214, para 43.
[59] ibid, paras 45-47.

when we determine whether a person is 'identifiable,' 'all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly,' need to be considered, which does not require that all of the information enabling the identification of the data subject must be in the hands of one person.[60]

The CJEU's decision gives more flexibility in understanding 'personal data' under the GDPR, especially in RTB, where various participants are involved. In summary, we can see that various information utilized in personalized advertising via RTB generally could be seen as personal data under EU data protection law. It does not require all data to be available for certain companies, as long as the nature of the data allows it being combine with other data and recognize individuals, and re-identification is not impossible considering the efforts, technology, and other means employed for re-identification.

3.2 The key stakeholders in the RTB ecosystems: interests, roles, and compliance practices

It is crucial to clarify the interests, roles, and compliance practices of key stakeholders within the RTB ecosystems. Delving into their interests is vital, as it enables the consideration of multiple perspectives from various participants, ensuring a balanced approach. By understanding the underlying incentives that influence their decisions and compliance efforts, a deeper comprehension of the ecosystem dynamics could be achieved. For example, the interest of processors may incentivize them to process personal data beyond the means and scope defined by controllers, thereby changing their role from processors to controllers in some situations.

Moreover, understanding the roles of stakeholders, defining them are controllers or processors is essential for grasping the essential aspects of their involvement, which subsequently aids in determining their compliance obligations and responsibilities within the entire ecosystems under the GDPR. Lastly, examining their compliance practices serves as a pivotal step in evaluating the effectiveness and implementation of regulations, the tensions between regulations and business models, and potential improvements. In this regard, the focus will be directed toward publishers,

[60] ibid, para 40.

advertisers, AdTech vendors, consent management platforms, and industry associations.

3.2.1 Publishers

Publishers own and operate websites or applications and make content available to users, such as news websites, social media platforms, video streaming services, and others. Many online platforms rely on digital advertising to create revenue rather than using pay mode, which means the content is available after the user's payment, or asks users to choose from them.[61] Since users' impressions or clicks are commonly used metrics for calculating the charges of ads,[62] platforms also strive to collect, utilize, and transfer users' data to participate in RTB. They aim to sell their ad space to the right advertisers at the right time to maximize revenue while minimizing costs and risks.

According to Article 4(7) of the GDPR, a 'controller' is a natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data.[63] In online advertising, publishers leverage the collection of personal data to achieve their objectives, namely, gaining a deeper understanding of their audience's interests, behaviors, and preferences. This enables them to effectively target ads to their audience, thereby increasing the likelihood of ad revenue and enhancing overall website performance.

Typically, DSPs and DMPs carry out data processing based on publishers' instructions, they help to transfer bid requests that contain personal data to other participants in RTB. Large platforms for example Meta and Google, often use their own tool to reach out to advertisers.[64] As a result, publishers should be considered data controllers because of their independent decision-making on how they should

[61] For example, on Der Spiegel, a German news website, where you can choose from 'with advertising and tracking' or 'read ad-free' two options, the former one you can consent and continue, second option you need to pay to avoid ads and no sharing of your data with advertisers < https://www.spiegel.de/> accessed 4 February 2024.
[62] Criteo, 'Terms and Conditions for Advertisers-Retail Media' <https://www.criteo.com/wp-content/uploads/2021/04/Retail-Media-Terms-for-Advertisers_April-2021.pdf> accessed 4 February 2024.
[63] The GDPR, art 4(7).
[64] Jiří Maršál, 'Legal Aspects of Online Behavioural Advertising' (Master's thesis, Univerzita Karlova 2022), 18, para 2.

collect personal data, what they should collect and via what kind of means.[65] In some situations, they can also be joint controller with other participants in RTB. [66]

As one of the important participants in RTB which directly interacts with users, the publisher's privacy policy needs to comply with the data protection law, especially the need to elaborate on how they will collect, process and protect personal data. In practice, publishers usually integrate cookie banners and other consent tools from CMP to obtain and manage user consent, usually, TCF is applied. TCF is developed by IAB, which provides a set of specifications and policies for organizations to communicate and manage user consent.[67] However, the Belgian DPA has declared the TCF invalid, which leaves legal uncertainty for publishers. How to ensure the consent is valid is becoming a tricky question in practice.

According to Article 24 of the GDPR, publishers, when acting as controllers, need to implement 'appropriate technical and organizational measures' to ensure their compliance work. Meanwhile, they need to inform data subjects about the processing of their personal data to comply with the transparency requirement.

3.2.2 Advertisers

Advertisers aim to reach potential shoppers at the right time and at a reasonable cost, aiming to increase the probability of purchase, and return on investment (ROI), and facilitate the right inventory. Their payment for ads incentivizes the entire RTB ecosystem and the utilization of personal data. It is based either on a user's click or impression, so catching the user's attention on online platforms is important for their business. In order to achieve this, they need to develop bidding strategies with DSPs, considering users' characteristics and targeting parameters and decide how they use user's data to make bid decisions.

Advertisers are usually regarded as data controllers because they are able to determine the means and purposes of data processing set in Article 4(7) of the GDPR. For example, advertisers have control over bid prices, targeting criteria, ad creative,

---

[65] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377, para 325.
[66] For example, when publishers are determining purposes and means of processing with CMPs and AdTech Vendors, they can be regarded as joint controllers under
[67] IAB Europe, 'The Transparency & Consent Framework (TCF) v2.2' (16 May 2023) < https://iabeurope.eu/transparency-consent-framework/> accessed 4 February 2024.

and budget allocation, which will determine how personal data will be used in RTB. In addition, after advertisers send the bid request, they may proceed to process personal data, where they can also be considered as data controllers.

The advertisers usually identify their target audience based on demographics, interests, behaviors, and other relevant criteria. They use data from their own customer database and other partners. Based on the data analysis and market research, they define parameters to categorize their potential shoppers. Advertisers' parameters will decide which kind of audience will receive their ads, thereby influencing receivers' first impression about their personal data abused. Thus, ensuring data minimization is the challenging part of their compliance work.

In addition, advertisers rely on a network of collaborators to function effectively. These collaborators include marketing partners, the data supply chain, and AdTech vendors. These entities play a crucial role in the AdTech ecosystems by providing tools, services, and access to personal data. Ensuring that the data received from AdTech companies has a valid legal basis is a critical aspect of their compliance efforts.

Typically, publishers engage with users and obtain consent from them via DMPs, advertisers do not acquire consent separately in RTB.[68] Publishers and advertisers usually process personal data at different stages, the consent from publishers may not guarantee or overlap the processing stage especially consistently profiling from advertisers. Although case-by-case analysis is needed when we allocate the processing activities and obligations for them, but the guarantee of a valid legal basis for processing in the whole process of RTB is vital.

3.2.3 AdTech Vendors

AdTech vendors, also called ad exchanges or intermediaries, play a crucial role in the digital advertising market by leveraging advertising technology through the integration of software systems and tools. Their objective is to assist publishers and advertisers in optimizing their ad campaigns for maximum revenue. This involves

[68] Jiří Maršál, 'Legal Aspects of Online Behavioural Advertising' (Master's thesis, Univerzita Karlova 2022), 73, para 1 <https://dspace.cuni.cz/bitstream/handle/20.500.11956/179019/120437070.pdf?sequence=1&isAllowed=y>accessed 5 March 2024.

efficiently reaching and attracting the right audience at the lowest cost, ultimately maximizing the conversion of ads into purchases. The operational efficiencies and ability to discover audiences are the most important drivers for them.[69] In order to maximize the efficiency of RTB, when AdTech companies receive bid requests, they will send it to multiple DSPs to reach potential advertisers, so it usually has a solid cooperation with both SSPs and DSPs, or some of them also function as a SSP or DSP.

Criteo, a France-based company, is one of the significant participants in online advertising in Europe, utilizing various AI models and machine learning technologies to collect and use personal data, helping their customers reach potential shoppers. For instance, they use Criteo Shopper Graph, intending to accomplish cross-platforms, cross-devices, and offline identifiers, capturing users' behaviors, and offering more related ads.[70] The entire process involves a wide range of data collection, utilization, transfer, and profiling.

Criteo is a representative AdTech company with more than a hundred partners, from which they obtain personal data or share data under certain contractual relationships. International data transfer is also common under its operations. Criteo participates in the TCF and follows IAB Europe's policies, complies with data minimization and privacy design, and defaults under the GDPR. In addition, they contractually require the advertisers and publishers who cooperate with them to comply with Criteo advertising guidelines and supply partner guidelines, and other regulations.[71]

In RTB ecosystems, Criteo can be a data controller when determining the purposes and means of processing. It can also be a data processor by following the instructions of its partners. As an intermediary company, its services, especially its smaller partners' data protection obligations, heavily rely on its contractual obligations and the voluntary conduct outlined in the contract.[72] There is no diligence investigation, binding audit requirement, or even liability for breaching data protection obligations,

---

[69] IAB Europe, 'Attitudes to Programmatic Advertising Report', (November 2023), 13, figure 7. <https://iabeurope.eu/wp-content/uploads/IAB-Europe-Attitudes-to-Programmatic-Advertising-Report-2023-FINAL.pdf> accessed 27 February 2024.
[70] Criteo, 'Retargeting' < https://www.criteo.com/digital-advertising-glossary/retargeting/> accessed 4 February 2024.
[71] Criteo, 'Privacy Policy' < https://www.criteo.com/privacy/> accessed 4 February 2024.
[72] Criteo, 'Criteo Data Protection Agreement' < https://www.criteo.com/wp-content/uploads/2023/04/Criteo-Data-Protection-Agreement-April23_without-Appendix-2.pdf> accessed 4 February 2024.

and other measures to ensure compliance with data protection law in their cooperation.[73] If their contractual partner breaches the contractual obligations without being investigated by the data protection authority, their compliance work on data protection will have significant uncertainty. It is hard to believe that they will have many incentives to prioritize personal data protection without any binding measures.

Moreover, if Criteo is investigated by the data protection authority, they can assert their compliance with data protection regulations by pointing to the clauses within their contracts with partners, which actually lead to a data protection vacuum.[74]

When Criteo acts as a data processor, and their partner as the controller, the utilization of personal data they receive from their partners is also restricted by contractual obligations, except for advertising and market services. In other words, when conducting personalized advertising, it can 'combine personal data it receives from a partner with personal data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with data subjects.' [75]

In my view, companies that hold considerable bargaining power as key participants have an inherent responsibility to ensure and enforce compliance with data protection laws across the entire data supply chain. This obligation includes taking proactive measures to not only scrutinize but also enhance the efficacy of consent mechanisms employed by their partners. It is imperative for powerful participants to exercise due diligence in ensuring that the consent processes align with legal requirements and user privacy.

Furthermore, these influential entities need to actively implement measures that go beyond contractual agreements. This includes robust monitoring and enforcement, utilizing advanced technologies, conducting audits, and carrying out periodic assessments to ensure partners continue to comply with contractual obligations and data protection laws.

---

[73] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), para 46.
[74] ibid, para 48.
[75] Criteo, 'Criteo Data Protection Agreement', 5, section.12.3 < https://www.criteo.com/wp-content/uploads/2023/04/Criteo-Data-Protection-Agreement-April23_without-Appendix-2.pdf> accessed 4 February 2024.

3.2.4 Consent management platforms

Consent management platforms are tools or systems designed and deployed for publishers to manage users' consent for collecting and processing their personal data in online advertising, they usually show to users as cookie banners.

