verbraucherzentrale

PERSPECTIVES FOR THE REGULATION OF PERSONALISED ADVERTISING

Position paper

10 February 2025

Imprint

Federation of German Consumer Organisations – Verbraucherzentrale Bundesverband e.V. (vzbv)

Team Digital and Media
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin, Germany

The Federation of German Consumer Organisations is registered in the German Lobby Register and the European Transparency Register. You can access the relevant entries here and here.

CONTENT

RELEVANCE TO CONSUMERS

Every day, consumers are faced with the decision of how their browsing habits and interests are collected, aggregated from diverse sources and utilised to create personalised marketing campaigns. Privacy policies often contain technical jargon and consent mechanisms are frequently complex and misleading, nudging consumers towards agreeing to their data being collected without a clear understanding of the consequences: companies categorise users into segments reaching from “Marlboro” and “weight loss” to “casino and gambling activities”, “speculative investments”, “fragile seniors” or “mums that shop like crazy” to influence them based on their preferences and vulnerabilities. Other companies track literally every step consumers take. The potential for abuse is immense, ranging from manipulation and discrimination to material as well as physical and psychological harm. Beyond individual harms, the structural risks for society associated with personalised advertising are deeply troubling. For example, the exploitation of personal data exacerbates societal polarisation and fragmentation by isolating groups with targeted content.

In view of these problems, consumers feel trapped between powerlessness and fatalism. These violations of consumer rights, coupled with far-reaching societal consequences, demand immediate attention to ensure accountability and prevent further harm.

SUMMARY

- The digital advertising ecosystem has evolved into a complex and opaque network involving thousands of actors that incentivises unchecked data collection and aggregation. Through tracking and profiling, consumers are targeted based on their personal preferences and individual vulnerabilities, leading to substantial informational and power asymmetries. This jeopardises privacy, facilitates manipulation and fosters discrimination, while consumers feel trapped between powerlessness and fatalism. Without effective regulatory intervention, the misuse of personal data will continue to escalate, undermining privacy, democracy and trust. Proper regulation must limit invasive practices, enforce transparency and ensure accountability to safeguard individual rights and protect societal values in the digital era.
- The consent model has conceptual and practical limitations. In particular, the complexity and business practices of the online advertising market make it virtually impossible for consumers to understand how their data is collected and used. Deceptive designs encourage agreement, the overwhelming number of consent requests exacerbates consumer fatigue. These limitations demonstrate the urgent need for stricter measures (as proposed below) to reduce risks within the advertising ecosystem. Only after these risks have been mitigated by the legislator can the relevant stakeholders redesign transparency mechanisms and consent processes to empower users and rebuild trust in data processing. Prioritising risk reduction is essential to ensure meaningful and sustainable consumer protection.
- The sector's purported attempts to increase transparency within the ecosystem and to implement adequate measures against unauthorised data processing have proven to be ineffective. The increasing use of Artificial Intelligence (AI) further exacerbates transparency issues and deepens power asymmetries, highlighting the urgent need for comprehensive regulatory intervention to address these systemic issues.
- Existing laws like the General Data Protection Regulation (GDPR), the ePrivacy Directive and related laws struggle to adequately address the systemic risks posed by personalised advertising. The GDPR's flexibility and broad definitions have inadvertently fostered implementation challenges as well as enforcement gaps. Sector-specific rule books like the Digital Service Act (DSA), the Regulation on the Transparency and Targeting of Political Advertising (TTPA) or the Artificial Intelligence Act (AIA) offer valuable measures but fall short of establishing comprehensive protections, as their scope is often limited to specific actors or contexts rather than addressing the ecosystem as a whole.

Therefore, the European Union (EU) should introduce a new horizontal legal framework to address the risks posed by profiling and tracking for advertising purposes to individuals and society. Such a framework should establish clear limits on data processing, mandate proper transparency measures and strengthen enforcement mechanisms. The exploitation of digital asymmetries and vulnerabilities mandates protections that extend beyond the limited tool of individual consent. This is the only way societal interests and fundamental rights can be upheld in the digital age. More concretely, tracking and profiling for advertising purposes should be prohibited.

In vzbv's view, this new legal framework should at least include the simultaneous implementation of the following substantive procedural, technical and organisational measures across multiple levels, ensuring these efforts are both aligned and complementary:

- Certain particularly invasive practices must be prohibited. This includes a clear ban on cross-site tracking and on the merging of collected data with external datasets. Additionally, new legislation should restrict companies from deriving further attributes from collected data to mitigate threats to privacy and individuals' autonomy. These measures would significantly impact all stages and actors within the advertising ecosystem, representing a decisive step towards comprehensive regulation.
- Beyond banning specific purposes and processing methods, the processing of sensitive data categories and the targeting of vulnerable consumer groups should be restricted. However, precise definitions tailored to the online advertising sector are crucial. For instance, a new regulation should expand the definition of sensitive data as laid down in the GDPR to include geolocation data. Additionally, new rules should take a new approach to vulnerability and incorporate situational vulnerabilities.
- To complement the ban on certain purposes and processing methods, a European registry for the advertising industry should be established. All entities processing personal data for personalised advertising should be required to register, providing inter alia details on their identity and processing purposes while unregistered entities should be barred from participation in the ecosystem. This registry would help identify and address structural risks to individuals and society. Additionally, mandatory certification should verify whether actors disclose their practices and comply with legal requirements.

I. INTRODUCTION

Digital advertising has been the dominant business model on the internet for many years. The online advertising industry promotes personalised advertising as essential to offer digital services “for free.” Over time, the market has evolved from a simple two-party system – advertisers and publishers – into a highly complex network of hundreds of actors. This shift has created a convoluted and opaque system that even the parties involved no longer fully understand (see Chapter II.1).

The report “Regulation of Online Advertising”[1] commissioned by the Federation of German Consumer Organisation (vzbv) demonstrates that personalised advertising intrudes deeply into the lives and rights of consumers. In vzbv’s view, this leads to severe individual risks for consumers and structural risks for society (see Chapter II.2). These intrusions into consumer rights and lives, combined with negative societal impacts, cannot be justified.

Existing laws fall short of effectively protecting consumers from these harms (see Chapter III). European regulations either address personalised advertising in overly abstract terms, focusing on narrow aspects of the issue or are outdated. They often rely on inadequate regulatory approaches, such as a strong focus on consent from the user, on the protection of sensitive data only or on safeguarding minors instead of all users. Additionally, legal uncertainties as well as the opacity and complexity of the online advertising market – combined with insufficient knowledge, capability and willingness among economic actors – create major implementation and enforcement gaps. As a consequence companies leverage these uncertainties and enforcement deficits to their benefit, undermining data protection standards and rules.

The ePrivacy-Regulation proposed by the European Commission in 2017 was intended to solve some of these issues. But even after eight years, the European legislator has been unable to agree on a common position. Many of the proposals from that time are however outdated. The need to adequately protect consumers from the aforementioned harms remains unchanged though and the deployment of technologies such as Artificial Intelligence (AI) makes addressing the risks more urgent than ever.

Therefore, a new comprehensive regulatory framework is urgently needed (see Chapter IV).

[1] Grafenstein, Max von; Herbort, Nina: Regulation of Online Advertising. Expert report commissioned by vzbv, 2024, https://www.vzbv.de/sites/default/files/2025-02/vzbv-Gutachten_Expert-Opinion_Grafenstein_Herbort_Online-Advertising.pdf, 06.02.2025.

