Prof. Dr. Max von Grafenstein, LL.M. I Dr. Nina Elisabeth Herbort

REGULATION OF ONLINE ADVERTISING

Expert Report

20. December 2024

Commissioned by:

Federation of German Consumer Organisations –
Verbraucherzentrale Bundesverband e.V.

Digital and Media
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

CONTENT

EXECUTIVE SUMMARY

The current ecosystem of personalised online advertising is very complex; in fact, it even appears messy and chaotic. The risks are correspondingly numerous and severe. Individual risks include uncontrolled insights into the private lives of consumers, manipulation, discrimination as well as material and health damage. Structural risks for society include risks to free competition, democracy, public discourse and solidarity, and even security and environmental protection. In view of non-transparent and manipulative consent processes and the high number of consents requested per day, consumers alternate in their mood between powerlessness and fatalism. Nevertheless, some see added value in personalised advertising, at least if it makes advertising more relevant. However, consumers are not able to verify this promise of the industry.

In recent years, a number of data protection-friendly approaches have emerged in the area of personalised advertising, such as approaches to improve consent processes by Personal Information Management Services (PIMS). On the other hand, structural-objective approaches have been developed to reduce risks independently of individual control by consumers, e.g. cohort-based personalisation, topics-based personalisation, contextual advertising, as well as encrypted and aggregated conversion measurement. However, there are also developments that threaten to worsen the current situation, such as the use of data protection law and AI technologies by quasi-monopolistic providers to further accumulate economic and informational power.

With the GDPR, the EU legislator has provided a general regulatory framework that would in principle be flexible enough to control the aforementioned risks and promote emerging data protection initiatives. However, the effective implementation of the GDPR suffers from a combination of four main factors: 1) the considerable legal uncertainties, 2) the complexity of the online advertising ecosystem, 3) the resulting lack of knowledge, ability and willingness of the economic players to implement the GDPR effectively and, 4) the high legal enforcement deficit. Against this background, the legislator has adopted several new laws, such as the Digital Services Act, Political Targeting Regulation and Artificial Intelligence Act that can be read as a learning curve, in the course of which it addressed the problems described in an increasingly specific manner: 1) the clarification of legal requirements for specific sectors and actors and 2) a clear assignment of technical and organisational cooperation obligations to overcome governance problems (and knowledge deficits) in complex processing networks.

In view of all these results, we propose a combined approach that, on the one hand, bans specific processing areas and, on the other hand, provides a more effective regulatory framework for the processing of personal data for personalised advertising in general. In particular, we propose a user-related ban of the processing of personal data of vulnerable groups. Furthermore, we are also discussing bans on the processing of personal data in other specific cases (e.g. with respect to certain actors or certain processes). The most far-reaching measure would, of course, be a general ban on personalised advertising. A general ban would have the advantage of eliminating the need for coordination and is, therefore, not only the most legally effective protection but also the most economically effective. However, a general ban contains the risk of patronising those consumers who basically see added value in the personalisation of advertising (if it really makes the advertising more relevant). This is why we are discussing a general ban more as a fallback regulation should it turn out that the risks cannot be effectively contained due to the excessive coordination efforts.

The report also takes a look at options for a more effective regulatory framework for personalised advertising in general. Such a framework must meet the requirements for both more effective consumer protection and data protection, as well as for fair competition. It should be emphasised that this regulatory framework we propose will hardly lead to any additional regulatory requirements, at least not for small and medium-sized advertising services. This is because our approach is based on the TCF with its technical, legal and organisational specifications as well as certification requirements. Structurally, the requirements are thus already implemented in the advertising ecosystem. To overcome the governance problem described, we convert the requirements into an objectively legally binding system. In sum, this creates a fairer level playing field, especially in relation to quasi-monopolistic Big Tech companies.

Ultimately, 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.

To create this fairer level playing field, we propose three main shifts of the TCF by statutory law: 1) to define five sub-purposes of personalised advertising according to their risks, namely retargeting, profile-based personalisation, cohort-based personalisation, contextual advertising and – as an annex purpose – success measurement, 2) to clearly assign legal responsibilities to implement specific technical-organisation protection measures to specific entities according to their role in the online advertising ecosystem, especially in order to ensure a common visual interface for consumers to better understand their risks and benefits of the respective advertising purpose and to much more effectively exercise their data subject rights; and to control comprehensive and effective implementation of these protection measures through GDPR-certification mechanisms, 3) to register all involved entities with all categories of identifiers, data, and inferred information that they use for the different advertising purposes in order to provide the knowledge basis for cross-societal oversight.

This legal framework is suitable for remedying deficits in the system at various levels. By creating transparency on an unprecedented scale and redesigning consent processes, it will first and foremost create a level playing file for users by reducing their risks to a socially acceptable level. Realistically, for the industry to work with and not against, economic benefits for the online advertising ecosystem will also be achieved: on a micro- and meso-economic level, innovative advertising services can gain a competitive advantage by restoring consumer trust with more privacy-friendly technologies. If this ensures that users are willing to engage with the technologies and their choices in the first place, studies show that more consent for certain processes can be achieved. On a macroeconomic level, this regulatory proposal creates a market in which consumers' expectations of online advertising and advertisers' offers can finally be brought into an efficient balance. Only when the coordination required for a socially sustainable advertising ecosystem proves to be prohibitively challenging, despite the approach proposed here, the legislator may have to ban personalised advertising in general. The risks to consumers and society caused by current online advertising practices are too high. However, in such a case, it is worth to emphasise again that a complete ban of personalised advertising would not only be the most legally effective measure, but also the most economically effective.

1. INTRODUCTION[*]

Saying that „Digital advertising is the lifeblood of the internet“[2] may sound exaggerated. But it's not. The industry selling the personalisation of such advertising like it was dopamine, something everybody needs for more happiness and joy, may sound surreal. But they do.

Digital advertising is the foundation for various business models that came alive or could only stay alive because the global advertising market has grown enormously. It was valued at 319 billion US Dollar in 2019, at 550 billion US Dollar in 2022[3] and is expected to reach 1089 billion US Dollar by 2027.[4]

This growth became possible by turning a simple two-party-system, where deals were arranged directly among advertiser and publisher into a brand new market with a network of hundreds of actors.[5] It started with the promise of new user experiences and increasing revenues, but quickly became a highly complex and opaque system that even the actors involved are no longer able to fully understand or control.[6]

The financial added value – which is mainly concentrated by a few major companies[7] – is offset by priceless high risks not only for individual internet users, but for society as a whole. The risks range from individual risks for the private lives of consumers, their autonomy in particular (but not only) when purchasing consumer goods, non-discrimination, health and finances, to societal risks for a democratically constituted society, a fair market economy, security and environmental health.

Up today, the advertising industry barely addresses these risks, but rather tries to emphasise the added value of personalised advertising: first, to make advertising more relevant to consumers, second, to make the advertising market much more efficient, and third, given the business models based on personalised advertising, the numerous digital services that can be offered “for free” (i.e. without financial compensation).

The current European regulatory framework does not prohibit personalised advertising (apart from individual exceptions)[8], but forces the actors involved to reduce the risks to such an extent that they are proportionate to the promised added value. However, numerous civil society, scientific and political stakeholders consider this current regulatory framework to be weak or even ineffective in practice. One of the main reasons for the weak implementation of data protection regulations in practice so far is that data protection law is rather complex with its current regulatory approach: in order to effectively contain the risks arising from data processing for personalised advertising, the responsible actors must design their technical-organisational systems accordingly.

[*] All links mentioned below were last accessed on November 7, 2024.

[2] Chen, The Battle for Digital Privacy Is Reshaping the Internet, New York Times, 16.9.2021; Fouad/ Santos/ Laperdrix, The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, PoPETS 2024, p. 450.

[3] Statista Research Department, Digital advertising spending worldwide from 2021 to 2027,

https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/.

[4] Allied Market Search 2020, https://www.alliedmarketresearch.com/internet-advertising-market.

[5] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 18.

[6] ICO, Update report into adtech and real time bidding, 2019, p. 6, 19, 21; ISBA, Programmatic Supply Chain Transparency - Study, May 2020, p. 7, 10.

[7] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 21: “The combined revenue of the largest European publishers has stagnated over the past ten years, while Alphabet and Meta’s revenues increased significantly during the same period”.

[8] See Art. 25 sect. 1 Digital Services Act.

However, this is accompanied by numerous challenges in coordinating the legal, technical and organisational requirements. The objectives, problem understandings, terminologies, processes and methods are fundamentally different at all these levels.

In the case of complex value networks such as the online advertising market, the players seem to be hardly able to successfully provide these coordination efforts. The Transparency and Consent Framework of the International Advertising Bureau Europe (IAB) is a prime example of these coordination challenges. With this framework, a network of thousands of companies is trying to agree on common legal, technical and organisational rules for obtaining informed consent from consumers and, on this basis, for collecting, sharing and processing their personal data for personalised advertising. Since an industry association usually agrees on the lowest common level with such self-regulation and primarily pursues its own economic interests, this framework inevitably falls short of a level that would also take appropriate account of the interests of consumers and society as a whole. But it is not just that companies are unable or unwilling to implement a higher level of protection; they are often also unsure how to do so. This is because an effective implementation is associated with numerous legal, technical and organisational issues that need to be clarified. The principle that a chain is only ever as strong as its weakest link also applies to data value chains. In value chains with over thousand participants, all of whom have to coordinate to provide for effective protection, it is therefore rather likely that the level of protection ultimately achieved will not reach the necessary level.