Some CMPs are also members of IAB Europe, they are based on the open RTB Protocols and support the TCF standard. TCF facilitates the capture of user's preferences through CMP, and those preferences are coded and stored in a 'TC String', which will be shared with the participants in the Open RTB so that they can easily know what users have consented to and object.[76] Together with other policies and terms, TCF aims to guarantee that CMPs comply with the data protection framework.[77]

Since CMPs usually act according to the instructions given by publishers, to show users their legal purposes, processing basis, transparency requirements and other information in consent pop-ups,[78] collect user consent and manage objections.[79] so, the CMP is usually regarded as a data processor on behalf of publishers.

Regarding the role of being controller, there are still arguments in practice, some research argues that CMPs can be regarded as data controllers under those situations: when they include additional processing activities in their tool; when they perform scanning and presorting of tracking technologies; when they include third-party vendors by default, and when they deploy interface manipulative design strategies.[80] I think a case-by-case analysis is needed for clarifying their roles, especially in which stages they are deciding their own purposes of processing, and in what situation they are on behalf of publishers or other participants to perform

---

[76] Gegevensbeschermingsautoriteit, 'The Belgium DPA to Restore Order to the Online Advertising Industry: IAB Europe Held Responsible for a Mechanism That Infringes the GDPR' (2 February 2022), para 4 <https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr> accessed 20 March 2024.

[77] IAB Europe, 'The Transparency & Consent Framework (TCF) v2.2' (16 May 2023) < https://iabeurope.eu/transparency-consent-framework/> accessed 4 February 2024.

[78] Cristiana Santos and others, 'Consent Management Platforms under the GDPR: Processors and/or Controllers?'（APF 2021 - 9th Annual Privacy Forum, Jun 2021, Oslo, Norway), 10, para 4 <https://doi.org/10.48550/arXiv.2104.06861> accessed 20 February 2024.

[79] IAB Europe, 'IAB Europe Transparency &Consent Framework Policies' (Version 2023-05-15.4.0.a), section6 <https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/> accessed 20 February 2024.

[80] Cristiana Santos and others, 'Consent Management Platforms under the GDPR: Processors and/or Controllers?'（APF 2021 - 9th Annual Privacy Forum, Jun 2021, Oslo, Norway), 18, para 4. <https://doi.org/10.48550/arXiv.2104.06861> accessed 20 February 2024.

processing, which is the key aspect that determining their role under the EU data protection framework.

CMPs, are created to obtain valid consent from users to comply with the data protection regulations, but the pursuit of interests is making their role rather than a neutral tool. Some CMPs are commercial themselves of compliance also about increasing customer conversion,[81] which incentive them to deploy manipulative design and facilitate consent.

In addition, the role and responsibilities of CMPs are not clearly stated in legal practices, when they are not sure about their legal status, their compliance will mainly market-orientated and operate business activities based on their best interest. In legal practice, they are able to pre-register hundreds of vendors during the installation process on a website, although not all of them will be actual participants in certain auctions, user's data will still be transferred to them, which actually violates the principle of transparency, fairness and minimization principles.[82]

3.2.5 Industry association, IAB Europe for example

There are many organizations that are active in online advertising, aiming to create a responsible digital advertising practice. For example, the Digital Advertising Alliance is a non-profit group led by advertising associations, it sets and enforces privacy rules for digital advertising, providing consumers with more transparency and control across websites and apps.[83] The European Interactive Digital Advertising Alliance is an industry association that offers tools providing simple information about personalized advertising to data-driven advertising companies in Europe.[84] Interactive Advertising Bureau Europe is a European-level association for the digital marketing and advertising ecosystems, which aims to establish frameworks and standards for businesses.[85] One of its significant contributions is that it developed and released the TCF to facilitate online advertising compliance with EU data

---

[81] For example, Quantcast commercial themselves 'Gain double-digital performance advertising outcomes', see < https://www.quantcast.com/home/> accessed 5 March 2024.
[82] Cristiana Santos and others, 'Consent Management Platforms under the GDPR: Processors and/or Controllers?'（APF 2021 - 9th Annual Privacy Forum, Jun 2021, Oslo, Norway), 18, para 4. <https://doi.org/10.48550/arXiv.2104.06861> accessed 20 February 2024.
[83] Digital Advertising Alliance, 'About the Participating Associations', <https://digitaladvertisingalliance.org/about> accessed 4 February 2024.
[84] European Interactive Digital Advertising Alliance (EDAA), 'About Us' <https://edaa.eu/> accessed 4 February 2024.
[85] IAB Europe, 'About Us' <https://iabeurope.eu/about-us/> accessed 4 February 2024.

protection regulations for advertisers, publishers, and consent management platforms, enabling users to make granular choices.[86]

When considering the function of various associations within the framework of EU data protection law, there is room for debate in practical application. However, the recent CJEU ruling in the IAB Europe case has shed light on the classification of these associations as data controllers.[87] IAB Europe thinks that it is not a data controller in the context of RTB. Instead, it asserts that it merely provides information to data subjects in compliance with the GDPR through a streamlined and standardized manner using the CMP. However, the actual processing purposes are determined by the participating organizations.[88]

Contrary to IAB Europe's stance, the Belgian DPA has deemed it a controller, implying its joint controllership with publishers, CMPs, and AdTech vendors within the framework of the TCF and Open RTB.[89]

This decision is based on several grounds. Firstly, IAB Europe interprets the concept of the controller broadly, following case law and guidelines from the EDPB. According to this interpretation, a natural or legal person need not process the personal data themselves or have direct access to be a controller; rather, influence the processing's purposes and means, ultimately impacting data subjects' fundamental rights to privacy and personal data protection, is sufficient.[90] IAB Europe is found to determine the processing purposes and means within the TCF, as outlined in policies developed by IAB Europe and IAB Tech Lab with other members. The opinion of the Belgium DPA was acknowledged by the CJEU.[91]

Referencing the Jehovah's Witness judgment, it is clarified that joint responsibility doesn't automatically imply equal responsibility among participants and does not extend to all stages of processing. Relevant circumstances, especially varying degrees

[86] IAB Europe, 'Transparency & Consent Framework' <https://iabeurope.eu/transparency-consent-framework/> accessed 4 February 2024.
[87] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214.
[88] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377, para 67.
[89] ibid, paras 62-80.
[90] Case C131/12 *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others* [2014] ECLI: EU:C:2014:317, para 38.
[91] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214, paras 52-69.

and stages of processing, must be considered.[92] In this case, IAB Europe can only be considered a controller regarding the subsequent processing when it has significantly influenced the determination of the purposes and methods of that processing.[93] However, the assessment of this question is left to the referring court.

In my opinion, a case-by-case assessment is necessary. According to the CJEU's ruling in 'Fashion ID', joint controllership is not a blanket concept applicable to all phases of a processing operation.[94] The Belgian DPA's decision and CJEU align with this perspective. However, neither of them exercises a thorough examination to ascertain IAB Europe's joint controller role at each stage to what extent and its corresponding obligations. A more thorough analysis is necessary to ensure a precise understanding of the joint controller dynamics and the associated responsibilities in the context of the IAB Europe's involvement.

After the Belgian DPA's decision invalided the IAB Europe's TCF, citing it did not provide a legal basis for processing and also violated other obligations under the GDPR,[95] the CJEU also confirmed the viewpoint that the TC String constitutes personal data, and IAB Europe as a data controller when determining the TCF. IAB Europe is under pressure to conform to GDPR standards. In response, IAB Europe has introduced compliance programs for both CMPs and Vendors aimed at safeguarding the TCF and ensuring adherence to TCF policies by participating organizations.

CMP compliance involves a two-stage process: pre-implementation validation and post-implementation enforcement. Failure to comply may lead to suspension from the TCF. Similarly, TCF Vendor compliance consists of completing a vendor compliance form detailing TCF implementation plans and measures in order to be added to the global vendors list.[96]

---

[92] Case C-25/17 *Tietosuojavaltuutettu v. Jehovan todistajat - uskonnollinen yhdyskunta* [2018] ECLI:EU:C:2018:551, para 69.
[93] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214, para 76.
[94] Case C-40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629, para 72.
[95] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022*[2022] DOS-2019-01377, paras 535-536.
[96] IAB Europe, 'TCF Compliance Programmes', < https://iabeurope.eu/tcf-compliance-programmes/> accessed 3 March 2024.

Furthermore, an accountability platform was released for feedback in December 2023.[97] However, some researchers argue that these measures fail to address security concerns in RTB adequately. The compliance programs lack transparency regarding the handling of personal data post-broadcast by RTB, focusing primarily on end-user device activities. Global accountability platforms rely heavily on self-reporting and are oblivious to unrecorded events.[98] These measures still could not take sufficient measures about who will get the data, and how they will use them from demand-side platforms in RTB. [99]

In essence, while IAB Europe's compliance efforts are commendable, there are lingering doubts about their effectiveness in addressing RTB security issues comprehensively.

3.3 Challenges in enforcing compliance

3.3.1 Complexity of the RTB transaction

The RTB system is an ecosystem where various participants converge. While we provided an overview of the process and main participants earlier, it was merely a simplified explanation. In reality, these participants operate across different stages of the process, and their roles are dynamic, often shifting depending on specific transactions. This dynamic nature complicates efforts by both authorities and stakeholders to define their roles and obligations under the GDPR.

In addition, there are many small entities involved, they can collect vast users' personal data at a low cost, but at the same time they might lack the expertise to navigate complex data protection regulations and contractual obligations from powerful companies in the realm.

The complexity of the ecosystems poses significant challenges in addressing transparency concerns. Ensuring a continuous valid legal basis for the collection and processing of data from various sources by key stakeholders becomes particularly

[97] IAB Tech Lab, 'IAB Tech Lab Launches Accountability Platform to Deliver Greater Transparency in the Use of Personal Data for Addressability' <https://iabtechlab.com/wp-content/uploads/2023/12/Accountability-Platform_Public-Comment_20231214.pdf> accessed 3 March 2024.
[98] Johnny Ryan and Cristiana Santos, 'An Unending Data Breach Immune to Audit? Can the TCF and RTB Be Reconciled with the GDPR?' (2022) Irish Council for Civil Liberties Research Paper, 6-14 <https://ssrn.com/abstract=4064729> accessed 22 January 2024.
[99] ibid 7.

challenging, informing data subjects about their rights, including access to their personal data, the right to object, withdraw consent, and other rights, is also complicated by the ecosystems' complexity. Additionally, allocating these obligations in a manner that is accessible and efficient for users is also a challenging part of compliance work.

3.3.2 Lack of coherent interpretation of regulations and detailed guidelines for participants

The interpretation of data protection laws may vary across member states of the European Union, yet data freely traverses borders. This results in divergent legal practices, impeding a consistent understanding of the law and causing uncertainty for businesses. For example, different from the Belgian DPA's decision, the German DPA had a decision on behavioral advertising that the IAB Europe is not a responsible controller under Article 4(7) of GDPR, it is only an industry association in the field of programmatic advertising.[100]

Furthermore, the EDPB and DPAs lack clear guidelines for the roles of RTB participants within this intricate ecosystem. Consequently, participants possess significant autonomy in determining their compliance measures. However, this autonomy often leads to prioritizing data monetization over responsible data compliance practices, or even if some companies are eager to comply with the law, the complexity of the ecosystems and regulations make it difficult for small companies to tell the accurate states of their processing, their roles and accordingly compliance measures.

Additionally, both large participants and small businesses bear similar responsibilities under the GDPR, despite their differing levels of bargaining power and resources, and their competition position, which will also influence the means of processing in RTB. Therefore, clear guidelines are important to rectify these disparities and ensure fairness and consistency in data protection compliance within RTB.