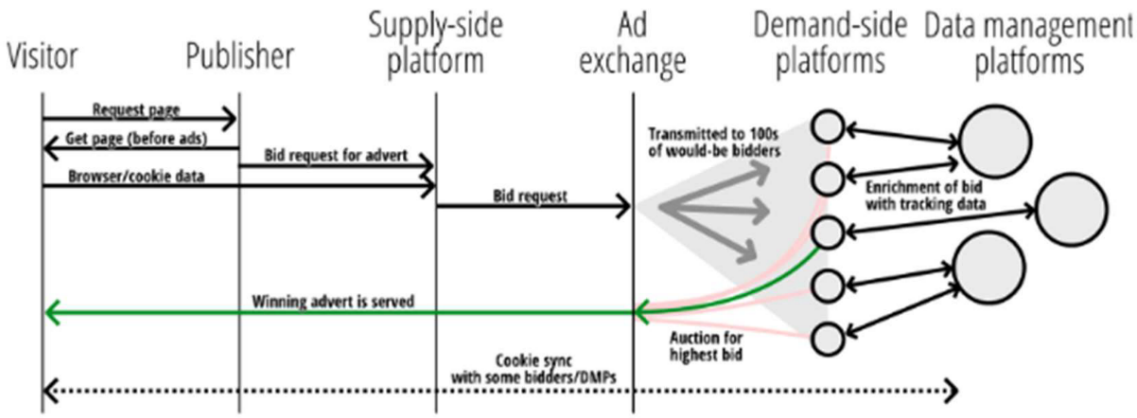
II. NEED FOR REGULATION

1. FUNCTIONING AND SCOPE OF THE ONLINE ADVERTISING MARKET

The digital advertising ecosystem has undergone a significant transformation, evolving from simple two-party relationships between advertisers and publishers into a complex process involving hundreds of actors (all these actors are called in short 'AdTech'), called **programmatic advertising and real-time bidding** ('RTB').

Programmatic advertising refers to the automated buying and selling of ad spaces tailored to the interests and behaviours of individual consumers ('personalised advertising'). When users visit a website or open an app that includes ad spaces (called 'publisher'), an automated auction process ('RTB') is triggered. Within milliseconds, hundreds of companies bid on these ad spaces through trading platforms to display ads they believe will engage the user, driven by profiling-based personalisation. Publishers collaborate with Supply-Side Platforms ('SSPs'), which market these ad spaces and connect publishers with Ad Exchanges and Demand-Side Platforms ('DSPs'). SSPs generate bid requests containing information about the user and the ad space, such as demographic data, device information, page content and geolocation data. These data points are collected through various technologies, including third-party cookies, fingerprinting, mobile advertising identifier in operating systems ('MAIDs'), login services, tracking-code in apps and server-side-tracking, which follow user behaviour across websites, devices and contexts ('web tracking'). Ad Exchanges are marketplaces, connecting SSPs with DSPs. DSPs, which act on behalf of advertisers, analyse the user data and webpage context in the bid requests to decide whether to place a bid and how much to bid. Often, they combine these data with data collected from other sources, like Data Brokers ('profiling'). Despite the many actors, the market is quite concentrated, with Google operating one of the largest Ad Exchanges as well as some of the largest SSPs and DSPs.

The following diagram[2] illustrates the main actors and processes in RTB:



[2] Veale, Michael; Zuiderveen Borgesius, Frederik: Adtech and Real-Time Bidding under European Data Protection Law, 2022, in: German Law Journal, H. 2, S. 226–256, p. 232, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/017F027B4E78EBCAE1DCBC1E12B93B9D/S2071832222000189a.pdf, 29.01.2025.

In December 2024, the United States Federal Trade Commission (FTC) took action against the Data Broker Mobilewalla, Inc.[3] The company was accused, among other allegations, of collecting and selling sensitive geolocation data without obtaining consumer consent. Particularly, the company stored consumer data collected during RTB-auctions, even when it did not win the auction. Furthermore, the collected data was neither anonymised nor adequately protected. Mobilewalla utilised this data to create profiles based on sensitive attributes such as health status or religious affiliation and sold these profiles to third parties. The FTC criticised these practices, highlighting that they exposed affected individuals to risks such as discrimination and violence.

To facilitate GDPR compliance in RTB, in 2018 the International Advertising Bureau Europe introduced the **Transparency & Consent Framework** (TCF), a standard for publishers and their partners to collect and share user consent across the advertising supply chain.[4] However, the TCF prioritises the economic interests of the industry over privacy protection, as data protection authorities and civil society were not involved in the standardisation process. This has resulted in minimal safeguards. The TCF lacks technical measures to prevent unauthorised data processing, allows data to be processed by numerous actors with limited oversight and leaves key roles, such as data controllers and processors, undefined. Consent banners further limit transparency and user autonomy by focusing on economic interests while failing to provide sufficient protections for vulnerable groups (like children) and for special categories[5] of data (like data relating to health, religion or race).

Furthermore, **AI** is increasingly revolutionising the digital advertising landscape, introducing new risks.[6] AI optimises RTB processes by automating bidding and enabling more efficient targeting. It also generates personalised advertisements in real time, enhancing engagement. However, large companies (like Google) with access to extensive datasets can leverage AI to outcompete smaller players, further consolidating their market power. This trend exacerbates transparency issues and deepens existing power asymmetries – both, between market players, as well as between AdTech companies and consumers – raising significant concerns for consumer protection.

However, it is widely debated whether personalised advertising delivers the promised improvements in efficiency and effectiveness.[7] For example, a May 2019 academic study from the United States indicates that audience tracking results in just a 4 percent

[3] Federal Trade Commission: FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data, 29.01.2025.

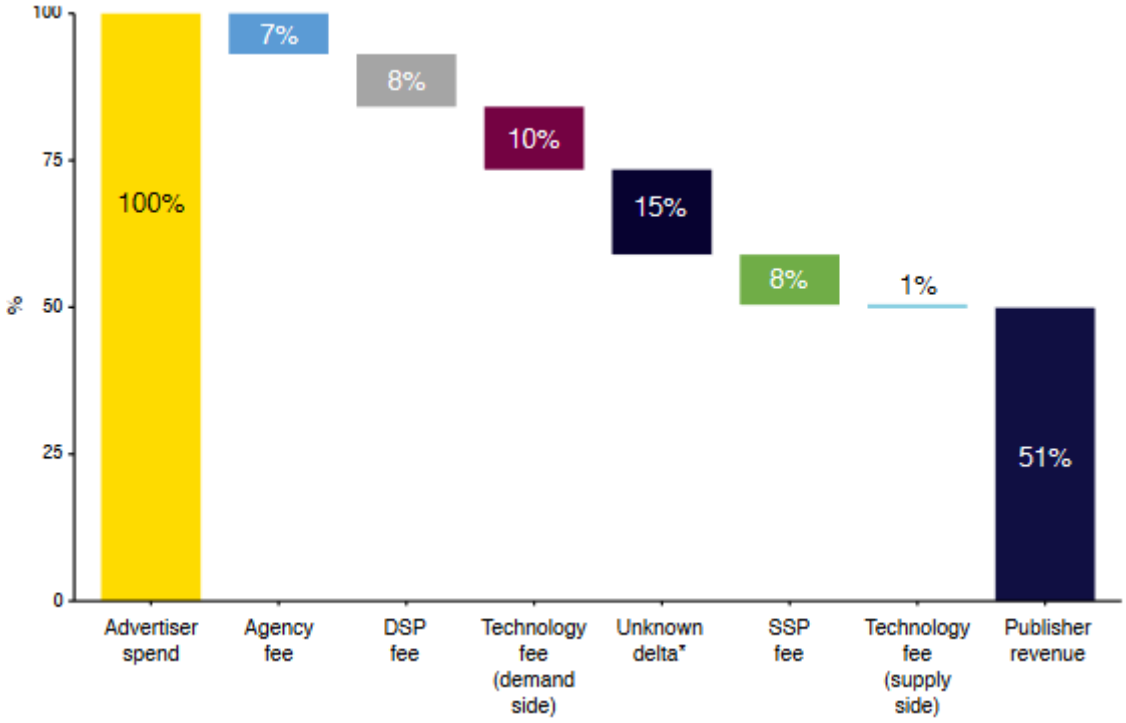
[4] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 20ff.

[5] See ebd., p. 23.

[6] See ebd., pp. 25f and p. 62.