Contrary to what one might expect, the quasi-monopolistic Big Tech companies currently appear to be the players most likely to achieve a higher level of protection. There are various reasons for this: first of all, it is financially easy for these companies to provide the necessary resources. Secondly, due to the vertical and horizontal integration of the various phases of the value chain, it is far easier for these companies to adapt their technical and organisational system accordingly. On their own end-user interface, these companies can obtain consent themselves, collect the personal data themselves, process the data themselves without having to share it with anyone, and finally play the advertising back on their own interfaces. They don't sell data, they just sell advertising space. Thirdly, companies are increasingly realising that they can also use data protection compliance to further marginalise their competitors. The less data they share, the greater their power. From a consumer protection perspective, this is problematic for two reasons: firstly, this concentration of power leads in the case of already powerful companies (especially in the case of so-called gatekeepers) to less and less competition and thus to a smaller and smaller range of digital products and services for consumers; and secondly, it leads to a concentration of information power, which data protection actually aims to prevent.

Against this background, we propose options for a regulatory framework in this report that, in our view, not only ensures an appropriate level of consumer and data protection in practice, but also, and above all, fair competition (though we only deal with competition-related aspects marginally). In this context, we propose to ban the processing of personal data for personalised advertising in certain cases, whereby we see different options to tailor such a ban (regarding certain types of data and groups of data subjects, certain actors or practices). Of course, the more far-reaching a ban is, the more it eliminates the need for coordination. If the data is not allowed to be processed in the first place, there is no need to set up technical and organisational protection measures to contain the risks. From this point of view, a general ban is not only the most legally effective protection, but also the most economically effective. However, a general ban also contains the risk of foregoing the efficiency gains of personalised advertising. Furthermore, a general ban would be patronising consumers who basically see added value in the personalisation of advertising, provided that it really makes the advertising more relevant to them. That is why we are discussing a general ban more as a fallback regulation should it turn out that the risks cannot be effectively contained due to the excessive coordination efforts, despite our regulatory proposals to reduce these efforts. However, we believe that it is possible to operate personalised advertising in a way that meets the requirements for effective consumer protection and data protection, as well as for fair competition. All that is needed is a more efficient framework.

To this aim, this report will identify 1) the existing risks of personalised advertising - taking into account consumer perceptions, 2) current developments, and 3) the current legal framework. On this basis, we will finally point out the need for alternative regulation. The report aims to outline which regulatory concepts could be considered in order to counter the actual effects and legal problems. The report deals with the regulation regarding the personalisation of advertising, the ecosystem behind it and the actors involved. The focus lies on network-related deficits as such, not on specific large digital firms in particular.[9] Finally, its aim is to highlight the need for complementary and alternative regulation due to the enormous risks and to point out different levels of regulatory options, whereby we approach the topic from a data protection perspective.

2 NEED FOR REGULATION: RISKS OF PERSONALISED ADVERTISING FOR THE FUNDAMENTAL RIGHTS OF DATA SUBJECTS AND FOR SOCIETY AS A WHOLE

To understand the profound and diverse risks posed by online advertising and to counteract them, it is necessary to clarify important parameters of the advertising ecosystem. The first part of this chapter is therefore dedicated to the definition and classification of frequently used terms, followed by an overview of the complex structure of the advertising ecosystems and its actors. The individual risks for users and structural risks for the society resulting from the advertising ecosystem are examined thereafter. Particular attention is paid to users' perception, in particular, how the current implementation of consent does not effectively empower them to protect themselves from the relevant risks. The increasing awareness of these risks and the changing legal framework have led to several technical or organisational developments and initiatives within the last years, all aiming to mitigate risks and enable more control. However, there are also opposing developments that further increase or complicate the risks and call into question the effectiveness of current protection. These developments will be systematically discussed at the end of this chapter.

2.1 DEFINITION AND CLARIFICATION OF TERMS

In this report we (don´t) use the following terms:

[9] For more insights specifically on large digital firms, see Kerber/ Specht-Riemenschneider, Synergies between Data Protection Law and Competition Law, 2021.

- **(End)user, consumer or data subject**: every natural person who is addressed by advertisements and affected by the associated processes - on a practical level it means everyone using the internet.
- **Digital services:** the entirety of online channels through which digital advertising is generally displayed, like websites, apps, social media platforms (hereinafter also shortened referred to as: website).
- **Online advertising or digital advertising**: includes all channels of advertising that are placed and distributed over the internet, like
    - **Search advertising:** sponsored entries which appear within a list of search results on a search engine website, typically labelled as ads or sponsored content, typically delivered to users based on keywords associated with their individual searches;[10] this kind of advertising is not within the scope of this report;
    - **EMail marketing**: sending commercial messages, typically to a group of people, via emails; this kind of advertising is not within the scope of this report;
    - **Social media advertising**: typically either takes the form of in-feed ads (which blend in with content on the platform), display banner ads or video ads (e.g. before a video begins) placed on social media websites or apps;
    - **Display advertising**: typically takes the form of display banner ads or video ads, provided within digital services (other than social media and search engines)
- **Personalised advertising**: to describe the processes within the online advertising ecosystem, terms such as behavioural advertising[11], targeted advertising[12] or tracking and profiling[13] are widely used. The terms describe different phases of the processing of personal data for the purposes of personalised or targeted advertising. A differentiation of the phases is useful for this report as it allows to identify different risks and thus also different protection requirements caused by each of them. However, in general, we use "personalised advertising" as a generic term to cover all steps and methods, the purpose of which is to display users a personalised ad; this includes sub-processes like
    - **(Web) tracking**: technical process independent from a purpose or method to collect data points over multiple different digital services and devices, which can be linked to individual users usually via a unique

[10] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 16.

[11] Art. 29 Working Party, Opinion 2/2010 on online behavioural advertising, p. 4: "Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests".

[12] Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, p. 4; Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 243, 244: "Targeted advertising could be defined *as a* commercial practice that uses data referring to individuals to select and display ads or other forms of commercial content for marketing purposes, based on the data subject's characteristics linked to said data which provides information about their digital behaviour".

[13] Verbraucherzentrale Bundesverbrand e.V., press release, 24.05.2024, https://www.vzbv.de/en/online-data-protection-majority-consumers-reject-personalised-advertising.

user identifier (ID); includes logins, third-party cookies, (tracking) pixel, browser fingerprinting and ID synchronisation; most widespread technology to follow the same user on different digital services and devices, collect and process personal data in order to place personalised advertisement[14]; only covers the observation as one part of personalised advertising but not the subsequent step of displaying the advertising and therefore not the actual influencing process.

    - **Retargeting**: process to re-identify a user across browsers and devices based on a specific event, e.g. if a consumer has clicked on an advertisement or even filled a shopping basket without clicking on the purchase button, retargeting aims to persuade this consumer to complete the purchase process over a certain period of time, regardless of where they are on the internet; based on retargeting, the consumer is therefore shown adverts for products or services related to the triggering event over a certain period of time and in various digital services that may be connected with the retargeting system.

    - **Profiling-based personalisation**: based on interest profiles, which are created by observing a user's behaviour over a certain period of time; the advertising industry creates these profiles by observing which websites users visit, which content they click on, how long they use them, what they ultimately buy, which other people they interact with, etc; the information can be used to draw conclusions about the user's interests, attitudes, characteristics and, of course, possible future behaviour.

    - **Cohort-based personalisation**: separates the phases of data collection and analysis on the one hand and the attribution of the generated buying interests to specific consumers on the other, affecting two basically different groups of data subjects.

    - **Contextual advertising**: Contextual advertising can either be displayed without the use of personal identifiers or with them.[15] As long as personal identifiers are used, we continue to assume a form of personalised advertising, albeit a very weak one.

- **(Online) advertising ecosystem, advertising market, advertising network or advertising industry**: the entirety of all parties involved in the delivery of online advertising, including website and app operators, advertisers, intermediaries, platform operators, browser operators, agencies and other service providers as outlined below in more detail in the following chapter 2.2.

    - **Publisher**: Entity that receives revenue from selling advertising space (so-called **inventory**) within the digital services that they own;[16] publishers may use a marketer service.

[14] Jha/ Trevisan/ Leonardi/ Mellia, On the Robustness of Topics API to a Re-Identification Attack, PoPETs 2023, p. 66.

[15] EDPB, Reply to the Commission’s Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, 13.12.2023, p. 5, https://www.edpb.europa.eu/system/files/2023-12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf.

[16] Examples of large publishers, especially in the EU are Alphabet and Meta, RTL Group, Canal+, ProSiebenSat.1 Media, Axel Springer, Hubert Burda Media, Mediaset, RAI, Bauer Media Group, TF1 Group, Ströer, Schibsted Media Group and PRISA.

- **Advertiser:** Entity that buys ad space from a publisher in order to display ads for their products or services;[17] advertisers may use an agency service and/or a purchasing service.