[100] Datenschutzkonferenz, *Resolution of the Conference of Independent Federal and State Data Protection Supervisory Authorities on Bahavioural Advertising* (4 June 2019) <https://www.datenschutzkonferenz-online.de/media/dskb/20190110_beschluss_verhaltensbasierte_werbung_alt.pdf> accessed 5 March 2024.

3.3.3 Cross-border issues and jurisdictional challenges

Participants in the RTB ecosystems often operate globally, with advertisers, publishers, and ad tech companies situated in different countries. This geographic diversity complicates the management of data flows and introduces cross-border considerations. Usually, data transferring from the EU outside the EEA relies on Standard Contractual Clauses; however, the sufficiency of this protection is still arguable. In addition, RTB participants need to navigate through different legal frameworks and regulations in various jurisdictions, including data protection law, consumer protection law, advertising law, and competition law, which may cause conflicts in legal compliance. Data sovereignty demand in some countries also poses more challenges there.

4 Effectiveness of EU law in regulating personalized advertising via RTB

The efficacy of EU legislation in governing personalized advertising via RTB relies on its capacity to ensure individual privacy rights with fast-developing digital advertising. This chapter aims to analyze the legal basis of data processing and transparency requirements within RTB. It is based on a solid understanding of the technical sides of the ecosystems and the main roles, interests, and compliance work of key participants. The goal is to evaluate the effectiveness of the EU data protection framework in addressing these issues.

4.1 Purposes and legal basis in personalized advertising via RTB

According to Recital 40 of the GDPR, in order to process personal data lawfully, it must be based on the consent of the individuals involved or some other legitimate basis.[101] On one side, this determines how processors handle personal data and what measures they take. On the other side, different legal basis provides data subjects with varying levels of control over their data.

In the digital advertising field, consent, legitimate interests and contractual necessity are commonly used as legal basis, but there is an ongoing debate in legal practice. While many researchers argue that consent should be the sole legal basis for processing personal data in personalized advertising, in reality, either the consent mechanism is not valid, or businesses are opting to use legitimate interests or others as their legal basis. This creates a gap between legislation and actual practice.

This chapter will first survey legal practices, and then analyze the meaning and requirements of valid consent. Afterward, a case will be examined to explore the challenges of obtaining consent. Finally, we will reexamine the feasibility of using legitimate interest as a legal basis for data processing in personalized advertising.

4.1.1 A survey of purposes and legal basis of data processing in practice

To comprehensively understand the real-world impact of consent mechanisms and legitimate interest as legal the basis for data processing, a detailed survey of various participants' purposes and legal basis will be undertaken. Purpose limitation requires data controllers to collect personal data based on their ‘specific, explicit and

[101] The GDPR, recital 40.

legitimate' purposes and process in a way compatible with those purposes, [102] legal bases justifying for processing personal data by the specified purpose, so it is necessary to investigate them together to see if they the legal basis are align with processing purposes. This investigation delves into key aspects to provide insight into the practical implementation of consent mechanisms and legitimate interest as the legal basis for processing, contributing to a better understanding of different participants' compliance with data protection regulations and the protection of data subjects' rights.

The investigation will focus on AdTech vendors who specifically contribute to digital advertising, here we choose Criteo, Open X[103] and the Trade Desk.[104] The survey will cover the following aspects: a. the clarity and specificity of data processing purposes; b. Choice among consent, legitimate interest and others; c. Easy to withdraw, object by data subjects or not; d. How well organizations document user's consent and legitimate interest processes.

Regarding the clarity and processing purposes and choice from consent, legitimate interest and others, we notice that all of the platforms state under EU law the legal basis they are using, mainly relying on consent and legitimate interest for advertising. Most participants, clearly state that they rely on users' consent for personalized advertising, interest-based advertising, and similar purposes.[105]

However, some points that deserve our attention. Firstly, some companies don not distinguish between different purposes; they use both for one purpose, and some of them could still contain personal data and facilitate to a certain extent personalized advertising, making it not easy for data subjects to figure out. For example, The Trade

[102] The GDPR, art. 5(1)(b), Art. 29 WP, *Opinion 03/2013 on Purpose Limitation*, WP 203 (2 April 2013).
[103] OpenX operates an advertising exchange that connects companies offering advertising space on their platforms. OpenX typically functions as SSP. See OpenX, 'OpenX Ad Exchange Privacy Policy' (19 December 2023) <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/#section-1> accessed 21 March 2024.
[104] The Trade Desk typically functions as a DSP. They provide technology that helps advertisers and their advertising agencies manage digital advertising campaigns across many channels. See the Trade Desk, 'Privacy and the Trade Desk Platform' (26 January 2024) <https://www.thetradedesk.com/us/privacy> accessed 21 March 2024.
[105] Criteo, 'How We Use Your Data?' (11 March 2022) <https://www.criteo.com/privacy/how-we-use-your-data/> accessed 22 March 2024; OpenX, 'OpenX Ad Exchange Privacy Policy, Why Do We Collect, Use, and Store This Personal Data' (19 December 2023) <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/#section-1> accessed 21 March 2024; The Trade Desk, 'Privacy and the Trade Desk Platform, European Union Controller/Processor Designation and Legal Bases' (26 January 2024) <https://www.thetradedesk.com/us/privacy> accessed 21 March 2024.

Desk, an AdTech company usually as a DSP, uses consent or legitimate interest to 'create identifiers for interests for groups.'[106] It depends on how they collect personal data, and it is not clear for data subjects. OpenX, an Ad exchange company, which relies on consent or legitimate interest to 'control the content and frequency of ads,' using real-time information about the context to ensure the relevance of the ads, which may include information of data subjects.[107]

Additionally, many of them use legitimate interest as a legal basis to train their models to facilitate personalized advertising, which is not clear how personal data may be used when it relates to business secrets but still facilitates personalized ads to a certain extent.[108]

Secondly, the format is vague on certain websites, and it is not easy for data subjects to realize when we are talking about using personal data for personalized advertising, what categories of data we are talking about.[109] This kind of vague and sweeping description gives some interpretation space for companies and uncertainty for data subjects. For example, they may turn to using legitimate interest to process personal data when data subjects opt out of their consent for specific purposes, especially when they state two legal bases for this certain purpose.

Ensuring ease of withdrawal or objection for data subjects is crucial. According to a survey of various participants, most companies offer clear instructions for opting out of personalized advertising. Furthermore, data subjects also retain the right to object to legitimate interest. Typically, these options are presented within a subset of choices, often under a section detailing data subjects' rights in the privacy policy, facilitating their exercise.

However, regarding the documentation of user consent and legitimate interest processes by organizations, privacy policies often provide limited information.

---

[106] The Trade Desk, 'Privacy and the Trade Desk Platform, European Union Controller/Processor Designation and Legal Bases' (26 January 2024) <https://www.thetradedesk.com/us/privacy> accessed 21 March 2024.
[107] OpenX, 'OpenX Ad Exchange Privacy Policy, Why Do We Collect, Use, and Store This Personal Data' (Last Updated 19 December 2023) <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/#section-1> accessed 21 March 2024.
[108] Criteo, 'How We Use Your Data?' (11 March 2022) <https://www.criteo.com/privacy/how-we-use-your-data/> accessed 22 March 2024.
[109] OpenX, 'OpenX Ad Exchange Privacy Policy, Why Do We Collect, Use, and Store This Personal Data' (19 December 2023) <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/#section-1> accessed 21 March 2024.

Instead, such documentation is commonly found in investigations carried out by data protection authorities and in press releases. This step is crucial because companies can obtain personal data from various sources. Failure to obtain consent for processing for personalized advertising purposes poses a threat to data subjects' rights to personal data and privacy.

Furthermore, it is essential for data subjects' rights concerning withdrawal or objection, as they typically receive notifications from controllers or processors regarding successful withdrawals or valid objections, but lack independent verification of this information.

The case of Criteo, as observed in the decision by the French data protection authority, underscores the importance of proper documentation. Criteo's partners were unable to furnish evidence demonstrating consent from data subjects, and Criteo omitted to request this information during their interactions. Consequently, during the DPA investigation, insufficient evidence was available to confirm that consent was lawfully obtained from data subjects.[110]

4.1.2 Meaning of valid consent

According to Article 4(11) of the GDPR, valid consent is defined as 'any freely given, specific, informed, and unambiguous indication of the data subject's wishes,'[111] which aims to give data subjects more control over their data.

When we delve into the concept of 'freely given,' various considerations come into play, including power imbalances, conditionality, granularity, and avoiding detriment.[112] Power imbalances, for instance, arise in situations like employment or when a public authority is the one obtaining consent, showing a strong and potentially coercive position.

Conditionality is about refraining from tying consent to unnecessary terms or conditions, ensuring that consent is not linked to aspects beyond the essential requirements of a contract or service. The granularity aspect emphasizes the

[110] CNIL, 'Personalised advertising: CRITEO Fined EUR 40 Million' (22 June 2022) < https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million> accessed 10 February 2024.
[111] The GDPR, art.4(11), art.7.
[112] The GDPR, recital 43, EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679,* Version 1.1 (4 May 2020).

importance of allowing data subjects to give separate consent to different data processing,[113] rather than bundling them together for multiple processing purposes. This is particularly relevant as services often involve various processing operations for distinct purposes.[114] Lastly, the concept of detriment underscores the need to ensure that freely given consent does not result in harm to the data subject.[115]

Moving on to the 'specific' element, this requirement aims to empower data subjects with control and transparency. Consent must be tied to 'one or more specific' purposes, allowing data subjects to exercise their choice for each.[116]

In terms of being 'informed,' the provision of minimal yet crucial information is key. This includes details such as the 'identity of the controller and the purposes of processing,' [117]the types of data to be collected and used,[118] the right to withdraw consent,[119] information about the use of data for automated decision-making,[120] and the potential risks associated with data transfers and appropriate safeguards in Article 46 of the GDPR.[121] [122]The way this information is conveyed is equally important, it should be presented in an intelligible and easily accessible form, using clear and plain language while avoiding unfair terms.[123]

Furthermore, for consent to be deemed valid, it must be an unambiguous indication of the data subject's wishes. This needs an affirmative and clear action from the data subject, discouraging reliance on silence, pre-ticked boxes, or inactivity, especially when processing involves multiple purposes.[124]

---

[113] The GDPR, recital 43.
[114] The GDPR, recital 43, EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679,* Version 1.1 (4 May 2020), s 42.
[115] The GDPR, recital 42.
[116] The GDPR, recital 43, EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679,* Version 1.1 (4 May 2020), s 55.
[117] The GDPR, recital 42.
[118] Art. 29 WP, *Opinion 15/2011 on the Definition of Consent,* WP 187(13 July 2011)19-20.
[119] The GDPR, art.7(3).
[120] The GDPR, art.22（2)(c).
[121] Under the GDPR Art.49 (1)(a), specific information is required about the absence of safeguards described in Art.46, when explicit consent is sought. Art. 29 WP, *Opinion 15/2011 on the Definition of Consent,* WP 187(13 July 2011),19.
[122] EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679,* Version 1.1 (4 May 2020), s 64-65.
[123] The GDPR, recital 42.
[124] The GDPR, recital 32.

Considering additional conditions for valid consent, as outlined in Article 7.1 of the GDPR, [125]the burden of proof lies with the controller. They must demonstrate the existence of valid consent throughout the entire data processing process. Additionally, the withdrawal of consent should be as easy as giving consent[126] and should not impose detriment, cost, or a reduction in service levels to the data subject. Failure to meet these principles may render the consent mechanism non-compliant with the GDPR.[127]

4.1.3 How to obtain valid consent?

When considering the validity of consent, we must not only adhere to the legal definition but also assess whether the consent effectively fulfills its role as outlined in data protection laws. It is evident from the earlier part of the discussion that the regulations and guidelines for obtaining valid consent are stringent.