[7] "There is limited evidence to suggest that the efficiency and efficacy gains to advertisers and publishers outweigh the societal impact of these products. There is a lack of independent analysis to assess the benefits of using personal data and profiling in advertising. The few studies that do exist fail to take into account important considerations such as the impact of fraud and buyer expectations."; Armitage, Catherine u. a.: Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. Study prepared for the European Commission, 2023, p. 96, https://data.europa.eu/doi/10.2759/294673, 29.01.2025.

increase in revenue for journalistic platforms.[8] Furthermore, a May 2020 study by PriceWaterhouseCoopers (PWC), commissioned by the British advertisers' association ISBA, found that only approximately 50 percent of advertiser spending actually reached the publishers whose websites hosted the ads. Alarmingly, the auditors were unable to trace the destination of 15 percent of advertiser spending, as the following diagram[9] shows.



The AdTech ecosystem has evolved into a complex and opaque network involving hundreds of actors. The industry's purported attempts to increase transparency within the ecosystem and to implement adequate security measures against unauthorised data processing have proven to be ineffective. The rise of AI further exacerbates transparency issues and deepens power asymmetries, highlighting the urgent need for comprehensive regulatory intervention to address these systemic issues.

2. INDIVIDUAL RISKS FOR CONSUMERS AND STRUCTURAL RISKS FOR SOCIETY

The structure of this **system incentivises all actors to collect and aggregate data**. Publishers aim to maximise their ad revenue by offering detailed user profiles, while advertisers seek precise targeting to optimise the impact of their ads. Meanwhile, interme-

[8] See Marotta, Veronica; Abhishek, Vibhanshu; Acquisti, Alessandro: Online Tracking and Publishers' Revenues: An Empirical Analysis, 2019, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf, 29.01.2025.

[9] ISBA: Programmatic supply chain transparency study, 2020, p. 8, https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf, 29.01.2025.

diaries and platforms benefit from data aggregation, which strengthens their market position and revenue streams. Therefore, data sharing is standard practice in this ecosystem, facilitated through processes like cookie synchronisation, where AdTech companies exchange user identifiers to enrich profiles. Even **offline activities** of users are tracked and incorporated into the advertising ecosystem. For instance, data is gathered when consumers use a loyalty card to purchase products in stores.[10] Additionally, apps can constantly monitor users' locations.

In July 2024, journalists from Bayerischer Rundfunk and Netzpolitik.org received a dataset containing 3.6 billion location data points from a Data Broker as a free sample.[11] The intention behind this was to persuade them to subscribe to a paid service that would provide monthly updates on the location data of millions of individuals. The dataset comprised detailed location information of mobile phones over a two-month period at the end of 2023, along with pseudonymous MAIDs of the devices. This enabled the creation of comprehensive movement profiles of the affected individuals, revealing insights into their homes, workplaces and leisure activities. Analysis of the data showed visits to sensitive locations such as addiction clinics, psychiatric facilities, brothels and prisons. Moreover, the data facilitated the identification of individuals working at external offices of the Bundesnachrichtendienst (BND; one of the German secret services) and other military or intelligence-related sites, posing a significant national security risk.

This data is often traded and integrated into user profiles. These enriched profiles can include hundreds of data points, encompassing highly sensitive information such as browsing history, age, gender, interests, device details and geolocation information.

Oracle was one of the major players in the online advertising industry (until it discontinued its advertising business in 2024). Oracle claimed to have assigned over two billion internet users to 30,000 data points, allowing it to categorise these individuals into 50,000 segments (such as "smokers" or "expectant parents"). It collaborated with numerous partners (like Facebook) to merge information from both the online and offline worlds. Oracle owned a range of other online advertising companies, including the data trading platform BlueKai, whose services were also embedded in German news websites, for example. In June 2020, a security researcher discovered a BlueKai database that was exposed to the internet without protection. This database contained billions of user records with alarming levels of detail. For instance, one supposedly pseudonymous data record identified a German man by name who, on April 19, 2020, deposited 10 Euro at a sports betting provider using a debit card. The data record included, among other details, the man's postal address, phone number and email address.[12]

[10] See International Working Group on Data Protection in Technology: Working Paper on the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market, 2021, para. 11, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20210424_WP_Risks-emerging-Tracking.pdf, 29.01.2025.

[11] Brunner, Katharina; Ciesielski, Rebecca; Zierer, Maximilian: Under Surveillance - How Location Data Jeopardizes German Security, 2024, https://interaktiv.br.de/ausspioniert-mit-standortdaten/en/index.html, 29.01.2025.

[12] Whittaker, Zack: Oracle's BlueKai tracks you across the web. That data spilled online, 2020, https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/, 29.01.2025.

A core issue lies in the **sheer scale, complexity and opacity of the online advertising market**. As early as June 2019, the British Information Commissioner's Office criticised the inability of affected individuals, regulatory authorities or even the companies involved to fully comprehend and control the flow of data.[13] This lack of transparency **undermines user privacy**, as "in a complex system such as the current advertising ecosystem, users can neither foresee nor effectively control which of their online behaviours are specifically monitored, with whom this information is shared and in what form it is ultimately used."[14] This situation results in unpredictable and uncontrollable intrusions into individuals' rights to respect for private life and the protection of personal data, which are particularly safeguarded by the European Charter of Fundamental Rights. Information collected for advertising purposes can, for example, reveal in which refuge women affected by violence are located, which route children of politicians take to school or where people live who actively campaign against the far right and for democracy. This may not only have a direct negative impact on those affected, but may also lead to chilling effects.

In the summer of 2024, netzpolitik.org once again obtained a dataset from a Data Broker as a free preview for a paid subscription.[15] Originating from the RTB process, the dataset covered a single day and revealed data being traded by approximately 40,000 apps. It included 47 million MAIDs linked to 380 million location data points, as well as information on devices, operating systems and telecom providers. Some apps provided precise location data capable of identifying users' residences, such as the queer dating app Hornet, Wetter Online or Flightradar24. Again, some affected individuals were identifiable. One commented[16]: "I feel under complete surveillance. It's terrifying. Seeing the points showing where I've been is suffocating. This is nobody's business and I never consented to this. I'm part of 'Omas gegen Rechts' [Grannies Against the Far Right]. During our vigils, someone from the AfD [the far right party 'Alternative für Deutschland'] always takes pictures of us. I don't want them to know where I live."[17]

However, the risks extend beyond privacy violations. AdTech companies create detailed user profiles, deriving insights using behavioural psychology and statistical methods, which are then used to influence consumer decisions. The risk for abuse by this **imbalance of power** is immense. Personal data is exploited to **target individual vulnerabilities**, such as emotional states or personal insecurities (see examples above), enabling manipulative strategies that subtly guide purchasing behaviour. „Physical and psychological harm to health may result from the targeting of particularly vulnerable groups (such as children or addicts). For example, when advertising specifically targets

[13] See Information Commissioner's Office: Update report into adtech and real time bidding, 2019, pp. 19ff, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, 29.01.2025.

[14] Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), p. 28.

[15] Dachwitz, Ingo; Meineck, Sebastian: New data set reveals 40,000 apps behind location tracking, 2025, https://netzpolitik.org/2025/databroker-files-new-data-set-reveals-40000-apps-behind-location-tracking/, 29.01.2025.

[16] Meineck, Sebastian; Dachwitz, Ingo: „Schnauze voll!" – das sagen Betroffene, 2025, https://netzpolitik.org/2025/databroker-files-schnauze-voll-das-sagen-betroffene/, 29.01.2025.

[17] Translation by vzbv

mental or physical weaknesses in order to market certain products, such as real or pseudo-medications, addictive products (e.g. legal drugs) or services (e.g. games) to people with these suspected weaknesses. In this context, it is important to emphasise that all people may experience vulnerability detached from group-related vulnerabilities. […] Even digital-savvy people can be situationally vulnerable in the digital society, for example if they are overloaded with information in unexpected situations or demoralised with constant requests for decisions."[18] This undermines consumer autonomy, as decisions are shaped by external influences rather than personal preferences.