2.2 STRUCTURE AND ACTORS OF THE ONLINE ADVERTISING ECOSYSTEM

In order to find regulatory approaches that more effectively counter the systemic risks, it is crucial to break down the complex structure of the online advertising market into individual players within the network, their relationship to each other and towards users.

2.2.1 Development of the online advertising ecosystem

When online advertising came up in 1994[18] processes were straightforward and the players involved could be counted on one hand. Advertisers bought inventory for a fixed amount of impressions at a fixed price from publishers (sometimes via agencies).[19] This simple two-party-system subsequently spread into various directions and dimensions and turned into a brand new market with a network of hundreds of actors.

To begin with, so-called advertising networks emerged as a way for advertisers to buy ad space from a group of publishers, rather than dealing with each one of them individually. Since the beginning of the 2000s, furthermore the carriers of advertising messages continuously expanded, with not only banners but also small display ads between website content, pop-ups or sponsored links being discovered as potential advertising space.[20]

Until then, advertising was not very targeted and therefore accompanied by a high level of scatter loss. With online advertising it suddenly became possible to take a new approach by addressing specific terminal devices or browsers and thus customers individually. Likewise the functionality of the internet established a direct feedback channel from the user to the provider. This channel opened up the possibility to capture user reactions or to comprehensively track and observe the user's behaviour on a website and beyond, through large parts of the internet, without the user being aware of it. Therefore, it became possible to kind of get to know the individual user behind the terminal device or browser, at least with a certain degree of probability, and to collect information about the user's characteristics, interests and intentions. The online advertising industry quickly realised that the profile of the individual user could not only be very detailed depending on the activities tracked, but used to address advertising only to those users who had certain characteristics, interests and intentions.

The option of tracking the individual's reaction to an ad likewise changed the billing models used. Whereas the number of potential consumers reached by an ad placement was the basis for billing by then, prices were subsequently calculated depending on the user's reaction to the advertisement. The metrics used to measure

[17] E.g. Procter & Gamble, Unilever, L’Oréal, Amazon, Nestlé, Volkswagen, Renault–Nissan–Mitsubishi Alliance, Stellantis, General Motors Company, Reckitt Benckiser Group.

[18] The US telecommunications company AT&T allegedly placed the world's first clickable advertising banner on the website “HotWired” (now “Wired”) on 27.10.1994, https://www.wired.com/2010/10/1027hotwired-banner-ads/.

[19] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 18.

[20] On market developments see Bundeskartellamt, Sektoruntersuchung Online-Werbung, Diskussionsbericht, August 2022, para. 15 et seq.

the success of online advertising include impressions, reach, engagement rate, click-through rate and conversion rate. Impressions refer to the total number of views of an advertisement, while reach represents the unique number of people who have seen it. The engagement rate is the percentage of sessions with interactions on an advertisement. The click-through-rate is the number of clicks that an advertisement receives divided by the number of times that advertisement is shown. Finally, the conversion rate is the number of transactions (purchases) made in relation to the number of times the advertisement is shown.[21] What all metrics have in common is that they require the observation of individual consumers, even if this data can then be aggregated across individuals in a later step.

2.2.2 Programmatic Advertising and Real Time Bidding

The new spectrum of possibilities as well as facilitation led to an increasing number of publishers selling ad space online. Since 2010 so-called **Programmatic Advertising** began to revolutionise this market by making it possible to buy and sell digital ad space across multiple websites and publishers in an automated way in real time. The new technology promised advertisers to reach new audiences, increase the speed at which an advertisement reaches its audience and reduce the costs, inefficiencies and limitations of traditional systems that relied on human ad buyers and salespeople.[22] Programmatic Advertising shall enable publishers to increase revenue by increasing the value of individual advertising space sold and sell space that would otherwise not be sold. At the same time, more and more intermediaries came onto the scene to make money through providing services to others in the ecosystem, such as agencies and management platforms.[23]

With programmatic advertising, publishers are able to individualise their inventory via an auction process in which the highest bidder is allowed to place its advertising. The transaction usually only takes a few fractions of a second and is known as **Real Time Bidding (RTB)**. The collection and sharing of data across different market participants gathered within RTB is facilitated by technical specifications called protocols that delineate exactly what data is shared between parties in a transaction and how the data sharing takes place. From 2025 on **OpenRTB**[24] will be the decisive protocol across the market.[25]

The automation is made possible by two key additional layers in the system consisting of a supply or sell side and a demand or buyer side.[26] The supply side acts as a representative of the publisher, while the demand side platform acts as a representative of the advertiser. Publishers use a **supply side platform (SSP)** to sell their inventory by placing advertising space on such a platform. In addition to technical details about the advertising space, the publisher can define a minimum price level and rules for

[21] See for example, Kočišová/ Štarchoň, The role of marketing metrics in social media: A comprehensive analysis, MS&I 2023.

[22] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 18.

[23] ICO, Update report into adtech and real time bidding, 2019, p. 8.

[24] IAB Tech Lab, Open RTB - Real-Time Bidding, https://iabtechlab.com/standards/openrtb/.

[25] Google announced to migrate from Google Authorized Buyers protocol to the OpenRTB protocol on 2.5.2025 to align more closely with industry standards, https://support.google.com/authorizedbuyers/answer/14745711?hl=en.

[26] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 19.

permissible advertising. The SSP bundles the offers of a large number of providers, making millions, if not billions, of possible advertising impressions available.

A **demand side platform (DSP)** is the counterpart to the SSP on the advertiser side. The advertiser (or an agency contracted by the advertiser) places a request for an advertising space on a DSP and defines, among other things, maximum bids, budget caps, target group parameters and target of the campaign. As with SSPs[27] there are a number of different DSP[28] providers. They differ depending on the number of customers they represent and the technology they use to execute the purchase (their infrastructure, bidding and optimization models).

When a user visits a website, an impression is created on the publisher's website. While the page loads, the SSP offers the advertising space for an auction by incorporating the information collected about the user in a **bid request** and sending it to the DSP.[29] The information in a bid request can vary but usually include the following:[30]

- details about the publishers website and referring sites (where the user came from), which shows, what users are reading or watching,
- the user's IP address (possibly with the final set of numbers removed),
- a unique identifier for the bid request,
- cookie IDs,
- user IDs,
- a user-agent string identifying the user's browser and device type, to which the impression will be delivered (desktop/mobile, brand, model, operating system, language settings, hashed MAC address etc.),
- the user's location (postal code),
- the user's time zone,
- the user´s year of birth, gender, income, family status and further demographic data, if known,
- the user’s site behaviour/ user journey (contextual and thematic preferences to certain topics and pages, interactions such as mouse cursor movement, scrolling, downloads, transitions to other pages through clicking on advertisements and links, search queries),
- information relating to the audience segmentation[31] of the user, if available.

The bid request is transmitted to the DSP so that advertisers can bid for the opportunity to insert their ad into the respective ad space on the publisher's service. It's no surprise that more detailed bid requests are deemed to be more attractive, either because they bring in higher revenue or because they are intended to enable more accurate targeting of adverts to individuals, or both.[32]

The DSP then receives the user profile and the traded advertising space, which is evaluated in a fraction of a second, to determine whether the user profile meets the

[27] For example Google (AdX), Teads, Xandr-AppNexus, Magnite-Rubicon, Smart AdServer, Rich Audience, Verizon, SpotX, OpenX).

[28] For example Google (DV360), The Trade Desk, Amazon, Adobe, Criteo, Xandr-AppNexus, MediaMath, Verizon.

[29] Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, p. 10 et seq.

[30] For more details see Ryan, Report - Behavioural advertising and personal data, 2018, Appendix 1, p. 12.

[31] See IAB, Data Segments & Techniques Lexicon, p. 4,

https://www.iab.com/wp-content/uploads/2016/01/IAB-Data-Lexicon-Update-2016.pdf.

[32] Becker, Consent Management Platforms and Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung, CR 2021, recital 22; ICO, Update report into adtech and real time bidding, 20.6.2019, p. 11.

existing parameters of the desired target group. Depending on the degree of fulfilment, the advertiser (automatically) submits a lower or higher bid via the DSP. The SSP, as a technical interface, collects the bids. The highest bid wins and is passed on to the publisher.

The (virtual) marketplace between SSP and DSP is called **AdExchange**. Such trading floors might be offered as a separate service, but the functions of ad exchanges are largely undertaken by SSPs today.[33] The scenario can be complicated by the fact that the levels of trade are multiplied by adding further AdExchanges.