In practice, the most common way to obtain consent is via Cookie banners, however, for policymakers and data protection authorities, it is not possible to exercise a fully automatic consent verification by technical means, so users' perceptions and experience with the website's consent implementation is still important for evaluation the validity of consent mechanisms. [128]

Users often trade their data for convenience without scrutinizing the specifics of their consent and its implications, plus many participants in RTB don not have compliance strength and motivations, making it difficult to meet consent standards in the context of RTB.

This prompts critical questions about the adequacy of relying solely on consent to safeguard personal data. Are we adequately protecting the data subject's interests by solely focusing on the technical validity of consent? Should policymakers, intervene to determine the actions controllers and processors must take, irrespective of consent? This discussion is not intended to undermine the validity of the consent system. Instead, it emphasizes the necessity of evaluating the efficacy of consent

[125] The GDPR, art.7(1).
[126] The GDPR, art.7(3).
[127] EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, Version 1.1 (4 May 2020), s 114-116.
[128] Cristiana Santos and others, 'Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners' (2020) TechReg 91, 92, <https://doi.org/10.26116/techreg.2020.009> accessed 8 February 2024.

mechanisms within the legal framework, and the importance of supplementing consent with additional measures to enhance personal data protection.

Upon closer examination of the complexity surrounding personalized ads and the RTB ecosystems, it becomes evident that all participants involved in this process collect and share data from their partners, which rely on contractual obligations that guarantee their partners collect personal data on a legally legal basis.

For data subjects, navigating this landscape can be challenging, since when we may think we are dealing with this company, but actually much more. So, it is essential to address the practical challenges and implications of obtaining consent in a manner that is transparent, understandable, and meaningful for data subjects specifically in RTB.

When considering how to obtain valid consent, it is vital to address several key aspects. One such aspect involves establishing a comprehensive online advertising management tool that spans across companies and devices. This tool would enable data subjects to collectively exercise their rights regarding personalized advertising. There are some attempts, but far from enough.

For instance, 'Your Online Choices,' developed by the European Interactive Digital Advertising Alliance (EDAA), offers users the ability to manage their preferences and opt out of personalized advertising from participating companies.[129] However, it primarily operates through self-regulatory mechanisms, and many companies may not be included in the program or fall outside its jurisdiction. Consequently, its effectiveness may be limited. In a recent attempt, it failed to provide information on my status with 75 companies within a span of 3 hours.

Additionally, it is crucial to consider the granularity of consent. Providing users with granular control over their consent preferences allows them to specify their preferences for different types of data processing and advertising. This includes options for opting in or opting out of personalized advertising and data-sharing practices.

[129] EDAA, 'Your Online Choices, A Guide to Online Behavioural Advertising' <https://youronlinechoices.eu/> accessed 10 February 2024.

Moreover, maintaining auditable records of user consent, in other words, being able to demonstrate the validity of consent is essential, so just rely on a contractual relationship, then simply tuck consent inside a contractual 'carpet bag' that gets passed around to everyone else in their chain as soon as users clicks 'I agree' is not valid and efficient.[130] These records should include details such as the date, time, and scope of consent provided by each user. They should be easily accessible and able to serve as evidence of compliance with data protection regulations when necessary.

The establishment of a comprehensive, standardized, and concise consent mechanism has been subject to regulatory requirements, with involvement from consent management platforms and industry organizations like IAB Europe.

However, the recent invalidation of the Transparency and TCF in RTB by the Belgian data protection authority has sparked industry uncertainty and argumentation regarding the legality of consent practices and their future implications. This issue will be explored in detail in the following section of this thesis.

4.1.4 The analysis of the feasibility of the Transparency and Consent Framework after the Belgian DPA's decision on IAB Europe, a case study

The TCF, developed by IAB Europe, is a tool that relies on standardization for RTB participants to facilitate compliance with data protection law, ePrivacy Directive, GDPR, guidelines from the EDPB and national data protection authorities [131] and also give data subjects more control over their data. Usually, publishers integrate the TCF into their platform using a CMP, when a user visits a website, the CMP presents a consent interface that informs the user about the purposes of their data processing for a user to choose. Then CMP communicates the user's choices and preferences to other participants via a standalized TC String for data processing.

On 2 February 2022, the Belgian DPA ruled that TCF in RTB does not comply with the GDPR and ePrivacy Directive, it failed to offer a valid legal basis for processing

[130] Natasha Lomas, 'How a Small French Privacy Ruling Could Remark Adtech for Good' (Techcrunch, 20 November 2018), para10 <https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/> accessed 8 February 2024.
[131] IAB Europe, 'Transparency & Consent Framework, what is the Transparency & Consent Framework (TFC)' <https://iabeurope.eu/transparency-consent-framework/> accessed 8 February 2024.

data in RTB[132] for the following reasons. Firstly, the purposes for processing are not clearly stated and even misleading in some cases; secondly, the user interface of the CMPs does not provide an overview of the categories of data collected; thirdly, it is difficult for users to obtain more information about the identity of all controllers they give consent to, and the information is too general and recipients are too many; lastly, the withdrawal of consent is not effective. [133]

From the reasoning, it seems like complying with the consent requirements set in the GDPR and guidelines is not possible in the RTB if they rely on the interpretation strictly because of RTB's complex nature.

On the one side, authorities argue that consent should be rely as only legal basis, but the interpretation actually excludes the TCF in RTB from compliance with the data protection law. [134] The authority also noticed that the recipients of the TC String are so many, especially DSPs, so it is not possible for the user to read their information of them even if it is available for users, so to what extent do the consent mechanisms in RTB is playing its role of endow control of their personal data is still arguable.

On the other side, TCF only offers standardized consent rather than providing changed consent signals to the AdTech vendors, and there is no measure to ensure that AdTech vendors cannot continue their processing based on a previously received consent signal,[135] so withdrawal consent for data subjects would not be as easy as obtain consent in this ecosystem.

So, when authorities examine the consent mechanisms in RTB, do they actually consider the implementation of it, and the balance of interest between different participants in RTB.[136] Or we can infer that the RTB ecosystems itself are not based on the adequate legal basis of the data protection law?

---

[132] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377, paras 424-425.
[133] ibid, paras 429-440.
[134] Gabbi Meskenaite, 'An Examination of the Criteria for Valid Consent Under the GDPR in the Light of the Rationale and Technological Neutrality' (Master's thesis, Lund University 2022Technische), 1, accessed 8 February 2024.
[135] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377, para 438.
[136] Gabbi Meskenaite, 'An Examination of the Criteria for Valid Consent Under the GDPR in the Light of the Rationale and Technological Neutrality' (Master's thesis, Lund University 2022Technische), 1, accessed 8 February 2024.

Despite the uncertainty surrounding TCF in RTB, the importance of TCF or similar signals cannot be ignored. These signals are widely utilized by businesses and endorsed by various stakeholders within the ecosystems, such as EDPB,[137] Access Now, None of Your Business (NOYB), and EDRI.[138]

However, current legal practices require further improvement. For instance, considerations need to extend to technical features, the granularity of user preferences within the private signal, determining the responsible party for decision-making and establishing mechanisms to mandate the signal's use.[139]

All of the issues are amplified in the RTB, the effect of consent should not be neglected when it actually gives data subjects' data self-determination and control, and enhanced transparency, but it is far from enough just to argue the rationality of the consent as a legal basis in RTB, but we also need to realize that it is not an comprehensive tool, other necessary measure or even legitimate interest and proactive intervention and supervision from data protection authorities are still need.

4.1.5 Examining the viability and dilemmas associated with using legitimate interest as a legal basis

Legitimate interest is a broad and vague concept that can be interpreted flexibly and extensively by controllers. It also reflects the dynamic relationship between data subjects and controllers. Furthermore, it is widely used as a legal basis by controllers in personal data processing practices, which has a close relationship and vital impact on the interests of data subjects.

Typically, a balancing test plus an opt-out option for data subjects serve as the main tools to present controls and safeguards on processing. If it has been well-designed and safeguards are in place, this means that the legitimate interests of the participants are not overridden by either the interests or privacy rights of the data

---

[137] EDPB, *Statement 03/2021 on the ePrivacy Regulation* (9 March 2021) <https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf> accessed 5 March 2024.

[138] Access Now, NOYB and EDRI, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (2021) <https://www.accessnow.org/cms/assets/uploads/2021/07/ePrivacy-4-column-Access-Now-noyb-EDRi.pdf> accessed 11 February 2024.

[139] Cristiana Santos & Harshvardhan J. Pandit, 'How Could the Upcoming ePrivacy Regulation Recognise Enforceable Privacy Signals in the EU?' (2023) OSF Preprints <https://doi.org/10.31219/osf.io/xvyf3> accessed 11 February 2024.

subjects. However, it is more commonly interpreted by controllers, supervisory authorities, national courts, and the CJEU, but it is not easy for data subjects to explain unless the case is reported to the data protection authorities.

In personalized advertising via RTB system practices, companies are eager to seek legitimate interest or other legal basis rather than data subjects' consent as a legal basis to process personal data. For example, in CRITEO case, the company argues that they believe that users' interests are aligned with the capabilities of a training model that delivers more personalized advertisements.[140] In recital 47 of the GDPR, it also mentioned that direct marketing is the legitimate interest for processing.[141]

However, according to article 5(3) of e privacy Directive and case law, most of legal researchers and authorities hold a different opinion, they think that legitimate in interests is not apply because personal data of a large scale and with significant impacts for the data subjects are processed in connection with personalized online advertising.[142] Taking Tiktok for an example, when they seek to change their legal basis for personalized advertising from consent to legitimate interests, the decision was against by Italian DPA. [143]

However, the question arises: why is legitimate interest still a topic of discussion when the use of consent for processing is becoming a consensus in legal academics and practices? In my opinion, legitimate interest, when coupled with appropriate safeguards and controls, actually guarantees data subjects minimum protections even when consent mechanisms are invalid. While consent prioritizes individual autonomy and choice, legitimate interest considers the broader societal and commercial interests at play, which is important for businesses in practice.

---

[140] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023).
[141] The GDPR, recital 47.
[142] ICO, 'Update Report Into AdTech and Real-time Bidding' (2019), 18, para 3; Chaoqun Li, 'Analysis of the Advertising Technology Industry's Compliance with the General Data Protection Regulation: a Case Study of the CNIL Investigation of the French Advertising Technology Giant Criteo' (Master's thesis, Technische Universität Dresden 2022), 44 <http://dx.doi.org/10.2139/ssrn.4307210> accessed 17 January 2024.
[143] Italian SA, 'TikTok: Italian SA Warns Against 'Personalized' Ads Based on Legitimate Interest' (EDPB News, 15 July 2022) <https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads-based-legitimate-interest_en> accessed 6 October 2023.

Additionally, the assessment of consent and data protection from the law is usually in backward status and performative, the legitimate interest assessment post advanced obligation for data controllers.

As previously argued, the consent mechanism appears to fall short in addressing the diverse interests of participants in RTB, highlighting existing gaps between legislation and the actual practices of online digital companies. In light of this, utilizing legitimate interest as a legal basis and conducting a balancing test typically necessitates controllers to satisfy three cumulative conditions: (a) the pursuit of a legitimate interest by a data controller or by third parties to whom the data are disclosed; (b) processing data for the purpose of the legitimate interests pursued; (c) ensuring that the fundamental rights and freedoms of the individuals affected by the data protection do not outweigh the legitimate interest pursued. [144]

Typically, a balancing test is required before resorting to legitimate interest as a legal basis. Moreover, in addition to the aforementioned conditions, other safeguards such as technical measures for data protection and transparency requirements should also be taken into consideration.[145] Thus, in my view, this process offers flexibility and efficiency for digital advertising participants, enabling them to maintain a competitive edge in this field.