An investigation by netzpolitik.org in 2023 showed how AdTech companies use tracking and profiling to exploit users' individual behaviour and vulnerabilities.[19] Researchers accessed the Ad Exchange Xandr, exposing over 650,000 segments in which AdTech companies categorised consumers according to keywords such as "Marlboro", "weight loss", "casino and gambling activities", "speculative investments", "fragile seniors" and "mums that shop like crazy". Moreover, netzpolitik.org's investigation showed how sensitive personal data is processed for tracking and profiling. Identified Categories included "eating disorder", "opiate addiction", "Arabic", "LGBTQ" and "breast cancer".

Discrimination is another major concern. Certain marginalised groups may be excluded from receiving certain advertisements or may be unfairly targeted based on their profiles. „For example, groups (which are mostly already socially disadvantaged) when looking for a job or flat may be excluded from these jobs or flats through personalised advertising for these jobs or flats."[20] Additionally, misleading advertisements or highly personalised offers can lead to financial losses or unhealthy choices, such as the promotion of harmful products.

A study by researchers from the Massachusetts Institute of Technology and the London Business School revealed that women see fewer career ads in the fields of science, technology, engineering and maths than men. In the study, a gender-neutral STEM career ad was placed on various social platforms and on Google's ad distribution network, which is responsible for distributing ads on various websites. As a result, 20 percent fewer women than men were exposed to the ad. According to the report, „this happened because younger women are a prized demographic and are more expensive to show ads to" and the advertising algorithms were designed to optimise the cost-effectiveness of the ads.[21]

Again, the use of AI largely amplifies these existing risks: "It threatens to make processes even more opaque, less fair and less contestable. The advancing and unpredictable opportunities in utilisation of AI includes challenges related to data protection

[18] Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), p. 30f.

[19] Netzpolitik.org: Die Xandr-Recherche, 2023, https://netzpolitik.org/tag/die-xandr-recherche/, 29.01.2025.

[20] Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), p. 30.

[21] Lambrecht, Anja; Tucker, Catherine: Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads, 2019, in: Management Science, H. 7, S. 2966–2981, https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2018.3093, 29.01.2025.

and regulation. Not least because AI enables the creation of hyper-personalised ad messages and targeting to individual consumers."[22]

Beyond individual harms, the **structural risks for society** associated with personalised advertising are deeply troubling. The exploitation of personal data exacerbates societal polarisation and fragmentation by isolating groups with targeted content. For example, political advertisements tailored to specific audiences may amplify divisions rather than fostering dialogue. Also, "the manipulation of individual voting decisions may have an **impact** not only on the individual's freedom to vote but also **on the democratic system** as a whole, just as the increasingly fine-grained customisation of insurance policies may undermine the principle of **social solidarity**."[23]

Moreover, the sheer volume of data collected and shared significantly increases **cybersecurity risks**, "not only for individual systems or organisations, but extend to critical infrastructure as a whole, e.g. through the more efficient distribution of malware or the tracking of people within the security sector"[24].

In August 2024, the State Office for the Protection of the Constitution of Baden-Württemberg issued a warning about a cyberattack campaign orchestrated by the state-controlled Russian cyber actor APT28. This attack specifically focused on diplomats through fake advertisements for luxury cars ("Diplomatic Car For Sale"), placed on legitimate websites. The intended victims were deceived into opening the fake advertisements and downloading the malware.[25]

Similarly, such campaigns targeting consumers can be exploited for online banking fraud, to steal confidential data (e.g., login credentials) or to deploy ransomware (that encrypts the victim's data and demands a ransom for decryption). Users often become infected without taking any direct action themselves. This cyber-threat by malvertising through online ads is so severe that the German Federal Office for Information Security (BSI) has issued strong warnings, even advising consumers to use ad blockers.[26]

The extensive use of data-driven technologies also presents significant **environmental concerns**.[27] The energy-intensive processes required for data collection, storage and analysis strain natural resources, contributing to environmental degradation.

All the harms raise fundamental questions about the adequacy of current regulatory frameworks and whether the control of these risks "should depend on the decision-making freedom of individuals or whether objective measures are needed"[28].

---

[22] Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), p. 31.

[23] Ebd., p. 32.

[24] Ebd.

[25] Landesamt für Verfassungsschutz Baden-Württemberg: Ausgeklügelte Cyberkampagne eines russischen Cyberakteurs, 2024, https://www.verfassungsschutz-bw.de/,Lde/Startseite/Arbeitsfelder/Cyberkampagne+APT+28, 29.01.2025.

[26] Bundesamt für Sicherheit in der Informationstechnik: Cyber attacks via online advertising, https://www.bsi.bund.de/dok/14095664, 29.01.2025.

[27] See Chapter 2.3; Armitage, Catherine, et al. (2023) (wie Anm. 7), pp. 89ff.

[28] Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), p. 32.

> The AdTech ecosystem incentivises unchecked data collection and aggregation, creating significant risks and harm for individuals and society. Without effective regulatory intervention, the misuse of personal data will continue to escalate, undermining privacy, equality and trust. Proper regulation must limit invasive practices, enforce transparency and ensure accountability across the value chain to safeguard individual rights and protect societal values in the digital era.

3. CONCEPTUAL AND PRACTICAL LIMITATIONS OF THE CONSENT MODEL

In most cases, AdTech companies try to justify data processing with the consent of the data subjects. However, the consent model faces significant conceptual and practical issues. Conceptually, the complexity and business practices of the online advertising market makes it virtually **impossible for consumers to understand** how their data is collected, processed and used. "[…] there is hardly any transparency about which actors have access to which personal data and in what way. To achieve this, the actors involved would have to coordinate in such a way that consumers would still be informed about who has what information about them even if these players do not have a direct end-user interface with consumers, but are active further down the data value chain. Consequently, there is hardly any effective consent mechanism through which laypersons can effectively control who gets access to what information or not."[29]

Furthermore, while consent is primarily used to protect privacy, it is **poorly suited to address broader risks** such as manipulation, discrimination or material and mental harm.[30] Consumers are unlikely to consent to such risks, even when fully informed. Moreover, consent mechanisms are inadequate for managing structural societal risks like threats to democracy, public discourse or fair competition, raising doubts about whether individual decisions should be the basis for addressing these collective risks.

From a practical perspective, the consent model suffers from numerous shortcomings.[31] Consent processes frequently employ **deceptive designs** that encourage agreement rather than refusal. The **overwhelming number of consent requests** exacerbates consumer fatigue, leading to thoughtless approvals that undermine the model's effectiveness. Moreover, studies show that even "consent given through a cookie banner that is designed according to current best practice rules is unlikely to constitute effective consent within the meaning of Art. 6 sect. 1 lit. a and Art. 25 sect. 1 GDPR"[32].

At the heart of the problem, however, lies the fact that data is frequently used beyond its original consented purposes, reflecting **poor implementation of purpose limitation** principles and **inadequate oversight**. Finally, users struggle to weigh up perceived benefits of personalised advertising against the risks, as the **risks are often concealed**, fostering widespread distrust and resignation. "In summary, it can be said that the problems that consumers see in the current practice of personalised advertising are

[29] Ebd., pp. 33f.

[30] See ebd., p. 35.

[31] See ebd., pp. 35ff.