Since the purchase of online advertising space today is in many cases not based (solely) on the environment of the inventory, but rather on what is known about the user who is visiting the website and will see the ad, personal data about the user plays an enormous role. Thus, publishers not only provide information about the advertising space to SSPs, but all they know about the user who will see the ad. Via the SSP this information will be forwarded to the advertising demand side, which tries to use this information to determine the user's fit with the target group it is addressing for the advertiser. Furthermore, in case the advertisers' demand side is able to at least identify the user pseudonymously, they can attempt to combine the information provided by the publisher with their own information about the user and thus gain a more accurate picture. **Data management platforms (DMP)**[34] are used to support these processes by managing user data from different sources. DMPs allow advertisers, DSPs, SSPs and publishers to analyse, categorise and collate incoming (mostly personal) data from multiple online and offline sources, combine it with (mostly personal) data provided by third parties, and create audiences, a process known as 'data matching' or 'enrichment'.[35] Advertisers may also match data they have about individual consumers with the data being shared by publishers in order to target (or exclude) specific users with (or from) advertising. Some DMPs integrate data from other second and third-party sources, such as data brokers, and make this data available to other platforms, including DSPs, SSPs and AdExchanges.[36] In some cases the functions of the DMP are already integrated into the SSPs or DSPs.[37]

Once the inventory has been sold, the advertising material still has to be displayed. In principle it would be possible to use a publisher's server, however, in practice, another actor is connected in between: to deliver the advertising material a third-party **Ad server** is used - both by publishers and by advertisers. In addition to delivering advertising material, Ad servers can also perform tasks on the publisher side by optimising the utilisation of advertising space, and on the advertiser side by tracking impressions delivered and the performance of ads as well as managing and optimising advertising campaigns. Ad servers therefore may collect further data generated during the delivery of the advertising material.[38]

[33] Bundeskartellamt, Sektoruntersuchung Online-Werbung, Diskussionsbericht, August 2022, recital 29.

[34] The best-known example is probably the company Cambridge Analytica; other examples are the Adex (Virtual Minds), Mapp, eXelate (by Nielsen), Adform, the Tradedesk, Oracle DMP (BlueKai), Salesforce and Adobe Audience Manager (Demdex).

[35] ICO, Update report into adtech and real time bidding, 2019, p. 11.

[36] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 33.

[37] Bundeskartellamt, Sektoruntersuchung Online-Werbung, Diskussionsbericht, August 2022, para. 31.

[38] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 33.

The collection of the user's information, the creation of the bid request, the auctioning, bidding and securing of the advertising space, subsequent presentation of the advert to the individual, up to performance measurement all take place in milliseconds[39] while the website is loading.

All of the above actors may operate across the ecosystem. A publisher may offer inventory on the website of its online newspaper and at the same time place ads for its own online newspaper on a social media platform. A SSP may likewise offer AdExchange and DSP services.[40]

The core business of today´s online advertising system therefore involves multiple categories of actors at different levels, with each category forming its own market in which hundreds of companies are active. Using programmatic advertising with its RTB system moreover means millions of bid requests are automatically processed every second, leading to a vast quantity of personal data leveraging from multiple data sources is shared throughout an ecosystem.[41]

2.2.3 Elements and extent of user behaviour targeting

The lifecycle of personalising ads includes

- **monitoring** user activities **across** different digital services from various players over time,
- **gathering** information and **analysing** it for the purpose of creating and developing users' **profiles**,
- in certain cases **aggregating** the information with **offline data** or data **actively provided** by the user (e.g. when they create an account online or when they log-in on a website)[42],
- **sharing** that personal data with third parties,
- **inferring** information about the user and draw conclusions on their preferences, tastes and interests,[43]
- **displaying** ads personalised on the basis of the resulting profile and finally
- analysing the users' **interaction** with the shown ad based on their profile.[44]

Schematically the system can be presented as follows:[45]

[39] Google, Authorized Buyers overview: 'This all happens within 100 milliseconds, or in real time.', https://support.google.com/authorizedbuyers/answer/6138000.

[40] Becker, Consent Management Platforms and Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung, CR 2021, recital 19 with reference to AppNexus, now known as Xandr.

[41] ICCL, The Biggest Data Breach, 2022, p.1: "RTB [...] tracks and shares what people view online and their real-world location 294 billion times in the U.S. and 197 billion times in Europe every day".

[42] Eberl, Tracking durch Identitätsprovider, Kuketz-Blog, 5.12.2021: Use of hashed email addresses.

[43] Art. 29 Working Party, Opinion 2/2010 on online behavioural advertising, p. 7: "There are two main approaches to building user profiles: i) Predictive profiles are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. ii) Explicit profiles are created from personal data that data subjects themselves provide to a web service, such as by registering. Both approaches can be combined. Additionally, predictive profiles may be made explicit at a later time, when a data subject creates login credentials for a website".

[44] EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, para. 20.

[45] Veale/ Zuiderveen Borgesius, Adtech and Real-Time Bidding under European Data Protection Law, German Law Journal 2022, p. 232.

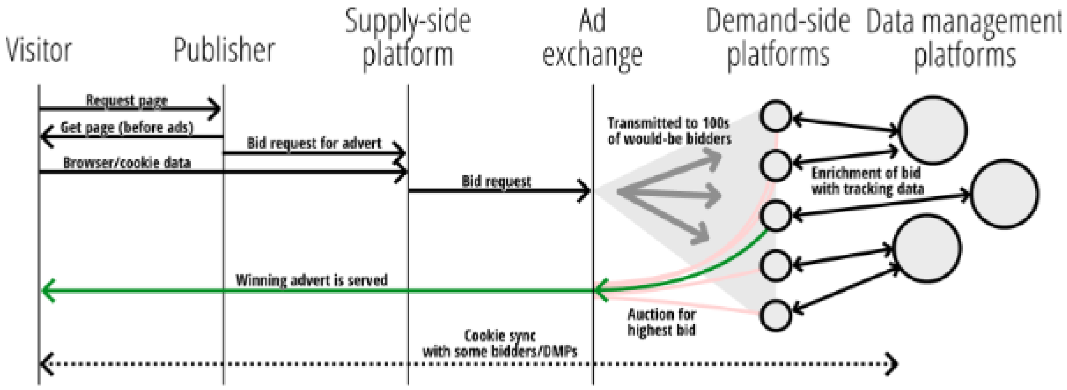


Figure 1: Scheme of the system

The observation of user activities can take place stateful, meaning the user browser saves an identifier locally which can be retrieved at a later time, or stateless, where information about the browser and/or network is used to create a unique fingerprint.[46]

When using **stateful tracking** a user is typically identified by a HTTP cookie in form of a small piece of data, which is sent from the website's or a third party server and stored in the user's browser the first time the user visits a website. Every time the user loads that website again, the browser sends the cookie back to the server to identify the user.[47] Over time, the cookie is enriched with information, ranging from simply recording the type of the browser accessing a particular page, over the setting of a unique identifier (UID) within the cookie, to remember the status of an individual user, including shopping items added in the cart of an online shop or the user's previous browsing activities, including dwell time and mouse movements. Other stateful methods include the JavaScript localStorage API, which enables Javascript code to save data in the user's browser.[48]

Because of a browser security feature called same-origin policy cookies are tied to a specific domain. In consequence every DSP, DMP, SSP and AdExchange in the advertising ecosystem has to build up their own UID system by inserting their code snippet under their own domain name to the HTML code of a publisher's website. So far, this would mean actors within the advertising market only have a local view of their users, since all participants use different ID systems that can´t be connected across domains.

To enable the actors to link separate IDs given to the same user and hence be able to identify users across the entire internet, a technique called **cookie syncing**, also known as cookie matching or mapping, was established. Cookie syncing is commonly achieved by employing HTTP 302 Redirect protocol to make a website available under more than one URL address. The process begins when a user visits a website which includes a code snippet from a third-party in its HTML code.[49] Even though the pixel tag

[46] Karaj/ Macbeth/ Berson/ Pujol, WhoTracks.Me: Shedding light on the opaque world of online tracking, Computers and Society 2019, p. 3.

[47] Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, pp. 11 et seq.

[48] Karaj/ Macbeth/ Berson/ Pujol, WhoTracks.Me: Shedding light on the opaque world of online tracking, Computers and Society 2019, p. 3.

[49] The code is commonly implemented through an embedded 1x1 image, known as pixel tags, 1x1 pixels or web bugs, Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, pp. 13 et seq.

is virtually invisible, it is served just like any other image online. The difference is the website is served from its own domain while the image is served from the tracker's domain. This allows the tracker to read and record the cookie's unique ID and the extended information it needs. The trick of cookie sync using a pixel is that, instead of returning the required 1x1 pixel immediately, one service redirects the browser to another service to retrieve the pixel. During the redirect process, the two services exchange the information and sync the user's ID.[50]

Since users are able to delete cookies by clearing the browser's cache or choose to disable cookies completely in their browser settings, there is at least some ability to accommodate or restrict tracking. **Stateless tracking** on the other hand combines certain hardware attributes information via browser APIs and network information, which on their own may not be unique, but when combined, create a unique and persistent identifier (called fingerprint). This renders it possible to identify a particular browser on a particular device.[51] It differs from stateful methods in that this value is a product of the host system, rather than a saved state, and therefore cannot be deleted or cleared by the user, meaning that fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off.

At this point, it should be made clear that the cookie syncing process described above does not have to be limited to cookies, but can be applied to all stateful and stateless identifiers. **Retargeting**, for example, is about recognising individual users across as many devices, browsers and services as possible in order to remind or persuade them to complete a purchase that has been started but not yet completed. For this purpose, it makes sense to collect as many identifiers as possible about a person (from logins, device IDs, email addresses, IP and network addresses to cookies and fingerprints) so that they can be recognised as one and the same person based on these **bundled identifiers**.