However, as many other researchers have pointed out, applying legitimate interest directly in personalized advertising remains challenging. Essentially, while direct marketing may be conducted under this personalized advertising scenario, individuals' fundamental rights still take precedence over other participants' commercial interests. Furthermore, legitimate interests still encounter issues concerning transparency and control, which can be easily abused and explained away by more influential participants, thereby introducing uncertainty into the legal framework.

Consequently, a dilemma arises when selecting the appropriate legal basis for personalized advertising. When consent seems ineffective in practice, determining

[144] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. , Rīgas pašvaldības SIA 'Rīgas satiksme'* [2017] ECLI:EU:C:2017:336, para 28.
[145] Office of the Data Protection Ombudsman of Finland, 'Controller's Legitimate Interests'< https://tietosuoja.fi/en/controller-s-legitimate-interests> accessed 11 February 2024.

sufficient controls and safeguards for the consent mechanism or viable alternatives becomes a complex question within this domain.

4.1.6 Evaluating the efficacy of EU legislation in establishing the legal basis for data processing in RTB

Upon examining the concepts of consent and legitimate interest, it becomes evident that neither offers a sufficient legal basis for data processing in RTB. Consent mechanisms are hindered by the complexity of contractual relationships and challenges associated with withdrawal procedures. Similarly, the legitimate interest of controllers in personalized advertising often fails to outweigh the fundamental interests of data subjects, rendering it an inadequate legal basis for data processing.

Although legal frameworks were not specifically designed for processing personal data in recommending systems via RTB, discrepancies between legislative design and implementation create urgent issues requiring attention from policymakers. As RTB symbolizes the digital world and increasingly complex commercial models emerge, it becomes imperative to either align the entire RTB ecosystem with EU data protection standards or implement alternative measures to safeguard the interests of data subjects.

4.2 Transparency

Transparency plays a crucial role in data protection, but it faces significant challenges within the RTB ecosystems. In this section, we delve into the detailed concept of transparency requirements, conduct a case study to assess the feasibility of meeting these requirements in RTB, and subsequently explore the challenges associated with achieving it. In the end, we will evaluate the effectiveness of EU law in addressing this aspect.

4.2.1 Understanding transparency in the EU data protection framework

Transparency requirement is a critical side of the data protection framework in EU data protection law. According to the EU Charter of Fundamental Rights, everyone has the right to data protection and their data should be processed based on a certain legal basis laid down by law fairly, they also have the right to access and rectify. [146] This is followed and elaborated in GDPR that personal data shall be processed

[146] European Union, Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art.8.

'lawfully, fairly and in a transparent manner in relation to data subject',[147] which sets transparency as one of the requirements of data processing. More specifically, transparency is about data subjects having the right to know why and which of their personal data are collected, used, consulted, or otherwise processed and to what extent and how the personal data are or will be processed,[148] who is involved in.

In the GDPR, transparency obligations mandate that controllers provide clear, accessible, fair processing information to data subjects. This includes details on data collection from the data subject,[149] data obtained from other sources,[150] as well as data subjects' rights to access, rectification, erasure, restriction of processing, notification obligations regarding rectification or erasure of personal data or restriction of processing, data portability, automated individual decision-making, and objection.[151]

The requirement emphasizes the use of simple and clear language and easily accessible formats.[152] One of the most important transparency obligations for controllers require them to empower data subjects to control their personal data, for example, data subjects need to consent if it applicable. Art. 29 WP gives clear guidelines on transparency under the GDPR.[153]

As a key aspect of the GDPR, transparency covers the whole life circle of data processing, ensuring that data subjects understand their rights and controllers' obligations. Failure to uphold transparency in the RTB ecosystems may prevent data subjects from exercising their rights, resulting in a loss of control over their personal data. For controllers it will potentially lead to abuse of personal data, inadequate protection of data subjects under the GDPR, and violations of data protection laws eventually.

---

[147] The GDPR, art 5(1)(a).
[148] European Data Protection Supervisory, 'Transparency', <https://www.edps.europa.eu/data-protection/our-work/subjects/transparency_en> accessed 12 February 2024.
[149] The GDPR, art.13.
[150] The GDPR, art.14.
[151] The GDPR, arts.15-22.
[152] The GDPR, art.12, recital 39.
[153] Art. 29 WP, *Guidelines on Transparency Under Regulation 2016/679*, WP260 rev.01 (11 April 2018) <file:///Users/nandao/Downloads/20180413_article_29_wp_transparency_guidelines_7B894B16-B8B9-B044-ED400A6DBAA4FA60_51025.pdf> accessed 28 March 2024.

The DSA, functioning as a comprehensive horizontal online regulation,[154] seeks to govern intermediary services, hosting services, and online platforms with the goal of establishing a safer digital environment. It aims to empower users with greater control and options, ultimately safeguarding the fundamental rights of citizens.[155]

The DSA has been applicable across the EU since February 17, 2024. Transparency requirement is also an important aspect of this regulation, by imposing transparency obligations towards users of online platforms, enabling them to make use of their rights as data subjects, the DSA supplements the GDPR to better realize the rights of data subjects and enhance transparency. [156]

In the DSA, there is a due diligence obligation to ensure a transparent and secure online environment, for instance, all providers of intermediary services must publish annual reports on their content moderation practices.[157] For very large operating platforms and very large online search engines, additional transparency requirements apply. There is a DSA transparency database which is used for providing information from providers of hosting services to users whenever they remove or otherwise restrict access to their content to increase the transparency of the processing. [158]

Furthermore, the DSA establishes regulations for online advertising. Platforms displaying ads are required to furnish recipients of the service with transparent and real-time information, including relevant parameters that identify them as recipients.[159] This provision facilitates data subjects' comprehension of the rationale behind ad delivery to them and the criteria involved. The Commission also encourages a code of conduct to ensure further transparency of online advertising at the national level or industries.[160]

---

[154] Sam Wrigley and others, 'My Name Is Personalised_ Political_Advertiser.py and I Approve This Message: Regulating Automated and Targeted Political Advertising in EU Law' (2023) 13 University of Luxembourg Law Research Paper, 12, para 1 <http://dx.doi.org/10.2139/ssrn.4561013>accessed 17 January 2024.
[155] European Commission, 'Questions and Answers: Digital Services Act, What is the Digital Services Act?' (Questions and answers, 25 April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348> accessed 4 October 2023.
[156] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final 'Explanatory Memorandum, Context of the Proposal, Consistency with Other Union Policies', 5, para 2 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825> accessed 28 March 2024.
[157] The DSA, art.13.
[158] European Commission, 'DSA Transparency Database FAQ', para 1, <https://transparency.dsa.ec.europa.eu/page/faq> accessed 12 February 2024.
[159] The DSA, arts. 24, 30.
[160] The DSA, art. 36.

Moreover, recipients have access to the parameters of the recommending system, along with options for recipients to modify or influence these parameters. This includes offering at least one option that is not based on profiling.[161] Additionally, the DSA includes provisions to prevent the use of dark patterns, also known as deceptive commercial practices.[162]

The AI Act [163]is a proposal from European Commission, which aims to establish a legal framework for AI, employing a risk-based approach tailored to various risk levels in different sectors and its scope extends beyond the exclusive focus on personal data processing.[164] AI models are deployed broadly on online platforms and AI Act is to ensure responsible and trustworthy of AI systems. AI Act mandates that high-risk AI systems must be designed and developed in a way that ensures their operation is sufficiently transparent, and make sure providers and users can reasonably understand how these systems function. [165]

As regulations address online personalized ads in RTB powered by AI models and other technologies, transparency is increasingly regarded as a crucial concept. Individuals expect to access information easily, clearly, and in an accessible format. Therefore, in the next section, we will shift our focus to legal practices, examining the challenges of transparency and the disparities between legislation and implementation.

4.2.2 Is that possible to meet transparency obligations under EU law in RTB ecosystems? A case study

On 15 June 2023, the National Commission on Informatics and Liberty (CNIL) fined Criteo 4 million euros for the following reasons: a) failure to demonstrate that the data subject gave its consent; b) failure to comply with the obligation of information and transparency; c) failure to respect the right of access; d) failure to comply with

[161] The DSA, art. 29.
[162] The DSA, recital 57-58.
[163] European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts [2024] P9_TA(2024)0138 <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf> accessed 28 March 2024.
[164] Elisabeth Steindl, 'Practitioners' Corner ·Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in light of the Draft AI Act and its Interplay with the GDPR' (2022) 8(2) EDPL, 313, para 2 <<DOI https://doi.org/10.21552/edpl/2022/2/20> accessed 28 March 2024.
[165] The AI Act, art.13.

the right to withdraw consent and erasure of data; e) failure to provide for an agreement between joint controllers. So, Criteo violates article 7.1, 12-13, 15.1, 7.3, 17.1 26 of the GDPR.[166]

Looking at this decision on a smaller scale, CNIL determined that Criteo violated transparency obligations due to the unclear and ambiguous descriptions of its data processing purposes, potentially leading users to provide misleading consent. However, I believe that all breaches in this case, stemming from the lack of transparency within the RTB ecosystems, can be attributed to the breach of transparency obligations under the GDPR.

In the previous chapter, we discussed the challenges associated with obtaining consent under the GDPR in the context of RTB, illustrating that it is difficult, and sometimes even impossible to meet consent requirements. In this case, consent emerges as a critical issue, shedding light on the complex mechanisms of RTB. CNIL ruled that Criteo failed to implement measures to ensure that the personal data they processed had obtained valid consent.

Additionally, more than half of their partner companies did not secure valid consent, yet Criteo lacked supervision measures.[167] As we explored in Section 4.3.1, it becomes evident that almost all participants in the ecosystems rely on others to facilitate digital advertising, especially regarding data sources and user's identification.

However, their reliance on partners' policies and legal obligations for data collection methods means they lack control, particularly in legal compliance. Most participants only enforce contractual obligations or restrictions or rely on audits after breaches occur. Thus, ensuring valid consent in advance, transparency and data subjects' control throughout the entire ecosystem becomes a significant challenge.

The way Criteo explained the reasons for processing data and the legal basis for it was a big focus in this case about transparency. The CNIL said that Criteo's explanations were unclear and too broad, making it hard for users to understand how their data would be used. This made it tough for people to object to their data being used this

[166] CNIL, 'Personalised Advertising: CRITEO Fined EUR 40 Million' (22 June 2022) <https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million> accessed 10 February 2024.
[167] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), paras 43-80.

way.[168] The CNIL is pretty strict about this, looking closely at Criteo's statements to see if they were misleading. When looking back at Criteo's privacy policy, it did lay out the reasons for processing data, the legal basis, and the types of data being used via a clear table, but it is important to note that Criteo also said they use the same kinds of data used for showing personalized ads to improve their ads performance, based on the company's interests.[169] Regarding whether this meets the transparency requirements, the CNIL did not provide a clear opinion.[170]

It can be seen that there is often a lack of explicit standards in determining transparency requirements, leaving room and uncertainty for interpretation and resulting in various practices in compliance. As for what purposes should rely on explicit consent as the processing basis to achieve personalized advertising, the law does not draw a clear line here. For example, whether indirectly promoting personalized advertising meets the requirements is highly dependent on a case-by-case assessment.

However, regarding the privacy policies of other participants, many companies still have vagueness expressions for processing purposes. Therefore, data subjects find it difficult to determine whether personal data can indirectly achieve personalized advertising through a certain purpose, leading to difficulties for data subjects to understand and exercise their rights, which is similar to directly excluding the motivation for data subjects to exercise their rights in today's attention-driven world.