[32] Ebd., p. 37.

so serious that there has been a widespread loss of trust in this form of data processing; consumers feel caught between powerlessness and fatalism."[33]

A particularly concerning development is the rise of so-called **pay-or-okay models**.[34] These models force users to choose between paid, tracking-free services or services that do not require a fee but include personalised advertising. Such models offer no real benefits to consumers. Instead, the European Court of Justice has ruled that users must retain the freedom to refuse consent to data processing without being forced to forgo the service entirely. However, the proliferation of these models creates a pervasive system in which users are frequently compelled to choose between tracking or the financial burden of subscription fees. Since few users can afford to pay for numerous services, they are effectively coerced into accepting tracking – not out of genuine agreement, but economic necessity. This dynamic threatens to make data protection a privilege reserved for wealthier users. What may appear legal - when assessing only the practice of a single company - can, within a systemic context, erode the fundamental principles of fairness and choice that underpin the GDPR. Moreover, the conceptual and practical shortcomings of consent persist within these models. This leads to the situation that users are forced to choose between **paying a fee or providing consent that fails to meet GDPR requirements**. Here again, "these risks may only be countered with objective requirements for personalised advertising that reduce the risks to a socially acceptable level, even for those who give their consent to personalised advertising (especially for those who did so due to a lack of financial means)."[35]

Some observers argue that consent as a legal basis for personalised advertising cannot be upheld and that it just shifts responsibility to the data subjects[36]. However, the authors of the report commissioned by vzbv suggest that these limitations can be addressed and mitigated through suitable measures[37]. However, they emphasise that "risks arising from the advertising ecosystem need to be reduced to a socially acceptable level through objective requirements for personalised advertising. Only then, in a second step, can transparency measures and consent mechanisms be redesigned so that they can once again fulfil their purpose. The reduction of risks is a prerequisite for more effective transparency and user control measures."[38]

> The limitations of the consent model highlight the urgent need for stricter rules for the entire advertising ecosystem to reduce risks related to privacy, manipulation, discrimination or material and mental harm. Only after these risks have been mitigated by the legislator, can the relevant stakeholders redesign transparency mechanisms and consent processes to empower users and rebuild trust in data processing. Prioritising risk reduction is essential to ensure meaningful consumer protection.

[33] Ebd., p. 35.

[34] See ebd., pp. 54ff.

[35] Ebd., p. 56.

[36] See Lisker, Mareike: Von der (Un-)Möglichkeit, digital mündig zu sein, 2023, Chapter 3 and p. 75, https://api-depositonce.tu-berlin.de/server/api/core/bitstreams/5f032944-eb28-4e06-b5bd-30a8d08695c9/content, 29.01.2025.

[37] See Chapter 4; Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 115ff.

[38] Ebd., p. 7.

4. RISK CONTROL APPROACHES FROM CIVIL SOCIETY AND INDUSTRY

Since the early 2010s, various approaches to mitigate the risks associated with personalised advertising have been discussed, particularly in response to growing concerns about privacy and data protection.

Contextual advertising[39] is a method of displaying ads based on the content being viewed, such as articles on health or technology, without processing personal data. This is achieved through URL analyses or linguistic methods that classify content and place thematically appropriate advertisements. Privacy advocates consider contextual advertising a privacy-friendly alternative to personalised advertising, as it eliminates the need for tracking and profiling. Reports even indicate higher revenues gained through context-based advertising as compared to personalised advertising. For example, several media companies – including the New York Times[40] and the Dutch public broadcaster[41] – have reportedly increased ad revenues after moving away from programmatic advertising and adopting contextual advertising models.

However, this approach is not without its weaknesses. The lack of standards has led to instances where methods labelled as contextual still process personal data, a phenomenon referred to as “privacy-washing”. Additionally, there is a risk that companies deliberately misuse context data for manipulative purposes or to exploit vulnerabilities, such as serving diet program ads alongside content related to eating disorders. Furthermore, advertisers are increasingly trying to use AI and natural language processing to infer the mood of the target group from the content consumed. On this basis, advertisers can tailor their messages to the current emotional state of the audience and thus increase engagement and effectiveness. This raises concerns about manipulation and invasive practices, such as exploiting emotional vulnerabilities or influencing sensitive decisions.

Personal Information Management Systems (PIMS)[42], also known as data trustees, privacy agents or privacy dashboards, are another widely discussed approach to empower users to manage their privacy preferences centrally. By providing users with more time and tools for informed decision-making, PIMS aim to alleviate consent fatigue and simplify privacy management. However, while there are promising initial concepts developed by civil society, practical implementation by the industry has revealed that existing models tend to serve the interests of the AdTech companies rather than those of consumers. In some cases, commercial PIMS may even enhance tracking capabilities instead of strengthening data protection, for example by using centralised identifiers to track users across multiple services.[43]

In general, the critical question is whether PIMS can truly live up to the expectations within the system of personalised advertising – especially when providers of digital services can implement PIMS on a purely voluntary basis. If PIMS were to genuinely

---

[39] See ebd., pp. 53ff.

[40] Davies, Jessica: After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue, 2019, https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/, 29.01.2025.

[41] Lomas, Natasha: Data from Dutch public broadcaster shows the value of ditching creepy ads, 2020, https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/, 29.01.2025.

[42] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 44ff.

[43] Ebd.

strengthen users' decision-making power, many providers might refrain from adopting them altogether. While, in the view of the authors of the report commissioned by vzbv, PIMS show some potential to empower users, their ability to do so depends heavily on the establishment of cooperative mechanisms between actors – such as PIMS-providers, publishers and AdTech-companies – and proper regulatory frameworks to safeguard consumer interests.

Discussions within the AdTech industry have also focused on new personalised advertising methods such as **cohort-based[44] and interest-based[45] approaches**, which aim to reduce individual data insights while meeting advertising demands. Unlike traditional tracking methods, these approaches do not rely on cookies but shift personalisation into the web browser itself. Cohort-based advertising groups users by shared characteristics derived from behavioural patterns, thereby reducing direct privacy intrusions. Similarly, Google's proposed Topics API, part of its Privacy Sandbox Initiative, is designed to analyse user browsing behaviour weekly to assign interest-based topics. Advertisers would access only one topic at a time and users would be given options to adjust or delete their profiles. By retaining data for just three weeks, the proposed Topics API aims to minimise profiling compared to traditional tracking methods.

Both cohort-based and interest-based approaches still pose privacy and ethical concerns, including risks related to tracking, re-identification, manipulation and discrimination. Furthermore, Topics has faced criticism for its centralised control by Google, which potentially reinforces the company's market dominance. These issues persist despite the reduced focus on individual profiling, and underscore the need for stronger safeguards, greater transparency and regulatory oversight to ensure such models prioritise consumer interests and protect fundamental rights.

There have also been **government-initiated and voluntary initiatives**[46] such as the European 'Cookie Pledge Initiative', which sought to establish an unified framework for cookie consent based on transparency and simplicity, and the German 'Good Practice Initiative for Cookie Consent Management', which focused on practical guidelines to standardise cookie banner designs and reduce user frustration while improving consent practices. However, these initiatives ultimately proved unsuccessful. Most importantly, their exclusive focus on cookie banners bear the risk of entrenching the existing ineffective level of protection, characterised by superficial compliance measures that fail to address fundamental issues such as inadequate user understanding of consent options, lack of transparency in data processing practices and limited accountability for misuse of data. Moreover, the initiatives lack legally binding provisions that are however critical to ensure consistent implementation and compliance across the ecosystem, as voluntary measures often fail to create accountability or incentivise meaningful participation. Notably, even these relatively modest initiatives were largely rejected by the AdTech industry. This demonstrates once again that voluntary commitments in this area are insufficient and that regulatory measures are required to address these issues effectively.

> Numerous initiatives and approaches by civil society and the AdTech industry aim to mitigate the risks associated with personalised advertising, focusing on various tech-

[44] See ebd., pp. 48f.

[45] See ebd., pp. 49ff.

[46] Ebd., pp. 56ff.

nical, organisational and regulatory aspects. Some of these approaches are promising from a data protection perspective. However, each approach also presents its own weaknesses and introduces new risks. Even without these limitations, they fail to constitute a coherent and comprehensive protection system.

III. CURRENT REGULATORY APPROACHES

In principal, personalised advertising is already regulated by existing European data protection laws, such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD). Furthermore, in recent years, legislators have enacted a series of sector-specific rule books that at least partially regulate personalised advertising, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the Regulation on the Transparency and Targeting of Political Advertising (TTPA) and the Artificial Intelligence Act (AIA). However, to what extent do these laws protect consumers from the systemic risks posed by personalised advertising? What gaps and issues remain? And which of their regulatory approaches could serve as inspiration for further regulation to address risks and close gaps?