What then happens to the data once it has been collected from the user by one of the aforementioned methods is unfathomable. Basically, there are two methods being used: On the one hand, advertising services generate **profiles** by collecting information about the historical behaviour, certain characteristics and possible interests, but also views, opinions, etc. of individual consumers. This information can either result from direct information provided by the consumer (for example, if they have indicated their age in a registration form) or it is based on inferences from the data entered or observed. There is also a second method used to generate inferences from data. In **cohort-based advertising**, advertising services aggregate the data about individual consumers across into statistical cohorts. Cohorts describe groups of consumers who share certain statistical characteristics (for example, men between 20 and 40 who have a high income and live in Berlin's Prenzlauer Berg neighbourhood like to drink latte macchiato). If a publisher finds that users of its website have these characteristics (i.e. male between 20 and 40 years old with an upper income and living in Berlin's Prenzlauer Berg district), advertising services assign these statistically determined interest to this person (i.e. that this person probably also likes to drink latte macchiato) and displays the corresponding adverts to them. In practice, both methods are also combined.

[50] Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, p. 14.

[51] Karaj/ Macbeth/ Berson/ Pujol, WhoTracks.Me: Shedding light on the opaque world of online tracking, Computers and Society 2019, p. 3: The method will usually require code execution, either via JavaScript or Flash, which is enabled to gather the data from APIs which provide device attributes like the device resolution, browser window size, installed fonts and plugins. Typically, information about the hardware type, installed software, the MAC address and the IP-address is also combined. More advanced methods leverage observations of the ways different hardware render HTML Canvas data or manipulate audio data in order to generate fingerprints.

This type of data collection can take on very large proportions. Among other things, the collected data is used to derive characteristics and summarise them in so-called **Audience Segments**, into which users are sorted accordingly. The extent to which this takes place was illustrated by a team of journalists in 2023.[52] They had come across a document on the internet which contained a list of more than 650,000 different categories into which users are categorised in order to target them more effectively with advertising. This included segments like "FR - Browser Language – Arabic", "Top Spending Geography – Casino and Gambling Activities", "Viagra – Unhealthy Place Visits", "Generation - Millennial $60K + Income", "DE - Demography - Conservative Retiree" or "Heavy buyer - wine and sparkling wine".

The document originates from the data management platform Xandr, a company owned by Microsoft (formerly known as AppNexus), that acts on several positions within the ecosystem, including SSP, DSP, AdExchange and cookie sync services. The non-governmental organisation NOYB has filed a complaint with the Italian data protection authority in July 2024 inter alia regarding the inadequacy and inaccuracy of this vast amount of categorisation.[53]

However, as already explained above in the definition of terms, online advertising does not necessarily have to take on such proportions. It is also possible, for example, not to display advertising based on the individual characteristics of the consumer, but primarily based on the content that a consumer is currently using. This so-called **contextual advertising** can also still require identifiers referring to an individual consumer, but the extent of the insights into their private life is considerably less than with the other types mentioned. What all types of advertising have in common, however, is that the **measurement of** their **success** always requires, at least initially, the observation of the behaviour of individual consumers. Of course, this observation data can be aggregated into cross-user statistics in further process steps (see also chapter 2.1).

2.2.4 IAB Transparency & Consent Framework

With the aim to promote compliance with the GDPR when the above-mentioned actors use the OpenRTB protocol, the International Advertising Bureau Europe (IAB) developed in 2018 the so-called Transparency & Consent Framework (TCF).[54] IAB Europe based in Brussels is part of the Interactive Advertising Bureau Inc (IAB Inc), an international association for the online advertising industry headquartered in NYC. The organisation represents the interests of 700 companies in the digital advertising and media industry.[55] In short, the TCF addresses the governance problem that only the publisher, due to its direct end-customer interface, is able to obtain the informed consent of the end user, but this consent may have to form the legal basis for all data processing steps of the entire network. The TCF solves this problem by providing a

[52] Dachwitz, Microsofts Datenmarktplatz Xandr: Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert, Netzpolitik, 8.6.2023.

[53] NOYB, complaint no. C-084, 9.7.2024 https://noyb.eu/sites/default/files/2024-07/Xandr%20Complaint-EN_redacted.pdf.

[54] According to its own policy IAB Europe is defined as "the entity that manages and governs the Framework", https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/.

[55] IAB Inc has 45 international sub-organisations under its umbrella of which IAB Europe takes care of those based in the EU, https://www.iab.com/our-story/. The members of IAB Europe are undertakings in the online advertising and marketing sector, which, in turn, have undertakings in that sector as members. The members of IAB Europe include, inter alia, undertakings which generate significant income through the sale of advertising space on websites or applications.

common standard with technical, organisational and legal requirements for obtaining and sharing consent among the actors.

2.2.4.1 Participants and components of the TCF

The TCF standard is not to be confused with the OpenRTB protocol developed by the IAB Technology Laboratory (IAB Tech Lab)[56], which is an instant and automated online auction system of user profiles for the purpose of selling and purchasing advertising space on the internet (see above chapter 2.2.2).[57] While OpenRTB concerns the end-to-end lifecycle of the advertising delivery process (taking place inside the system), the TCF was presented as a solution capable of bringing the auction system into conformity with the GDPR vis-a-vis the user. According to IAB Europe the TCF shall be used as a “cross-industry voluntary standard that is intended to enable publishers of websites and apps (first parties) and technology partners that support the delivery, personalisation or measurement of advertising and content (third parties or vendors) to work together and provide users with a standardised experience when they make privacy choices”.[58] The TCF thus plays a role in the operation of the OpenRTB protocol, since it shall make it legally possible to transcribe the user’s privacy preferences in order to communicate them to potential advertisers and digital advertising services.[59]

In case publishers want to make use of the TCF to organise their communication with users of their website on the one hand and the advertising ecosystem on the other hand, they often involve another actor, namely the provider of a **consent management platform (CMP).**[60] A CMP is a service provider who implements, on behalf of the website, a banner or pop-up on the website in order to ask users for their consent inter alia regarding personalised advertising.

Besides the visual “cookie banner” element, CMPs also enable a technical connection to the advertising ecosystem via an Application Programming Interface (API) in order to exchange information about the users privacy choices with all service providers in the delivery chain, like Ad server, DSPs, DMPs and SSPs (collectively called **Vendors** in the context of TCF). For these communication processes between publishers, vendors and users, the TCF creates a framework of rules consisting of uniform guidelines, organisational instructions, technical specifications, protocols and contractual obligations that enable publishers and actors of the advertising ecosystem to communicate the user's choices regarding specific processing purposes (see in the next sub-chapter).

Every operator of a CMP and every vendor that wants to participate in the TCF has to complete a registration and certification process first, during which they need to commit

[56] According to the organisation's information it is a non-profit consortium founded in 2014 that involves a global community of members in order to develop fundamental technologies and standards that enable growth and trust in the digital media ecosystem, https://iabtechlab.com/.

[57] The Belgian data protection authority had to deal with the question of controllership regarding TCF and OpenRTB. The authority came to the conclusion that the OpenRTB is a standard whose use does not require the processing of personal data. However, organisations that use the standard can process personal data, whereby the participants themselves determine the purposes and means of the processing. Consequently, the participants are controllers in this context while IAB Tech Lab just acts as a "supplier" of the OpenRTB standard, APD, 2.2.2022, DOS-2019-01377, para. 46, https://www.edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf

[58] https://iabeurope.eu/transparency-consent-framework/.

[59] ECJ, 7.3.2024, C-604/22, para. 26 - IAB Europe.

[60] Becker, Consent Management Platforms und Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung, CR 2021, para. 5.

themselves to the TCF “Terms and Conditions”[61] as well as the “TCF Policies”.[62] The policy is divided into five chapters and two appendices, which describe the participants, obligations, permitted purposes (Appendix A) and the design of cookie banners and other setting options (Appendix B). On the other hand, participants need to fulfil technical requirements laid down in “Transparency and Consent (TC) String with Global Vendor List Format” and “The Consent Management Platform API” that facilitates the recording of users’ privacy preferences by means of the CMP.[63] Those preferences are subsequently encoded and stored in a standardised signalling code composed of a combination of letters and characters referred to by IAB Europe as the **TC String**. For each of the processing purposes that IAB Europe has conclusively defined, the TC String contains information as to whether the website visitor has given consent or explicitly opted out with regard to a specific vendor. The TC String therefore serves as a central means of communication within the TCF and is shared with all vendors participating in the OpenRTB protocol. Usually the website or, on behalf of it, the CMP sets a cookie on the user’s browser after the user has made a selection within the banner.[64]

2.2.4.2 Defined purposes, features and limitations

Versions 1.1 to 2.1 of the TCF were published between April 2018 and August 2020 and have been replaced by version 2.2, which was introduced in May 2023. Appendix A of the TCF 2.2 policy defines the following purposes:

- Purpose 1: Store and/or access information on a device
- Purpose 2: Use limited data to select advertising
- Purpose 3: Create profiles for personalised advertising
- Purpose 4: Use profiles to select personalised advertising
- Purpose 5: Create profiles to personalise content
- Purpose 6: Use profiles to select personalised content
- Purpose 7: Measure advertising performance
- Purpose 8: Measure content performance
- Purpose 9: Understand audiences through statistics or combinations of data from different sources
- Purpose 10: Develop and improve services
- Purpose 11: Use limited data to select content

- Special Purpose 1: Ensure security, prevent and detect fraud, and fix errors
- Special Purpose 2: Deliver and present advertising and content
- Special Purpose 3: Save and communicate privacy choices

- Feature 1: Match and combine data from other data sources
- Feature 2: Link different devices
- Feature 3: Identify devices based on information transmitted automatically

- Special Feature 1: Use precise geolocation data
- Special Feature 2: Actively scan device characteristics for identification

[61] Currently dated April 2023, https://iabeurope.eu/wp-content/uploads/IABEurope_TransparencyConsentFramework_TermsConditions.pdf.