Ensuring the efficient exercise of data subjects' rights is an important aspect of transparency. In the case at the handle, the CNIL ruled that Criteo failed to respect data subjects' rights to access their personal data, withdraw their consent, and request to be forgotten. It ruled based on that Criteo could not provide all the requested personal information in a clear and understandable manner,[171] which is actually as important as the content of the transparency information they provided,

[168] ibid, paras 96-98.
[169] Criteo, 'Privacy Policy' (11 March 2022) < https://www.criteo.com/privacy/> accessed 13 February 2024.
[170] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), para 103.
[171] ibid, para 121.

just as Art. 29 WP stated 'the concept of transparency in the GDPR is user-centric rather than legalistic'.[172]

However, the comprehensiveness of data and clarity often conflict with each other, so the extent and level of detail that data controllers should provide is unclear, resulting in a lack of clarity in practice. This also raises questions about whether Criteo could identify a person's data without revealing other users' data and if they could ensure that the information they provided was understandable to the average person. In my opinion, achieving this in the RTB ecosystems is not easy, as we discussed earlier, group targeting is common in recommender systems via RTB, and AI models are widely used, so it may bring challenges to explainable and distinguishable.

Regarding the right to be forgotten, Criteo stated on their website that 'individuals wishing to withdraw consent or exercise their right to erasure could click on 'disable Criteo services' to stop receiving ads from Criteo and tracking and matching their identifiers'.[173] However, this does not mean that the data subject's data will be deleted from Criteo's operations, as processing may still occur based on Criteo's legitimate interests. This differs from people's understanding of this right.

Furthermore, in the case of Case C-507/17, the CJEU ruled that the right to erasure is not absolute and is granted only when an individual's personal data protection rights outweigh the public interest in maintaining access to the information.[174] This raises the question of whether controllers' legitimate interests in processing also need to be considered and balanced against data subjects' erasure right. If so, how and what factors need to be taken into consideration? There is a lack of detailed illustrations.

In accordance with Article 26 of the GDPR, when joint controllers are involved, the respective responsibilities, especially regarding the exercise of data subjects' rights, their roles, and relationships, should be clearly defined and made available to data subjects.[175] In this case, according to CNIL's opinion, the allocation of obligations

---

[172] Art. 29 WP, *Guidelines on Transparency Under Regulation 2016/679*, WP260 rev.01 (11 April 2018) , 5, s 4 <file:///Users/nandao/Downloads/20180413_article_29_wp_transparency_guidelines_7B894B16-B8B9-B044-ED400A6DBAA4FA60_51025.pdf> accessed 28 March 2024.
[173] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), para 125.
[174] Case C-507/17 *Google LLC, successor in law to Google Inc., v. Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772, paras 60-61; Case C131/12 *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others* [2014] ECLI: EU:C:2014:317, para 99.
[175] The GDPR, art. 26.

among joint controllers must encompass all obligations under the GDPR to determine which joint controller is responsible for each of those obligations.[176]

However, the investigation showed that 'the agreements signed by the company and its partners do not specify certain respective obligations of the data controller regarding GDPR requirements. These include obligations such as exercising data subjects' rights, notifying supervisory authorities and data subjects of data breaches, and conducting impact assessments in accordance with Article 35 of the GDPR'.[177] When data subjects do not know how and to whom they can exercise their rights, which is a violation of transparency obligation.

For each participant who typically has more than a hundred partners, they are joint controllers with some of them, and usually not all of them are easy to reach out to by data subjects, if they do not actually understand the data processing in RTB, data subjects could not learn in advance about the scope and consequences of processing, which will lead to a surprise them at a later point of processing.[178] While it may be easier to identify such cases with companies like Criteo due to ongoing cases, for hundreds of other participants in RTB, contracts are treated more like business secrets and are only available to their partners. They can only be examined during investigations. Therefore, ensuring that this information is available to data subjects is crucial.

4.2.3 Challenges faced in achieving transparency in data protection law within the RTB

The RTB ecosystems, as repeatedly emphasized in this thesis, are remarkably complex. It involves a multitude of global participants, many of whom rely on contractual relationships to conduct online personalized advertising. These entities depend on their partners for accessing personal data and mutually share their own data to facilitate ad delivery.

However, when controllers are regarded as joint controllers, they often lack detailed insights into their roles in processing personal data and assisting data subjects with

---

[176] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023), para 142.
[177] ibid, paras.143-144.
[178] Art. 29 WP, *Guidelines on Transparency Under Regulation 2016/679*, WP260 rev.01 (11 April 2018) ,7, s 10 <file:///Users/nandao/Downloads/20180413_article_29_wp_transparency_guidelines_7B894B16-B8B9-B044-ED400A6DBAA4FA60_51025.pdf> accessed 28 March 2024.

their rights. Consequently, data subjects may encounter challenges in identifying the appropriate party for assistance to exercise their rights, potentially leading to disproportionate efforts or work in vain. Moreover, the dynamic nature of participants' roles within the ecosystems allows for interpretations among parties, while the reliance on partners for establishing a legal basis for processing may hinder effective regulation of partners' behavior in line with data protection laws.

Therefore, the complexity of the ecosystems presents specific challenges to transparency, making it difficult to ensure adequate adherence to regulatory requirements.

Consideration and balance of interests among various participants in RTB are important factors affecting transparency. At its core, the selection of the legal basis for processing data, whether consent or legitimate interest, hinges on prioritizing the legitimate interests of controllers or the interests of data subjects. This choice impacts the compliance measures, foundational frameworks, and business models of processors, all of which greatly influence transparency.

For instance, in the case of Criteo,[179] if data controllers and processors only cease advertising options for data subjects who choose to opt-out or exercise their right to be forgotten, rather than terminating all usage of their data, it could potentially harm controllers' ability to effectively utilize the data they have acquired, thus impacting their competitive edge built on data-driven assets.

Additionally, considerations of privacy compliance and interests for both small and large platform companies play a crucial role in the overall transparency of the ecosystems. Presently, data protection law cases primarily focus on major platform companies such as Google, Meta, Criteo, etc., but thousands of small companies also serve as significant participants in data leakage and illegal use of personal data.

However, imposing additional inappropriate compliance requirements may hinder the growth of small platform companies, consequently restricting market competition. Therefore, determining the allocation of rights and responsibilities based on the platform’s interests, between small and large platform companies will

[179] CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* (SAN-2023-009 2023).

also influence the transparency of the entire ecosystem. For example, in the AdTech industry, the GDPR enhances transparency and data protection, yet it also adversely affects competition by bolstering the position of large online platforms like Google and Facebook in certain markets.[180] This grant large platforms means to undermine competitors by limiting access to necessary data for effective competition.

Moreover, research shows that greater transparency about some of the ways online ads are personalized for individuals appears to diminish data subjects' support for this practice.[181] Data subjects' opinions will also influence the economic model in online advertising. Hence, balancing participants' interests in the RTB ecosystems is a crucial factor in discussions about transparency.

Transparency threshold and its impact on efficiency also need to be considered. Transparency obligations play a crucial role in reducing information asymmetry in RTB. However, it is notable to recognize that increasing transparency and imposing data subject control is not always universally positive. Several factors come into play, including the type of personal data involved and the emotional context of data subjects.[182]

In the context of RTB, challenges arise due to the multitude of participants and the complexity and lengthy privacy policies. Data subjects often allocate limited attention to reading these policies and cannot understand how their data are used, so we could not assume that they can make meaningful privacy decisions.[183] When policymakers deal with decisions concerning online privacy issues, it remains challenging to ascertain the most relevant interpretation: whether users consistently act rationally, if their rationality is impeded, or if they are simply unable to make informed and rationale choices.

These considerations are important in determining the extent to which data protection laws can intervene on behalf of users, ensuring a balanced level of control

---

[180] Damien Geradin and others, 'GDPR Myopia: How a Well-Intended Regulation Ended up Favoring Google in Ad Tech' (2020) 17(1) ECJ 47, 47, <https://ssrn.com/abstract=3598130> accessed 13 February 2024.
[181] Darren M. Stevenson, 'Data, Trust, and Transparency in Personalized Advertising' (DPhil thesis, University of Michgan 2016), 223, para 3.
[182] Bo Zhang and others, 'Privacy Concerns in Online Recommender Systems: Influences of Control and User Data Input' (In Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, USA, 2014) 159, 159.
[183] Sophie C. Boerman and others, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) J. Advert 363, 374, <https://doi.org/10.1080/00913367.2017.1339368> accessed 13 February 2024.

and establishing post-transparency obligations and guidelines for platforms rather than giving full sovereignty to data subjects who are not really fully rational, knowledgeable, and informed.

Complex algorithms, AI models, machine learning, and other technologies play an important role in RTB, AI is especially seen as the key driver of growth of programmatic growth,[184] which may influence the future strategy of digital ads.

However, these technologies often operate opaquely, and lack of explainability, making their decision-making processes difficult for users to understand. Basically, the concept of explainability in AI models involves presenting information in a way that humans can reasonably understand. However, the absence of a precise definition means that the manner of presentation can vary depending on factors such as the user's expertise, preferences, and other contextual variables.[185]

AI models deployed in RTB can efficiently detect and integrate complex non-linear patterns in data, analyzing various factors like user demographics, browsing history, and device type to predict user behavior. While enhancing targeting and prediction accuracy, this complexity poses challenges in transparency and explainability, and readability is usually negatively relevant to performance.[186]

It becomes challenging to explain how certain things you put into the model affect its predictions, leaving users confused about ad targeting practices and personalized experiences online. The intricate interactions among variables further complicate the interpretation and validation of the model's decisions by advertisers and platform operators, hindering effective communication with users.

4.2.4 Evaluating the effectiveness of the EU data protection framework

We explore the transparency within the EU data protection framework, where the GDPR serves as the fundamental and representative regulation, which initiates the data governance in the EU. The GDPR is further clarified through case law and

[184] IAB Europe, 'Attitudes to Programmatic Advertising Report' (November 2023), 4 <https://iabeurope.eu/wp-content/uploads/IAB-Europe-Attitudes-to-Programmatic-Advertising-Report-2023-FINAL.pdf> accessed 27 February 2024.
[185] Filip Karlo Došilović and others, 'Explainable artificial intelligence: A survey' (41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018) 0210, 0211 <DOI: 10.23919/MIPRO.2018.8400040> accessed 5 March 2024.
[186] ibid 0211, figure 1.

integrated into companies' compliance work. Additionally, the DSA introduces transparency requirements for online platforms to enhance user trust and mitigate risks associated with digital services, while the AI Act aims to regulate AI models by enhancing explainability and transparency.

Together, they form part of the EU's data governance strategy and expand upon it by emphasizing different aspects of it. Transparency is a fundamental value and principle in each of these regulations. By prioritizing transparency, their goal is to promote responsible AI, foster trust in online platforms, and enhance data protection throughout the EU.

However, when considering the implementation of transparency in RTB, we encounter challenges due to the intricate nature of the ecosystems. Participants in this ecosystem depend on each other contractually to collect personal data and ensure compliance with data protection laws, which complicates transparency efforts. Deceptive practices and circumvention of compliance measures hinder data subjects' ability to exercise their rights effectively without further intervention.

The GDPR establishes a fundamental transparency requirement for controllers and processors, driving compliance efforts in practice. However, despite the GDPR and EDPB aiming to harmonize data protection laws within the EU, interpretation and implementation largely fall under national data protection authorities. This decentralized approach may lead to inconsistencies in interpretation, especially given the borderless nature of the online environment within the EU.