1. GENERAL DATA PROTECTION REGULATION (GDPR)[47]

GDPR establishes a comprehensive framework for protecting the rights of data subjects. However, **GDPR lacks specific provisions** for personalised advertising, which has led to insufficient implementation of its principles in practice. The use of vague legal terms and balancing tests was intentionally chosen by the legislator to ensure flexibility in the face of technological developments and to promote fairness in individual cases. This flexibility, however, also generates legal uncertainty, making the enforcement of GDPR more complicated and leading to prolonged legal disputes.

In particular, GDPR provides a **broad definition of profiling** but does not address the associated risks in detail. Specific requirements apply only when profiling results in automated decisions that produce legal effects or significantly impact to individuals.[48] For advertising-related profiling, only the general GDPR principles apply[49], even though advertising-related profiling poses considerable risks. The general principles lack clear boundaries to ensure decision-making autonomy and to prevent discrimination, such as banning certain invasive practices. The European legislator has introduced sector-specific bans on high-risk profiling through the DSA and the TTPA, but no horizontal rules exist to date. Again, the broad definition of profiling in the GDPR creates uncertainties regarding the scope of its prohibitions.

Furthermore, GDPR grants special protections only to certain **vulnerable groups**, such as children or in the context of sensitive data. This approach overlooks the existing in-

[47] See ebd., pp. 67ff.

[48] Such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

[49] See Article 29 Data Protection Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2028, p. 22, https://ec.europa.eu/newsroom/article29/items/612053, 29.01.2025.

formational and power imbalances in the digital world (discussed as “digital asymmetry”[50]). Advertising companies exploit these imbalances by categorising users based on personal preferences and vulnerabilities to target them accordingly (see above). Existing obligations, such as the provision of information and access on the basis of consent, contribute little to solving this issue.[51] Every individual must be considered vulnerable in these contexts. This makes a new regulatory approach all the more necessary.[52]

To minimise risks, the principle of **purpose limitation** is intended to ensure that data is used solely for its original collected purpose. This principle aims, inter alia, to empower individuals to make informed decisions regarding data use. Companies must specify their processing purposes clearly and precisely, a standard often unmet in personalised advertising, where vague terms like “'improving the user experience” or “marketing purposes” prevail.[53] This lack of transparency renders consent ineffective, as the extent of data processing remains unclear for the data subject. Moreover, technical and organisational measures to prevent unlawful processing are often absent, as exemplified by the TCF, which does not mandate reporting obligations for data misuse. The industry criticises GDPR for being too vague and that authorities provide insufficient guidance on defining data processing purposes, which in turn would lead to uncertainties. However, “it is doubtful whether the problem in fact arises from controllers being in a position not able to define a precise purpose. Or rather that controllers want to gloss over the true purposes in the best possible way.”[54] A new regulatory approach should ensure that companies have to specify and differentiate purposes in a clear and understandable way in order to identify and mitigate risks for individuals and society.

The principle of **data minimisation** mandates limiting data collection to what is necessary for the processing purpose. In the context of social networks, the Court of Justice of the European Union has emphasised that indiscriminate use of all data, regardless of sensitivity, constitutes a disproportionate interference. Data should be collected and stored only if essential. Unlimited data retention is disproportionate as it entails potentially boundless data volumes and creates a sense of perpetual surveillance. These requirements should extend to the advertising ecosystem as it has historically processed excessive data. However, “the way personal data is organised and stored, is in direct contrast to the principles to […] keep the data relevant and limited to what is necessary for the marketing purposes.”[55] Future rules should establish clearer limits on the scope of legal data processing.

To implement its provisions, GDPR underscores “**data protection by design**”, requiring safeguards throughout all stages of data processing. This entails system design, empirical validation of the measures’ effectiveness and adherence to the state of the art. Empirical validation is particularly crucial to prevent manipulation and discrimination in personalised advertising, where systems often prioritise industry interests over those of individuals. Controllers must demonstrate how their systems address risks such as

---

[50] See Helberger, Natali u. a.: EU Consumer Protection 2.0 - Structural asymmetries in digital consumer markets. A joint report from research conducted under the EUCP2.0 project, 2021, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf, 29.01.2025.

[51] See ebd., pp. 29ff.

[52] See ebd., S. 7ff.

[53] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 68ff.

[54] Ebd., p. 70.

[55] Ebd., p. 73.

manipulation and discrimination. However, practical implementation faces significant shortcomings, including a lack of expertise and guidance.

While GDPR was intended to improve **enforcement** against international players and high-risk business models, the practice of data protection authorities (DPAs) falls short of expectations, particularly in the area of personalised advertising.[56] The market's complexity and lack of transparency make it challenging to identify which entities process personal data and who bears responsibility. Effective enforcement is hindered by limited resources and limited technical expertise, compounded by the DPAs broad portfolios and constrained staffing. Moreover, some DPAs receive thousands of complaints annually about minor infringements, diverting resources away from systemically relevant cases. Finally, some companies exploit procedural objections, prolonging litigation and exacerbating the imbalance between DPAs and corporations. Despite significant enforcement efforts since 2018, the number of resolved relevant cases remains low. Without clear legal imperative, companies are unlikely to discontinue criticised practices.[57]

2. DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS (EPD)[58]

The ePD from 2009 regulates personalised advertising by allowing access to and storage of information on user's devices only with prior user consent (or within a narrow technical exception). This includes the use of cookies for tracking and advertising. It complements GDPR, as it applies regardless of whether the stored or accessed information qualifies as personal data. However, the subsequent processing of personal data enabled by such access remains subject to the general provisions of GDPR.

Since the ePD already requires user consent and clear information before allowing access to users' devices, it creates – in principal - a significant barrier to data processing for personalised advertising. However, despite its technology-neutral approach, the **evolution of new tracking methods** such as fingerprinting, MAIDs, server-side tracking and the deployment of AI has created uncertainties. These include difficulties in detection, assessing legal compliance (as it is disputed whether information is stored on or retrieved from users' devices) and the circumvention of user consent mechanisms.

Moreover, the ePD relies exclusively on consent as a legal basis and does not establish clear limits for personalised advertising. Regarding the requirements for consent, it merely refers to GDPR. "Likewise the same interpretation questions arise regarding how freely, specific, informed and unambiguous a user's permission was given. In consequence, the same disputes regarding a lack of transparency, manipulation of user decision-making by dark patterns and alike influence how the law is applied."[59]

To counter these shortcomings, the ePD was intended to be replaced, modernised and harmonised across the EU by a proposal for an ePrivacy Regulation, published by the European Commission in 2017. However, even after eight years, no consensus has been reached between the European co-legislators. Therefore, a new regulation that

[56] See in detail Chapter 3.1.3; ebd., pp. 78ff.

[57] See Armitage, Catherine, et al. (2023) (wie Anm. 7), p. 249 and p. 252.

[58] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 86ff.

[59] Ebd., p. 89.

effectively protects consumers by closing gaps in the regulation of tracking technologies and harmonising enforcement mechanisms across Member States remains urgently needed.

3. DIGITAL MARKETS ACT (DMA)[60]

The DMA, which came into force in November 2022, aims to increase competitiveness in concentrated digital markets. It addresses abuse of market power by large digital platforms that play a systemic role within the EU internal market ('gatekeepers'). These include large online marketplaces, social media networks, search engine providers and (mobile) operation systems that dominate their respective sectors. It complements competition law by countering unfair practices of these gatekeepers towards businesses and end users. Notably, it imposes restrictions on the commercial use of data that these platforms can collect and use across different services.

Inter alia, the DMA **prohibits gatekeepers from using, combining or sharing personal data across services without obtaining explicit user consent**. Such consent must adhere to the standards set by the GDPR. Requests for the same consent may only be made once a year to reduce user fatigue. Additionally, gatekeepers are required to offer a less personalised yet equivalent alternative.