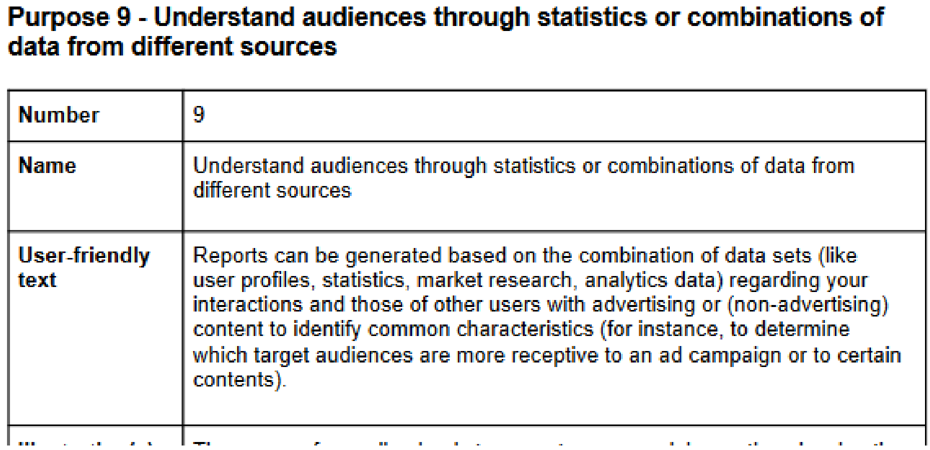
[62] The current Version 2024-06-3.5.0 has 77 pages, https://iabeurope.eu/transparency-consent-framework-file/TCF%20Policies%20-%20TransparencyConsentFramework_Policies_Version%202024-06-3.5.0.pdf.

[63] https://iabeurope.eu/tcf-supporting-resources/.

[64] ECJ, 7.3.2024, C-604/22, para. 25 - IAB Europe: When they are combined, the TC String and this cookie can be linked to a user’s IP address.

It should be emphasised that TCF version 2.2 does not contain any specifications for the situation where websites or other digital services are aimed at children and young people or process special categories of data. Furthermore TCF version 2.2 does not take into account any national implementation of the ePrivacy Directive.

Within its policy the IAB Europe accompanies every purpose with an information text that publishers need to use within the CMP on their website - neither changing the defined purposes nor the wording is allowed. However, since the introduction of TCF 2.0, it has been possible to bundle purposes. The following is an excerpt from the current policy regarding purpose 9:



Purpose 9 - Understand audiences through statistics or combinations of data from different sources

Number	9
Name	Understand audiences through statistics or combinations of data from different sources
User-friendly text	Reports can be generated based on the combination of data sets (like user profiles, statistics, market research, analytics data) regarding your interactions and those of other users with advertising or (non-advertising) content to identify common characteristics (for instance, to determine which target audiences are more receptive to an ad campaign or to certain contents).

Figure 2: IAB TCF Purpose 9

Apart from the requirements mentioned, the TCF does not provide any further specifications regarding the specific design of informed consent. In principle, a publisher is free to decide how to design a cookie banner and whether to rely on a CMP. However, due to a lack of appropriate resources, the vast majority of publishers rely on standard consent banner designs, as offered by CMPs. Regularly such standard solutions offered by CMP providers contain limited design and configuration options since these providers need to fulfil IAB Europe's registration requirements in order to be competitive.[65] However, the user interface of a CMP (e.g. colour, size, labelling and functionality of buttons) is only partially part of the TCF; these factors can therefore at least partly be determined by providers of CMPs or publishers themselves.[66] This also applies to the textual and visual information shown across the different visual layers of a cookie-banner and the question of how to design the consent and reject-buttons.

During their registration process, vendors have to disclose the purposes they intend to rely on for data processing. After their verification with IAB Europe, vendors receive an ID and are included in a global vendor list.[67] Even though the TCF defines numerous technical, organisational and legal requirements for the collection and sharing of informed consent between the actors, it does not clarify the legal relationship between them, in particular whether they are controllers, joint controllers or processors in terms

[65] The list of currently certified website-CMPs includes 104 entries,https://iabeurope.eu/cmp-list/.

[66] Halank/ Koglin, Datenschutzberater 2020, p. 93.

[67] The list currently comprises 865 entries, https://iabeurope.eu/vendor-list-tcf/. Only very few advertising technology providers are not registered with TCF 2.2 by now, inter alia captcha technologies and the “VG Wort Zählpixel”, a tracking pixel which is used to count views of text documents for the purpose of remunerating authors of electronically published documents.

of data protection law. In particular, vendors are regularly only referred to as "partners" within cookie banners or data protection information.

2.2.4.3 Governance aspects

In this context, it should also be made clear that the TCF is a form of self-regulation. Unlike direct state regulation or co-regulation, the TCF is therefore a purely privately initiated and organised standard. The fact that the private players have created this standard in order to comply with data protection requirements does not affect the character of self-regulation.[68] This clarification is important because the TCF is primarily pursuing its own economic interests and not the interests of consumers or society as a whole. Accordingly, no representatives of consumer or societal interests (such as consumer protection or data protection authorities) were or are involved in the standardisation process.

In relation to the one-sided representation of industry interests, there is another important governance aspect that is worth being emphasised here. Since self-regulation primarily pursues its own interests, the more stakeholders that are involved in it, the more business-friendly the level of protection will be. This is because the more stakeholders that are involved, the more likely it is that one of them will have an interest in further reducing a particular legal, technical or organisational requirement in their favour. For governance reasons, the result is then the lowest common level of protection. In addition, the advertising industry organised through the IAB not only do not want to implement a higher level of protection or, for governance reasons, are unable to do so, but often do not even know how to do it. The purposes described above are a vivid example of this. How purposes must be formulated in concrete terms so that they are sufficiently specific – as required by Art. 5 sect. 1 lit. b GDPR (see chapter 3.1.2.1.) – was one of the best kept secrets of data protection law for almost 60 years.[69] There are numerous other questions regarding the interpretation of certain legal norms of data protection law and their technical and organisational implementation.[70] These uncertainties, combined with the one-sided representation of interests and the aforementioned governance mechanisms, result in a level of protection that does not effectively protect against the risks for consumers and the society as a whole.

The very nature of self-regulation also explains other characteristics of the TCF. For example, the IAB Europe's terms and policies are only contractual agreements binding on a civil law basis. Further, no technical measures are in place that prevent actors within the advertising ecosystem from processing user data.[71] As soon as access to user data has been opened and this data has entered the system, it will be released to an excessive number of companies. Even though IABs policy says a “Vendor must not transmit a user’s personal data to an entity outside of the Framework unless it has a justified basis for relying on that entity’s having a Legal Basis for processing the

[68] Voßkuhle/ Eifert/ Möllers, Grundlagen des Verwaltungsrechts, para. 144 et seq.

[69] See already Benda, Privatsphäre und Persönlichkeitsprofil, 1974, p. 27; more recently Nissenbaum, Respect for Context as a Benchmark for privacy online: what it is and isn’t, 2015, p. 291; summing up the debate until 2018 v. Grafenstein, The Principle of Purpose Limitation in Data Protection Law, 2018.

[70] V. Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I., EDPL 2020, pp. 509 et seq.

[71] Ryan, Report - Behavioural advertising and personal data, 2018, p. 6: “trust everyone” approach.

personal data in question",[72] from a technical point of view nothing stands in the way of data processing, rather civil law agreements.[73]

2.2.5 Influence and potential of (generative) AI within the advertising ecosystem

Programmatic advertising and the advertising market around it is facing a revolution by the use of artificial intelligence (AI).[74] Actors from across the entire advertising ecosystem are utilising AI, at least to a certain degree and in various ways, to optimise and manage RTB or create content, improve operational efficiencies and optimise campaigns.[75] Basically almost every online ad already today relies on AI to reach the users eyes and ears in real-time.[76] Strictly speaking, this new era began already around ten years ago, but is raised to a whole new level by the use of so-called generative AI, meaning a technology that creates new content, including text, images, audio or video, when prompted by a user.[77]

Inter alia advertisers can use generative AI to create multiple ad variations and formats (e.g. different designs and sizes) automatically and simultaneously.[78] Thus advertisers are able to generate more content for the same or less money and to test different ad creatives, refine their campaigns and even create new ad formats.[79] The options to include AI in digital advertising are almost endless. In a recently published whitepaper, IAB Inc described the the most pervasive and powerful ones potentials including:[80]

- Examining millions of data points about a customer to decide frequency and effectiveness when serving ads (whereby AI-driven platforms require fewer interest categories for precise targeting),
- Generating detailed, comprehensive, and bespoke reports measuring campaign performance,
- Developing deeper and more precise insights about audiences (which may reveal more information such as gender, age, and other demographic information; interests; and purchasing behaviour),
- Testing hundreds or thousands of variations of ads quickly and automatically,
- Generating of content (i.e., specific campaign assets such as photos, videos, text, or the creation of the actual advertisements).