Additionally, the GDPR does not adequately address the specific transparency challenges posed by RTB, making it difficult for data subjects to exercise their rights effectively when transparency is guaranteed mainly through contractual relationships layer by layer in RTB without additional intervention.

In conjunction with the GDPR, the DSA strives to establish transparency and accountability in the digital field, making transparency a core principle, that supplements the GDPR in regulating digital ads. Requirements for online platforms to maintain databases are instrumental in enhancing transparency, particularly in data removal processes.

However, in recommending systems, there remains uncertainty about how platforms will engage users and allow them to influence recommendations. Additionally, in RTB practices with multiple participants, clarifying responsibilities and ensuring transparency in parameter allocation from data collection to ad output pose challenges, which still need further clarification in legal practices.

While not directly targeting RTB or data protection issues, the AI Act aims to ensure transparency in High-risk AI systems, including that could potentially utilized in ad targeting and prediction. The transparency guarantee within the AI Act seeks to empower deployers to comprehend the system's operations and outputs, ensuring their correct usage. [187] Concerning the obligation of transparency to users, interactions with AI systems shall be disclosed, particularly when individuals encounter 'emotion recognition systems or biometric categorization systems.' [188]This obligation primarily ensures that users are informed about interactions or exposures rather than providing transparency for a reasonable understanding of AI systems.

The AI Act, adopted by the European Parliament in March 2024, excluded clauses from previous amendments that guaranteed users a reasonable understanding of AI systems, such as understanding their operations, functionality, and data processing, which is in the previous amendment.[189] This actually diminishes the AI Act's influence on enhancing transparency in the field of data protection.

In addition, the requirement for transparency to deployers only applies to high-risk AI systems, leaving out other AI models used in online advertising. Additionally, ensuring transparency relies on understanding AI models after they have made their decisions. This means we extract information from the AI models, but we do not fully rely on understanding how the AI model actually works. Relying too much on this can lead to interpretations that seem convincing but are actually misleading, similar to

[187] AI Act, art.13.
[188] AI Act, art.50.
[189] Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA (2023)0236, (2023), Amendment 300 <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.docx> accessed 5 March 2024.

the mechanism that humans might try to justify and defend our decisions afterward.[190]

In summary, although the regulatory framework seems comprehensive, it still fails to adequately address some challenges in the area of RTB and lacks effective implementation in practice. Addressing challenges specified in RTB ecosystems, empowering users to influence recommendation systems, and ensuring user understanding of AI processes, without rationalizing AI outcomes afterward, requires further clarification.

Without clarification of key issues and stringent enforcement measures, the asymmetry within RTB could intensify, making it increasingly challenging to ensure transparency amidst rapidly advancing technologies.

[190] Filip Karlo Došilović and others, 'Explainable Artificial Intelligence: A Survey' (41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018), 0210, 0211 <DOI: 10.23919/MIPRO.2018.8400040> accessed 5 March 2024.

5 Enhancing the effectiveness of EU Law: opportunities

From the previous chapter, we analyzed the role of key stakeholders in RTB and the inadequacy of EU data protection law in addressing legal basis and transparency requirements. In this section, we will explore potential opportunities for enhancing the effectiveness of the EU data protection law.

When implementing the data protection framework, it is essential to clarify the value orientation. The digital advertising field involves numerous unbalanced participants, which may intersect with competition law, consumer protection law, contract law and others. Without clarifying the value orientation, data protection measures will not contribute to business growth nor effectively safeguard data subjects.

Drawing from CJEU case law, we observe a trend toward prioritizing the protection of data subjects, exemplified by the broad interpretation of 'personal data' and 'controller' within the GDPR. However, this alone is insufficient; it is crucial to strike a balance among the interests of various stakeholders as the GDPR intersects with the DSA and AI Act in the future.

In addition, more detailed data protection guidelines for the RTB scenario at the EU level, under the leadership of the EDPB are necessary. This involves clarifying the roles, responsibilities, and compliance practices of the main stakeholders in RTB, as well as providing relevant guidelines and references for privacy design.

Industry organizations and other non-governmental data protection organizations play a pivotal role in influencing online personalized advertising practices, an aspect that deserves greater attention in legal practices. In recent times, the development of data protection laws, particularly driven by legal cases raised by some organizations for example NGO NOYB, these litigations contribute to a detailed interpretation of the GDPR and empower data subjects.[191]

However, they also have drawbacks, such as litigation may lead to settlements or huge time-consuming. As previously mentioned, regulations often lack the ability to

[191] NOYB has dealt with complaints involving numerous online companies, such as Google Ireland Limited, Meta Ireland Limited, Instagram, WhatsApp Ireland Limited, Criteo, Netflix, Spotify, Amazon, and more, encompassing a broad spectrum of online activities. Their initiatives span various projects, including addressing issues related to cookie banners, profiling, automated decision-making, online and mobile tracking, data subjects' rights, forced consent, consent bypass, and others. Many of these cases play a crucial role in clarifying interpretations and upholding data protection standards. See <https://noyb.eu/en> accessed 21 February 2024.

balance interests among different participants in RTB. Therefore, industry organizations could emerge as a significant trend in addressing data protection while still maintaining business and technological efficiency.

Specifically, collaboration between authorities and industry organizations is crucial. This collaboration can reduce the gap between regulations and legal practices through important cooperation and due diligence before legal actions. This maximizes the efficiency of data protection mechanisms and helps prevent situations like the invalidation of the widely used TCF in RTB by authorities.

Moreover, enhancing the efficiency of tools offered by industry organizations is essential. For instance, while many platforms mention that 'Your Online Choices,' operated by the EDAA, could be a useful tool for managing consent and preferences, its usability and smoothness are often lacking. Expecting data subjects to spend significant time managing consent through such tools is unreasonable. Therefore, user-friendly tools that integrate all consent and preferences are valuable, which not only improve efficiency but also enhance transparency in data collection and utilization.

The data processing on the web is usually technology-intensive,[192] so using technologies in detecting data protection violations and increasing data protection could be valuable. For example, privacy measurement tool has the potential to play a role in keeping online privacy incursions and power imbalances in check, so they must be made available broadly rather than within the research community. [193]

With the exploration of AI models and other technologies, the violation of data protection is becoming more invisible, this is also applied in RTB, when data is shared with hundreds of DSPs, the data utilization is not clear for other participants in the ecosystems no wonder data subjects, so the available technological tool can be useful, which need cooperation from multiple stakeholders and the present in a user-friendly way. For example, the NGO NOYB uses automated website cans to enforce

[192] Cristiana Santos and others, 'Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners' (2020) TechReg 91, 92, <https://doi.org/10.26116/techreg.2020.009> accessed 8 February 2024.
[193] Steve Englehardt, Arvind Narayanan, 'Online Tracking: A 1-million-site Measurement and Analysis' (In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 2016) 1388, 1400 <https://doi.org/10.1145/2976749.2978313> accessed 21 February 2024.

the compliance of cookie banners with the GDPR, which is a great example of showing the benefits of technological tools.

6 Conclusion

In summary, this thesis has investigated the efficacy of EU data protection law in overseeing personalized advertising within the RTB ecosystems. It has become evident that current regulatory measures are insufficient for several reasons.

Firstly, upon analyzing the intricate dynamics and legal practices within the ecosystems, it is apparent that roles and obligations among its various participants remain unclear, leading to ineffective compliance practices.

Secondly, guaranteeing valid consent for personalized ads in RTB under the GDPR is challenging due to the complex nature of the ecosystems. Participants often rely on their partners' contractual obligations to ensure consent, but there is a lack of robust measures to ensure it. Additionally, it can be difficult for data subjects to exercise their withdrawal right, as seen in instances such as the Belgian DPA invalidating the TC String and CNIL's decision on Criteo. While legitimate interests may provide some safeguards, they cannot override data subjects' fundamental rights.

Moreover, meeting transparency requirements within the data protection framework proves impractical due to complex contractual relationships layer by layer and real-time data sharing while data subjects lack sufficient knowledge and powerful tools to assert their personal choices and control over their data.

The existing regulatory framework inadequately tackles the intricate challenges posed by personalized advertising within the RTB ecosystems, resulting in a gap between regulations and practical implementation. On one hand, fostering collaboration between regulatory authorities and industry organizations, along with enhancing available tools, can help alleviate gaps between regulations and actual practices, thereby enhancing efficiency and transparency in this domain. On the other hand, embracing technology-driven solutions to detect and address data protection violations is crucial for safeguarding individuals' privacy and data security.

From a legal standpoint, future research could explore strategies to address inefficiencies in consent mechanisms for personalized ads via RTB, specifically, efforts should aim to narrow the legal gap between regulations and actual compliance practices. Additionally, studying the evolving trends in the online advertising

ecosystems after Belgian DPA's decision on RTB and revealed non-compliance work in the ecosystems, remains an important area of inquiry.

Bibliography

Books and Articles

- Scaife L, *Handbook of Social Media and the Law* (1st edn, Informa Law from Routledge 2015).
- McConville M, Chui W. H. (eds), *Research Methods for Law* (2nd edn, Edinburgh University Press 2017).
- Webley L, 'Stumbling Blocks in Empirical Legal Research: Case Study Research' (2016) Law and Method.
- Quach S and others, 'Digital Technologies: Tensions in Privacy and Data' (2022) 50 J. of the Acad. Mark. Sci 1299 <https://doi.org/10.1007/s11747-022-00845-y> accessed 17 January 2014.
- Febria L L, and Setiyanto A, 'Privacy Concerns in Personalized Advertising Effectiveness on Social Media' (2021) 5(2) SIJDEB 147 <DOI: 10.29259/sijdeb.v5i2.147-156> accessed 17 January 2024.
- Zhang B and others, 'Privacy Concerns in Online Recommender Systems: Influences of Control and User Data Input' (In Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, USA, 2014) 159.
- Veale M and others 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?' (2022) TechReg 12 <https://ssrn.com/abstract=4206059>accessed 17 January 2024.
- Matte C and others 'Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?' (In proceedings of Privacy Technologies and Policy: 8th Annual Privacy Forum, Lisbon, October 2020) <https://doi.org/10.1007/978-3-030-55196-4_10> accessed 17 January 2024.
- Li C Q, 'Analysis of the Advertising Technology Industry's Compliance with the General Data Protection Regulation: a Case Study of the CNIL Investigation of the French Advertising Technology Giant Criteo' (Master's thesis, Technische

Universität Dresden 2022) <http://dx.doi.org/10.2139/ssrn.4307210> accessed 17 January 2024.

- Kollnig K, 'Priorities for More Effective Tech Regulation' (2023) ArXiv Computers and Society <https://doi.org/10.48550/arXiv.2302.13950> accessed 17 January 2024.

- Lin K and others, 'Investigating Deceptive Design in GDPR's Legitimate Interest' (In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, 2023) <https://doi.org/10.1145/3544548.3580637> accessed 17 January 2024.

- Davoli G, 'Is Winter Coming for Online Behavioural Advertising? The Future of Targeted Advertising in the EU' (Master's thesis, Tilburg University 2023) .

- Ryan J and Santos C, 'An Unending Data Breach Immune to Audit? Can the TCF and RTB Be Reconciled with the GDPR?' (2022) Irish Council for Civil Liberties Research Paper <https://ssrn.com/abstract=4064729> accessed 22 January 2024.

- Bholasing J, 'How Technological Advances in the Big Data Era Make It Impossible to Define the 'Personal' in GDPR's 'Personal Data' ' (2022) 8(3) EDPL 346< https://doi.org/10.21552/edpl/2022/3/5> accessed 17 January 2024.

- Wrigley S and others, 'My Name Is Personalised_ Political_Advertiser.py and I Approve This Message: Regulating Automated and Targeted Political Advertising in EU Law' (2023) 13 University of Luxembourg Law Research Paper<http://dx.doi.org/10.2139/ssrn.4561013>accessed 17 January 2024.