However, the DMA does not comprehensively address the fundamental issues and risks of the current online advertising ecosystem. Its scope is limited to a small number of gatekeepers and specific processes, which prevents the achievement of fundamental transparency or simplification of the system. Furthermore, the effectiveness of the DMA relies heavily on consent requirements, which are grounded in GDPR and therefore share the inherent issues analysed above, such as the risk of consent being granted without a full understanding of its implications. Also, as a vzbv report shows: gatekeepers implement this DMA obligations inadequately and use deceptive designs to make users consent to the combination of data across their services.[61]

4. DIGITAL SERVICES ACT (DSA)[62]

The DSA, which also came into force in November 2022, addresses risks associated with online platforms, focusing on the spread of content that violates existing laws by infringes individual rights or societal interests. The DSA focusses on the role platform providers play in facilitating such dissemination. Unlike GDPR, the DSA **emphasises the dangers associated with tracking and profiling for advertising purposes**: these manipulative techniques could adversely impact entire groups and exacerbate societal harm, for instance, by contributing to disinformation campaigns or discriminating against specific groups.[63]

Accordingly, the DSA **prohibits** online platforms from displaying ads to users based on profiling, as defined under GDPR, that involves special categories of personal data or data of minors. However, GDPR's broad definition of profiling creates uncertainties about the scope of these bans. Furthermore, like GDPR, this approach fails to address

---

[60] See ebd., pp. 107ff.

[61] Verbraucherzentrale Bundesverband: Combining Data and Bundeling Services under the Digital Markets Act, 2024, https://www.vzbv.de/sites/default/files/2024-07/DMA-Report_English_2.pdf, 29.01.2025.

[62] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 103ff.

[63] „When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups."; Recital 69 DSA

the existing digital asymmetry. In the context of personalised advertising, every individual should be considered vulnerable.

Platform providers are required to provide **transparent information** enabling users to understand why they are being shown a specific advertisement. This includes details about advertisers funding the ad and the targeting parameters used. Very large online platforms (VLOPs) face additional transparency obligations, such as maintaining a public advertising repository containing information about their target audiences and their reach. VLOPs are also required to provide an "on/off" toggle for recommender systems. The DSA further introduces co-regulatory tools, such as codes of conduct, akin to those in GDPR.

However, the scope of these rules is limited to platforms/intermediaries and does not extend to tracking and profiling practices across the open internet. While absolute bans on profiling for advertising purposes are a welcome development, it can only be an initial step towards addressing the aforementioned issues.

5. REGULATION ON TRANSPARENCY AND TARGETING OF POLITICAL ADVERTISING (TTPA)[64]

The TTPA came into force in April 2024 to enhance the transparency of political advertising within the EU, ensure the integrity of election campaigns and combat disinformation. It contains structural requirements and rights for data subjects that specify or complement GDPR. It contains explicit prohibitions and obligations linked to specific processing activities.

The processing of personal data for political targeting is allowed under the TTPA only if the data is **directly collected from the data subjects and no sensitive data is used for profiling**. However, as already observed with the DSA, ambiguities arise regarding the scope of the rules due to the broad definition of profiling and the narrow understanding of sensitive data in GDPR. Additionally, there is uncertainty on whether data collected by joint controllers is also subject to these restrictions or whether it could constitute an exception.

The TTPA obliges publishers of political advertising to provide comprehensive **transparency** information. This includes details about the sponsor of the advertisement, the target audiences and the categories of data used. This information must be easily accessible and linked to the advertisement. Furthermore, the TTPA introduces a **public European advertising repository**, where political advertisements and their accompanying information will be accessible for a period of seven years. The aim is to identify societal risks and foster public debate. Additionally, actors within the advertising ecosystem are required to exchange information in machine-readable formats and to notify each other of errors or gaps to fulfil transparency obligations.

6. ARTIFICIAL INTELLIGENCE ACT (AIA)[65]

The AIA, which came into force in August 2024, aims to ensure a high level of protection for health, safety and the fundamental rights enshrined in the European Charter of Fundamental Rights against the harmful effects of AI systems. Its scope is broadly de-

[64] See Grafenstein, Max von; Herbort, Nina (2024) (wie Anm. 1), pp. 100ff.

[65] See ebd., pp. 94ff.

fined and closely resembles a general product safety regulation for AI systems. Accordingly, its structure aligns with product liability law and primarily imposes general obligations rather than granting individual users' rights.

"In contrast to the GDPR, which only sets conditions for the processing of personal data to ensure that the risks for the data subjects concerned are proportionate to the added value (of the data processor, third parties and/or the general public), the AI Act contains a real **ban on certain AI practices**"[66], including the use of subliminal or manipulative techniques that significantly distort the behaviour of individuals or groups, leading to harmful decisions; exploiting vulnerabilities of individuals or groups (e.g. on age, disability or social status) to manipulate their behaviour, resulting in substantial harm; and employing AI systems for social scoring of individuals or groups that results in unfavourable treatment in unrelated contexts. However, terms like "substantial harm" or "discriminatory treatment" are open to interpretation. Moreover, it presupposes a degree of intent on the part of the providers that is difficult to prove in practice.

The AIA sets out detailed rules for the **technical and organisational design** of so-called high-risk AI systems. They must implement specific measures, such as risk management systems, data quality and technical documentation. It also specifies **coordination duties** among providers, importers, distributors and deployers. Providers must undergo a conformity (self-)assessment, affix a CE marking and register the system in an EU database. Deployers, importers and distributors must ensure that only compliant systems are placed on the market and must report emerging risks and serious incidents to the authorities and take corrective actions. Deployers must operate systems according to instructions, ensure oversight and notify relevant parties of risks.

The AIA's provisions do not apply to personalised advertising since such systems are generally not classified as high-risk AI systems. However, the AIA could inspire new legislation for personalised advertising regarding the definition and distribution of obligations among actors in the ecosystem and serve as generally accepted rules or state-of-the-art practices for interpreting "data protection by design" under GDPR.

> Existing laws like GDPR, the ePD and related EU regulations struggle to adequately address the systemic risks posed by personalised advertising. GDPR's flexibility and broad definitions have inadvertently fostered legal uncertainty and implementation challenges. Sector-specific laws like the DSA, the TTPA or the AIA offer valuable measures but fall short of establishing comprehensive protections, as their scope is limited to specific actors or contexts rather than addressing the ecosystem as a whole. Therefore, the EU should introduce a new horizontal legal framework to address the risks posed by personalised advertising to individuals and society. Such framework should establish clear limits on data processing, mandate proper transparency measures and strengthen enforcement. The exploitation of digital asymmetries and vulnerabilities mandates protections that extend beyond individual consent to safeguard societal interests and uphold fundamental rights in the digital age. Specifically, tracking and profiling for advertising purposes should be prohibited.

[66] Ebd., p. 95.

IV. OUTLINES FOR A NEW REGULATION

As shown, in recent years, the European legislator has introduced several laws addressing aspects of personalised advertising. The comprehensive review of these laws reveals a discernible trajectory in the legislator's approach. For instance, the regulators have increasingly implemented explicit bans on certain data processing methods, like combining or cross-using personal data, and the processing of certain data categories, delineated clearer legal standards for particular sectors and actors and imposed structured technical and organisational cooperation obligations. These findings and approaches provide a foundation for developing a new regulation for personalised advertising.

In light of these considerations and the report commissioned[67], vzbv concludes that such regulation should at least include the simultaneous implementation of the following substantive procedural, technical and organisational measures across multiple levels, ensuring these efforts are both aligned and complementary.

1. BANS ON TRACKING AND PROFILING FOR ADVERTISTING PURPOSES

It is essential to counter the significant threat that certain advertising practices pose to individual consumers as well as the structural risks they pose to society . These risks can be significantly mitigated through a **ban on data processing for specific purposes and some types of processing methods**, as well as a prohibition on the use of particular categories of data.

To address the core of the data processing chain, comprehensive **restrictions on cross-site tracking** are vital. Such a ban would ensure that only the data necessary for first-party advertising is collected, thereby preventing the construction of detailed user profiles. The TTPA adopts a similar approach by mandating that controllers process only data collected directly from data subjects. However, a clear and enforceable definition of cross-site tracking would be necessary to ensure the prohibition covers all methods of linking user activities across websites, apps, services or devices for advertising purposes, regardless of the technology employed.