All actors in the advertising ecosystem are leveraging generative AI to unlock the multitude of new opportunities. To name some examples, tools like ChatGPT and copy.ai are used to create headlines and advertising copy. Leading online advertising platforms like Meta and Amazon have all debuted AI tools to help their advertisers

[72] IAB Europe Transparency & Consent Framework Policie, chapter III.14 para. 16.

[73] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 31: "Once personal information is collected, it can behave as a public good - a nonrival, non-excludable good that can be easily and cheaply copied and quickly spread through a complex web of companies and data brokers".

[74] Scheppe, Wie KI das Marketing für Unternehmen revolutioniert, Handelsblatt, 2.1.2024; McKay, Big Brands Experiment with Generative AI for Advertising, Maginative, 18.8.2023.

[75] IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, 2024, p. 5.

[76] Kaput, AI in Advertising: Everything You Need to Know, Marketing Artificial Intelligence Institute, 22.1.2024.

[77] Libonati/ Fernandez, The Digital Advertising Revolution: How Artificial Intelligence Is Changing the Game, Globant, 19.10.2023.

[78] Libonati/ Fernandez, The Digital Advertising Revolution: How Artificial Intelligence Is Changing the Game, Globant, 19.10.2023.

[79] Kaput, AI in Advertising: Everything You Need to Know, Marketing Artificial Intelligence Institute, 22.1.2024.

[80] See IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, 2024, pp. 10 et seq. with further references.

create messages, images, and videos for their respective systems.[81] Increasingly, marketers are using AI to tailor highly-personalised advertisements at scale, based on, among other things, age, geography, and interests.[82]

2.2.6 Critics, Complaints and Proceedings before the Belgian authority and ECJ

As early as September 2018 a group of privacy activists and organisations and academic researchers simultaneously filed complaints against Google and the IAB's RTB with the Irish and UK data protection authority, saying RTB is the biggest data breach in history (known as the "Ryan Report).[83] During 2019, the complaints were extended to several more authorities (including Poland, Spain, Belgium and Germany).[84]

In 2019 the UK's data protection authority, the Information Commissioner's Office (ICO), published a report criticising the fact that neither the data subjects nor the supervisory authorities nor even the companies involved could understand, track and control the data flows in this system: "The complex nature of the ecosystem means that in our view participants are engaging with it without fully understanding the privacy and ethical issues involved [...] In many cases there is a reliance on contractual agreements to protect how bid request data is shared, secured and deleted. This does not seem appropriate given the type of personal data sharing and the number of intermediaries involved".[85]

However, criticism is not only coming from data protection experts, but also from publishers, advertising services, and advertisers. In a study conducted for the British advertisers' association ISBA in 2020, the auditors concluded that only about 50 percent of the advertising money invested by advertisers actually reached the publishers on whose websites the advertising was displayed. Even more astonishing is the fact that the auditors were unable to trace the whereabouts of 15 percent of the funds.[86] These figures cast serious doubt on the promised efficiency gains of the current online advertising market in general and personalised advertising in particular.

The dissatisfied statements from within the advertising system are even more interesting. While the combined revenue of the largest European publishers has stagnated over the past ten years, Alphabet and Meta's global revenues increased significantly during the same period.[87] A recent study prepared for the European Commission describes the situation as a "frenemy" dynamic.[88] Those at the outer edge of the network, namely publishers and advertisers, have become completely dependent on the ecosystem, especially the two largest platforms, without any feasible alternative.

[81] IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, 2024, p. 7.

[82] Vanian, How the Generative A.I. Boom Could Forever Change Online Advertising, CNBC, 8.7.2023.

[83] Ryan, Report - Behavioural advertising and personal data, 2018; see also ICCL, The Biggest Data Breach - ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe, 2022.

[84] For a detailed timeline see https://assortedmaterials.com/rtb-evidence/.

[85] ICO, Update report into adtech and real time bidding, 2019, p. 6.

[86] ISBA, Programmatic Supply Chain Transparency - Study, May 2020, p. 8: "15% of

advertiser spend – the unknown delta, representing around one-third of supply chain costs – could not be attributed".

[87] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 21 et seq.

[88] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 10, 245.

During surveys[89] with several small- and medium-sized advertisers and publishers, the authors of the study gathered insights like advertisers saying, it's a take it or leave it situation and publishers losing revenue if they do not submit to the system.[90] Furthermore, advertisers complain about the lack of transparency in performance measurement, especially on the part of the large quasi-monopolies from Silicon Valley. They also fear increasing reputational damage to their brands as a result of criticism of the data protection violations within the personalised advertising ecosystem.[91]

In 2019 the Belgian data protection supervisory authority, Autorité de protection des données (APD), received various complaints about IAB and TCF 2.0 (including the Ryan Report) and subsequently initiated an investigation. Following consultation with other European supervisory authorities between November 2021 and January 2022, the APD issued a fine and injunction on February 2, 2022.[92] Essentially, IAB Europe was accused that the information it receives from CMPs in the TC String and forwards to vendors contains personal data. As all IAB participants consciously and intentionally cooperate in this, the APD assumes joint controllership. In addition to some infringements that only affect the IAB Europe itself (such as lack of appointment of a data protection officer, lack of entries in the register of procedures), APD identified further infringements in its decision that potentially also affect all participants in TCF:

- namely insufficient transparency, esp. that the description of the purpose is not transparent enough, the categories of data processed are not mentioned, the enrichment of data in the context of modern programmatic marketing under the OpenRTB protocol is not explained transparently,
- Even more important, an insufficient legal basis, amongst others, because consent is only informed if data subjects are given access to their profiles, into which the data based on their consent will flow, and
- insufficient technical-organisational measures to control access and use of the personal data by hundreds of vendors.

IAB Europe was given six months to rectify the deficiencies identified. IAB Europe appealed against this and the fine before the Belgian Market Court.[93] The Market Court in turn stayed the proceedings and referred two questions to the European Court of Justice (ECJ) for a preliminary ruling in September 2022. In its decision, the ECJ affirmed the question of the personal reference of the TCF strings and the joint controllership of IAB Europe for the processing of this data together with the other actors of the ecosystem.[94] The other questions previously raised, which concern all actors, remained unaffected by the decision.

[89] The interviews were undertaken between January and April 2022 with nine advertisers and eight publishers, as well as several relevant trade associations, p. 113.

[90] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 121 et. seq, p. 136.

[91] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 125 et seq.

[92] APD, 2.2.2022, DOS-2019-01377, https://www.edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf.

[93] IAB Europe, press release, 4.3.2022, https://iabeurope.eu/iab-europe-appeals-belgian-data-protection-authority-ruling/.

[94] ECJ, 7.3.2024, C-604/22, para. 51 - IAB Europe.

2.3 INDIVIDUAL RISKS FOR CONSUMERS AND STRUCTURAL RISKS FOR THE SOCIETY

In view of the practices of the personalised advertising ecosystem described, both experts and laypersons discuss the following risks caused by the processing of personal data for the purposes of personalised advertising.

2.3.1 Individual risks to privacy: neither foreseeable nor controllable insights into private live

Experts and consumers stress that **possible insights into the consumers' private lives and thus privacy** is where the most pressing threat from personalised advertising lies. 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.[95] The risks that the system imposes on individuals have a variety of different impacts depending on the

- context of data collection or the type of data collected,
- the information about the consumers inferred from the data analysis and
- the extent to which and how many other people get to know this information.

In the context of data collection and the type of the data collected, a further distinction can be made between the **classic privacy spheres**, namely the intimate sphere, the private sphere, the social sphere and the public sphere. In principle, the different spheres and types of data are associated with different expectations of privacy protection against intrusion or unauthorised access and correspondingly different legal protection requirements.[96] For example, while information about the intimate sphere (e.g. diaries, diseases, sexual interests and behaviour) and other special spatial, technical or social spheres that belong to the core area of private life (e.g. privacy at home, privacy of communications, privacy of the family, privacy of the child) are considered particularly worthy of protection, there is significantly less protection of privacy in public.[97] However, even in public, there is undoubtedly privacy protection against the creation of profiles.[98] A well-known example of the latter is movement data, which, if stored permanently and systematically, may be compiled into comprehensive movement profiles that go far beyond the usual social "passer-by situation".[99]

Apart from the classic spheres of privacy, there are also special types of data that are considered particularly worthy of protection due to their **increased potential for abuse**. This category includes in particular the types of data mentioned in Art. 9 GDPR, which reveal, for example, racial and ethnic origin, political opinions, religious beliefs, but also other types of data such as movement data.[100] Due to the ubiquity of tracking

[95] Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 244; Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, pp. 31 et seq.