- Wang C and others, 'Toward Privacy-Preserving Personalized Recommendation Services' (2018) 4(1) Engineering 21<https://doi.org/10.1016/j.eng.2018.02.005> accessed 17 January 2024.

- Cooper D and others, 'Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising' (2021) JCM 8 <http://dx.doi.org/10.2139/ssrn.4012936> accessed 18 March 2024.

- Maršál J, ‘Legal Aspects of Online Behavioural Advertising’ (Master’ thesis, Univerzita Karlova 2022).

- Veale M, Borgesius F Z, ‘Adtech and Real-time Bidding under European Data Protection law’ (2022) 23 GLJ 226 <DOI:10.1017/glj.2022.18> accessed 3 March 2024.

- Sung K and others, ‘Re-Identification of Mobile Devices Using Real-time Bidding Advertising Networks’ (In Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, Association for Computing Machinery, New York, Article 48, 2020) <https://doi.org/10.1145/3372224.3419205> accessed 17 January 2024.

- Ouaftouh S and others, ‘A User Dimension-Based Classification’ (10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, Morocco,2015) <DOI: 10.1109/SITA.2015.7358378> accessed 18 January 2024.

- Avdagić-Golub E and others, ‘Profiling Contact Center Customers for Optimization of Call Routing Using Data Mining Techniques’ (20th International Symposium INFOTEH-JAHORINA, 2021) <DOI: 10.1109/INFOTEH51037.2021.9400671> accessed 18 January 2024.

- Santos C and others, ‘Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners’ (2020) TechReg 91 <https://doi.org/10.26116/techreg.2020.009> accessed 8 February 2024.

  —— and others, ‘Consent Management Platforms under the GDPR: Processors and/or Controllers?’ (APF 2021 - 9th Annual Privacy Forum, Jun 2021, Oslo, Norway) <https://doi.org/10.48550/arXiv.2104.06861> accessed 20 February 2024.

  ——and Pandit H J, ‘How Could the Upcoming ePrivacy Regulation Recognise Enforceable Privacy Signals in the EU?’ (2023) OSF Preprints <https://doi.org/10.31219/osf.io/xvyf3> accessed 11 February 2024.

- Eke C I and others, 'A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions' (2019) 7 in IEEE Access 144907 <DOI: 10.1109/ACCESS.2019.2944243> accessed 18 January 2024.
- Benedikt K, 'Belgian Data Protection Authority Ruling - Online Advertising on the Brink of Extinction?' (2022) 8(1) EDPL 85 <https://doi.org/10.21552/edpl/2022/1/13> accessed 29 January.
- Jiménez J A E, 'Privacy in Online Advertising Platforms' (DPhil thesis, Universitat Politècnica de Catalunya 2020) <https://upcommons.upc.edu/bitstream/handle/2117/330390/TJAEJ1de1.pdf> accessed 22 January 2024.
- Meskenaite G, 'An Examination of the Criteria for Valid Consent Under the GDPR in the Light of the Rationale and Technological Neutrality' (Master's thesis, Lund University 2022Technische) accessed 8 February 2024.
- Steindl E, 'Practitioners' Corner ·Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in light of the Draft AI Act and its Interplay with the GDPR' (2022) 8(2) EDPL <DOI https://doi.org/10.21552/edpl/2022/2/20> accessed 28 March 2024.
- Geradin D and others, 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech' (2020) 17(1) ECJ 47 <https://ssrn.com/abstract=3598130> accessed 13 February 2024.
- Stevenson D M, 'Data, Trust, and Transparency in Personalized Advertising', (DPhil thesis, University of Michgan 2016).
- Boerman S C and others, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) J. Advert 363 <https://doi.org/10.1080/00913367.2017.1339368> accessed 13 February 2024.
- Englehardt S, Narayanan A, 'Online Tracking: A 1-million-site Measurement and Analysis' (In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing

Machinery, New York, USA, 2016) <https://doi.org/10.1145/2976749.2978313> accessed 21 February 2024.

- Došilović F K and others, 'Explainable artificial intelligence: A survey' (41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018) 0210<DOI: 10.23919/MIPRO.2018.8400040> accessed 5 March 2024.

Legislation, Guidelines

- European Union, Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art.8.

- 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/ (General Data Protection Regulation) [2016] OJ L 119/1.

- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

- European Parliament legislative resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2024] P9_TA (2024)0138.

- Art. 29 WP, *Opinion 15/2011 on the Definition of Consent*, WP 187 (13 July 2011).

- Art. 29 WP, *Opinion 03/2013 on Purpose Limitation*, WP 203 (2 April 2013).

- Art. 29 WP, *Guidelines on Transparency Under Regulation 2016/679*, WP260 rev.01 (11 April 2018).

- EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679* (Version 1.1, 4 May 2020).

- EDPB, *Statement 03/2021 on the ePrivacy Regulation* (9 March 2021).

The EU Cases & National DPAs' Decisions

- Case C131/12 *Google Spain SL v Agencia Española de protección de Datos (AEPD) and Others* [2014] ECLI: EU:C:2014:317.
- Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* [2017] ECLI:EU:C:2017:336.
- Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat - uskonnollinen yhdyskunta* [2018] ECLI:EU:C:2018:551.
- Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629.
- Case C-507/17 *Google LLC, successor in law to Google Inc., v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772.
- Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214.
- Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022* [2022] DOS-2019-01377.
- CNIL, *Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO* [2023] SAN-2023-009.
- Datenschutzkonferenz, *Resolution of the Conference of Independent Federal and State Data Protection Supervisory Authorities on Bahavioural Advertising* (4 June 2019) <https://www.datenschutzkonferenz-online.de/media/dskb/20190110_beschluss_verhaltensbasierte_werbung_alt.pdf> accessed 5 March 2024.

Other sources

- ICO, 'Update Report into AdTech and Real Time Bidding' (2019).

- ICO, ‘Data Protection and Privacy Expectations for Online Advertising Proposals’ (2021).

- GfK, ‘European Online, An Experience Driven by Advertising’ (6 September 2017) <https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf> accessed 27 February 2024.

- European Data Protection Supervisory, ‘Transparency’ <https://www.edps.europa.eu/data-protection/our-work/subjects/transparency_en> accessed 12 February 2024.

- Office of the Data Protection Ombudsman of Finland, ‘Controller's legitimate interests’ <https://tietosuoja.fi/en/controller-s-legitimate-interests> accessed 11 February 2024.

- European commission, ‘DSA Transparency Database FAQ” <https://transparency.dsa.ec.europa.eu/page/faq> accessed 12 February 2024.

- German SAs, ‘Cross-state Audit: Consent on Media Companies’ Websites is Mostly Ineffective - Improvements are Needed’ (EDPB News, 30 June 2021) <https://edpb.europa.eu/news/national-news/2021/german-sas-cross-state-audit-consent-media-companies-websites-mostly_en> accessed 4 October 2023.

- ICCL, ‘ICCL Lawsuit Takes Aim at Google, Facebook, Amazon, Twitter and the Entire Online Advertising Industry’ (15 June 2021), < https://www.iccl.ie/news/press-announcement-rtb-lawsuit/> accessed 8 February 2024.

- Italian SA, ‘TikTok: Italian SA Warns Against 'Personalized' Ads Based on Legitimate Interest’ (EDPB News, 15 July 2022) <https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads-based-legitimate-interest_en> accessed 6 October 2023.

- Gegevensbeschermingsautoriteit, 'The Belgium DPA to Restore Order to the Online Advertising Industry: IAB Europe Held Responsible for a Mechanism That Infringes the GDPR' (2 February 2022) <https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr> accessed 20 March 2024.

- IAB Europe, 'The Transparency & Consent Framework (TCF) v2.2' (16 May 2023) <https://iabeurope.eu/transparency-consent-framework/> accessed 4 February 2024.

- IAB Europe, 'IAB Europe Transparency &Consent Framework Policies ' (Version 2023-05-15.4.0.a) <https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/> accessed 20 February 2024.

- IAB Europe, 'About Us', <https://iabeurope.eu/about-us/> accessed 4 February 2024.

- IAB Europe, 'Transparency & Consent Framework' <https://iabeurope.eu/transparency-consent-framework/> accessed 4 February 2024.

- IAB Europe, 'What Would an Internet Without Targeted Ads Look Like' (April 2021) <https://iabeurope.eu/wp-content/uploads/2021/04/IAB-Europe_What-Would-an-Internet-Without-Targeted-Ads-Look-Like_April-2021.pdf> accessed 27 February 2024.

- IAB Europe, 'Attitudes to Programmatic Advertising Report' (November 2023), 5, Figure 3 <https://iabeurope.eu/wp-content/uploads/IAB-Europe-Attitudes-to-Programmatic-Advertising-Report-2023-FINAL.pdf> accessed 27 February 2024.

- IAB Europe, 'TCF Compliance Programmes', <https://iabeurope.eu/tcf-compliance-programmes/> accessed 3 March 2024.

- IAB Tech Lab, 'IAB Tech Lab Launches Accountability Platform to Deliver Greater Transparency in the Use of Personal Data for Addressability'

<https://iabtechlab.com/wp-content/uploads/2023/12/Accountability-Platform_Public-Comment_20231214.pdf> accessed 3 March 2024.

- Criteo, 'Terms and Conditions for Advertisers-Retail Media' <https://www.criteo.com/wp-content/uploads/2021/04/Retail-Media-Terms-for-Advertisers_April-2021.pdf> accessed 4 February 2024.
- Criteo, 'Retargeting' <https://www.criteo.com/digital-advertising-glossary/retargeting/> accessed 4 February 2024.
- Criteo, 'Privacy Policy' <https://www.criteo.com/privacy/> accessed 4 February 2024.
- Criteo, 'Criteo Data Protection Agreement' < https://www.criteo.com/wp-content/uploads/2023/04/Criteo-Data-Protection-Agreement-April23_without-Appendix-2.pdf> accessed 4 February 2024.
- Digital Advertising Alliance, 'About the Participating Associations", <https://digitaladvertisingalliance.org/about> accessed 4 February 2024.
- EDAA, 'About Us', <https://edaa.eu/> accessed 4 February 2024.
- EDAA, 'Your Online Choices, A Guide to Online Behavioural Advertising' < https://youronlinechoices.eu/> accessed 10 February 2024.
- CNIL, 'Personalised Advertising: CRITEO Fined EUR 40 Million' (22 June 2022) <https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million> accessed 10 February 2024.
- European Commission, 'Questions and Answers: Digital Services Act, What is the Digital Services Act?' (Questions and answers, 25 April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348> accessed 4 October 2023.
- Access Now, NOYB and EDRI, Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2021).

- NOYB, <https://noyb.eu/en> accessed 21 February 2024.
- Lomas N, ‘How a Small French Privacy Ruling Could Remark Adtech for Good’ (Techcrunch, 20 November 2018) <https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/> accessed 8 February 2024.
- Der Spiegel < https://www.spiegel.de/> accessed 4 February 2024.
- Quantcast, ‘Gain Double-digital Performance Advertising Outcomes’ < https://www.quantcast.com/home/> accessed 5 March 2024.
- OpenX, ‘OpenX Ad Exchange Privacy Policy’ (19 December 2023) <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/#section-1> accessed 21 March 2024.
- The Trade Desk, ‘Privacy and the Trade Desk Platform’ (26 January 2024) <https://www.thetradedesk.com/us/privacy> accessed 21 March 2024.
- Chat GPT 3.5 <https://chat.openai.com/>
- Copilot <https://copilot.microsoft.com/>