Another approach draws partial inspiration from the DMA, which restricts gatekeepers from **combining or cross-using personal data** without explicit consent. However, expanding this restriction to encompass all actors in the advertising ecosystem requires adaptation, as the current framework leaves loopholes, such as the continued reliance on consent as a legal basis. Therefore, a future legal framework should include a clear ban on merging collected data with external datasets, such as offline information or data enriched through Data Brokers. Synchronisation techniques within advertising systems have advanced to the point where siloed data collection no longer guarantees data isolation. Also, companies should be prohibited from collecting or storing consumer data during participation in online advertising auctions for purposes unrelated to the auction itself.[68] Additionally, inferred data presents additional risks, as it can lead to inaccurate conclusions or sensitive inferences, increasing user vulnerability. New regu-

[67] See Chapter 5; ebd., pp 128ff.

[68] As it was an order from the FTC to Mobilewalla. Federal Trade Commission (wie Anm. 3).

lation should therefore **restrict companies from deriving further attributes** from collected data to mitigate threats to privacy and individuals' autonomy. These measures would significantly affect all stages and actors within the advertising ecosystem, representing a decisive regulatory intervention.

Besides the ban on specific purposes and processing methods, the processing of **sensitive data types and the targeting of vulnerable groups** should be prohibited. This is already partially reflected in the TTPA and the DSA. Both frameworks limit "targeting techniques" or "ad-delivery techniques" that rely on profiling using special categories of personal data. However, GDPR's broad definition of profiling creates ambiguities, leading to uncertainties about the scope of such prohibitions. Furthermore, in the digital age, all users are vulnerable to situational risks, regardless of demographic characteristics or whether sensitive data is processed. Even tech-savvy users may encounter online scenarios where they face exposure to risks, for example when AdTech companies exploit their individual vulnerabilities, as shown above. The AIA reflects this by prohibiting AI systems that exploit vulnerabilities of individuals or specific groups in certain circumstances. However, more precise definitions tailored to the online advertising sector are necessary. These should include, for example, expanding the definition of sensitive data to incorporate geolocation data and a broader understanding of situational vulnerabilities.

With these proposed measures, the ecosystem of programmatic advertising and real-time bidding would undergo a **fundamental transformation**, shifting its focus from user-profile-driven targeting to a more context-based approach. This paradigm change prioritises data minimisation and user privacy while maintaining the core functionalities of automated auctions for ad placements: In this revised framework, when users visit a digital service, an automated auction process will still be initiated. However, Supply-Side Platforms would be restricted to including only first-party information and non-personalised contextual signals in bid requests. Such data could encompass the content of the webpage, ad placement details (e.g. size or location on the page) and general device information (e.g. browser type or operating system). The prohibition of external data merging would also eliminate the role of Data Brokers in supplementing bid requests with third-party data. This ensures that ad profiles remain devoid of sensitive data and data such as browsing history or offline user activity (e.g. loyalty card data and geolocation information). Instead, advertisers and DSPs would rely exclusively on their first-party datasets (e.g. anonymised customer purchase histories collected through their own platforms) or aggregated, non-individualised insights to guide bidding strategies.

These changes would incentivise advertisers to shift their strategies towards contextual targeting, prioritising the alignment of ad placements with specific content instead of relying on behavioural profiling of individuals. Publishers would need to focus on enhancing the value of their ad spaces through quality content and audience engagement rather than leveraging user tracking. Therefore, this revised system fosters a leaner and more privacy-focused advertising model. Although this shift may lead to less detailed targeting capabilities, it enhances transparency and reduces the risks of exploitation, manipulation and discrimination.

> Addressing the risks inherent in modern advertising practices requires a multifaceted regulatory approach. By restricting tracking and profiling for advertising purposes, it is possible to protect consumers and society from the harm caused by invasive advertising practices. In particular, such restriction should include a ban on practices

such as cross-site tracking, data aggregation and deriving sensitive attributes, as well as the processing of sensitive data and targeting vulnerable groups.

2. EUROPEAN ADVERTISING INDUSTRY REGISTRY

As a complementary measure to the aforementioned bans, building on practices established under the TTPA and the AIA, a European Advertising Industry Registry should be created, complemented by a mandatory certification mechanism. The registry could ensure the availability of comprehensive information necessary to identify and counter structural risks for individuals and society. Additionally, the certification mechanism could verify whether the actors involved have implemented all essential protective measures.

The **European Advertising Industry Registry** could be managed by the European Commission or a dedicated EU agency. It should require all entities processing personal data for personalised advertising to register and obtain a unique Ad Industry ID. To register, companies should need to provide information such as their name, address, role in the advertising ecosystem, the types of data and identifiers used, the purposes of data processing and certification details. Entities failing to register should be prohibited from participating in the advertising ecosystem. Each registered actor should also be required to maintain detailed records of their data processing activities, including identifiers and interest profiles linked to data subjects, sources and dates of data collection, legal bases and purposes for data processing and recipients of personal data, along with their roles and access dates. Advertisers should be obliged to define their requirements when contracting participants in the advertising ecosystem. They should specify the nature and purpose of the advertising campaign, target audience criteria, exclusion parameters (e.g. exclusion of certain interests or data) and risk mitigation measures for data subjects. Incomplete or inaccurate records should result in a prohibition on data processing for personalised advertising.

To ensure compliance, tools provided under GDPR, such as **codes of conduct and mandatory certification mechanisms,** including external audits, should be utilised. External audits could be a pivotal mechanism to increase accountability, in particular for gatekeepers. They compel these entities to disclose their practices, demonstrate legal compliance and ensure that they do not exploit their market dominance at the expense of data protection or consumer interests. Additionally, these audits ensure that data protection is not misused as a pretext for expanding market power.

The transfer of personal data should only be permitted if the recipient is registered in the Registry, specifies the intended purposes of data processing, possesses the necessary certifications and ensures that the intended processing complies with the legal basis on which the data was originally collected. If a data recipient fails to comply with these obligations, the data provider should immediately cease the data transfer and notify the relevant authorities and affected stakeholders.

To ensure effective implementation, all stakeholders within the advertising ecosystem must have clearly defined and distinct roles. As a complementary measure to prohibiting certain purposes and processing methods, establishing a European registry for the advertising industry and introducing mandatory certification would be key steps toward enhancing transparency and accountability. These measures would not only strengthen data protection but also foster trust among stakeholders, creating a more sustainable and equitable advertising ecosystem.

3. TECHNICAL AND ORGANISATIONAL MEASURES

For a new regulation to be effectively applied, it must be both more specific than GDPR and adaptable to technological developments. GDPR requires data controllers to implement **technical and organisational measures** that effectively protect fundamental rights. These measures must be **empirically proven to be effective and conform to the state of the art**. The obligation to adopt the most effective market solutions could drive continuous improvements and innovation in data protection.

However, it is crucial for effective implementation that legislators provide additional support by clarifying the elements and parameters that are particularly significant and how controllers have to demonstrate their effectiveness. For example, clarifications are needed on how data controllers should design user interfaces. Specifically, this includes details on the data basis for displaying personalised advertising, as outlined in the TTPA and DSA, and the ability to toggle personalisation on and off to assess its relevance. Consumers should have **access to information** such as interest profiles, the raw data used, identifiers and a comprehensive list of all data recipients involved. Furthermore, information and tools for **exercising data subject rights** should be easily accessible through interfaces located directly on the same page where personalised advertising is displayed. While these elements can already be derived from GDPR, they should be further specified in new regulations to prevent legal uncertainty.

> Aligning new rules with the principles of “data protection by design” while addressing specific technological and organisational aspects can significantly enhance data protection. By ensuring clarity, accessibility and empirical validation of measures, both consumers and data controllers can benefit from a more transparent and trustworthy framework for handling personal data.