[96] v. Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I., EDPL 2020, pp. 201 et seq.

[97] Rupp, V./ Grafenstein v., M., Clarifying “personal data” and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection, Computer Law & Security Review, 2024, 1-25, DOI: 10.1016/j.clsr.2023.105932.

[98] ECHR, 25.9.2001, no. 44787/98, para. 56 - P.G. and J.H. v. the UK: “There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”; ECHR, 28.1.2003, no. 44647/98, para. 57 - Peck v. the UK; ECHR, ECHR, 17.7.2003, no. 63737/00, para. 36 - Perry v. the United Kingdom.

[99] ECHR, 2.12.2010, no. 35623/05 - Uzun v. Germany.

[100] EDPB, Guidelines 5/2020 on consent under Regulation 2016/679.

technologies in our increasingly digitalised life, the processing of data for personalised advertising may principally amount to such interference into all these various private spheres.

However, due to the profiling that underlies the personalisation of advertising, not only the context of data collection or the type of the data collected per se, but also the **information that is inferred from the data analysis** is particularly relevant. Just to give a few examples: The food that consumers order may reveal their religious affiliation, just as the places they go, the social network they belong to and the things they do are likely to reveal other interests, inclinations and similar aspects of their private life.[101] Therefore, it is not only about the data originally collected, but also about the inferred information that reveals further insights into the private lives of the consumers when the data is further analysed.

Finally, an interference with private life can be assessed according to the **extent to which and how many people have access to this private information**. So, for laypersons, it makes a difference whether this information is only processed by a machine or whether another person is given access to this information. If another person gets access to the information, it is relevant in which social role that person gets access to the information, and how many people get access to it. If private information is "only" processed by a machine, this does not mean that this would not pose a problem for laypersons. Rather, it must be taken into account that this machine usually belongs to a person and that this person can probably access this information at any time.[102] The issue here is therefore not that there is no interference with private life, but rather how intensive this interference would be and how likely it is that such inference is realised. Thus, the issue is how great the risk of a privacy inference is.

2.3.2 Individual risks of manipulation, discrimination, material and health harm

Beside the risk to the private lives, personalised advertising causes numerous other risks for consumers. With the advent of information technologies, it has long been recognised that the relevance of data is not only determined by the type of the data collected or the context of collection, but above all by the purpose for which the data is used. The collection, analysis and segmentation of user data within the current advertising system enables the actors involved to draw such a precise picture of each user’s current state of mind, beliefs and opinions that makes it easy to exploit their irrationalities, needs, cognitive biases, fears and vulnerabilities for **manipulation**.[103] The risk is intensified by the fact that receiving messages personalised in a way that

[101] ECJ, 20.12.2017, C-434/16, para. 34 et seq.: “The use of the expression ‘any information’ in the definition of the concept of ‘personal data’, within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject. As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.”; Ehmann/ Selmayr/ *Klabunde/ Horváth*, Art. 4 GDPR, para.10.

[102] V. Grafenstein/ Jakobi/ Stevens, Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods, Computer Law & Security Review, 2022, p. 18: “For example, with respect to the ‘human in the loop’ debate surrounding voice assistants, one workshop participant said he had not considered the pure processing of private information by an algorithm as an intrusion into his privacy (because such a privacy intrusion apparently requires, in his opinion, a human who gets the private information). On the other hand, another participant said that the more people have access to such information,the more conspicuously their privacy would be concerned”.

[103] Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 245; Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy Press 26.9.2023.

specifically targets the personality of individuals hinders their ability to accurately sense when and how they are being manipulated.[104]

With respect to the consumer market, the processing of personal data for personalised advertising causes the risk of being manipulated when purchasing consumer goods.[105] Similarly, if tracking technologies and profiling are used not only for advertising **in the context of purchasing consumer goods, but also in other contexts**, this poses a risk to further fundamental rights. In the context of elections, so-called political micro-targeting may pose a risk to free (i.e. non-manipulated) individual voting decisions.[106] The most striking example here is probably the case of the British consulting company Cambridge Analytica that collected personal data belonging to millions of Facebook users without their consent, predominantly to be used for political advertising.[107] The same applies to the personalisation of news, where there is a risk to freedom of information of individuals.

Both experts and laypersons also see further risks for consumers. These include the **risk of discrimination** resulting from the fact that personalised advertising is only displayed to certain groups of people and not to the public as a whole.[108] This may not only lead to discrimination against groups with certain characteristics, which is considered "inappropriate" (“sachwidrig”) and socially intolerable (see, for example, the constitutionally guaranteed freedoms from discrimination under Art. 20 et seq. ECFR and the anti-discrimination laws at the level of ordinary law). Rather, personalisation may also **undermine additional rights to freedom and participation**. 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.[109]

The personalisation of advertising may also lead to **material as well as physical and psychological harm** for consumers. At the very least, the risk of material damage arises from the fact that consumers may buy services or products that they had not initially intended to buy or do not fit their best interests.[110] In the case of price discrimination, this means consumers buying goods or products at a higher price than other groups of people who are shown a lower price.[111] According to some observers, personalised advertising also favours **fraud**.[112] Last but not least, **physical and psychological harm to health** may result from the targeting of particularly vulnerable

[104] Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, p. 7.

[105] Google euphemistically speaks of „[…] shape your consumer‘s decision […] Anticipate the micro-moments for your target audience, and commit to being there to help when those moments occur“, Google, The Basics of Micro-Moments, 2016; Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy Press 26.9.2023; AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 85 et seq.

[106] Scott, Cambridge Analytica did work for Brexit groups, says ex-staffer, Politico 30.7.2019; AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 86 et seq.

[107] A pre-GDPR investigation by the ICO led to a fine of 500.000 british pounds, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/#.

[108] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 82 et seq.

[109] Dunphy, Women are seeing fewer STEM job ads than men: are marketing algorithms promoting gender bias?, European Scientist 28.7.2018.

[110] Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 245.

[111] See, for example, Rützel, Rechtsfragen algorithmischer Preisdiskriminierung: eine rechtsgebietsübergreifende Untersuchung. 2023.

[112] Meyer, Warum seriöse Websites Werbung von Fake-Shops schalten, Deutschlandfunk 11.4.2023; Mayer, Manipulierte Bilder, falsche Nachrichten: Wie es betrügerische Werbeanzeigen immer wieder in Online-Medien schaffen, Tagesspiegel 21.3.2023.

groups (such as children or addicts). For example, when advertising specifically targets 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.[113]

In this context, it is important to emphasise that all people may experience vulnerability detached from group-related vulnerabilities.[114] Depending on situations or contexts, older people who are overwhelmed by the speed of changing and emerging digital requirements can be vulnerable. Or children who know how to use devices and new services, but not how to deal with the sudden threats posed by digital communication. But 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.[115] Or even more trivial: lack of understanding of targeting can make consumers vulnerable.[116]

After all, the use of AI primarily represents an intensification of the already existing individual, economic and social risks.[117] 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 and regulation. Not least because AI enables the creation of hyper-personalised ad messages and targeting to individual consumers. [118]

2.3.3 Structural risks for the society (esp. democracy, solidarity, fair competition)

Beside risks for individual consumers or groups of consumers, the processing of personal data for personal advertising also causes **risks for third parties or structural risks for society as a whole**. The first situation is often referred to with the term “third party effect”, which describes the ethical claim that an agreement, exchange or simply actions between two parties must not lead to another being harmed.[119] However, this phenomenon is not uncommon, especially in data protection law because of the conclusions that can be drawn not only from data, but also from the absence of data. For example, it is possible that only those consumers who allow insights into their private lives will be shown a lower price. By default, all others would receive the ‘normal’ price. When a price is lower than a ‘normal’ price and when the lower price becomes the ‘normal’ price and everyone else now pays the higher price is, of course, up for debate. Our aim with this example was just to illustrate that such third-party effects can also occur in the area of personalised advertising. This example also shows that the boundaries between self-determination and third-party effects are rather fluent, and lead to corresponding problems in the search for appropriate protection mechanisms.

[113] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 86.

[114] Kroschwald, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, p. 5; Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, p. 6.

[115] For example, by using so-called dark patterns when asking for consent in connection with online services and platforms, see EDPB, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, 2023.

[116] Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, pp. 7 et seq.

[117] Vigliarolo, Turns out AI chatbots are way more persuasive than humans, The Register, 3.4.2024.

[118] IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, 2024, p. 12.

[119] Engle, Third Party Effect of Fundamental Rights (Drittwirkung), HanseLR 2009, pp. 165 et seq.

This is all the more true with respect to structural risks for the society as a whole. In particular, risks to **(IT) security** are observed not only for individual systems or organisations, but extend to critical infrastructure as a whole, e.g. through the more efficient distribution of malware[120] or the tracking of people within the security sector[121]. In addition, observers also discuss the dissemination of **misinformation** / harmful content that may damage the public discourse space.[122] Similarly, 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,[123] just as the increasingly fine-grained customisation of insurance policies may undermine the principle of **social solidarity**.[124] Last but not least, critics also mention the **negative environmental** impact of the personalisation of advertising.[125]

With all these societal risks, the question is as to whether their control should depend on the decision-making freedom of individuals or whether objective measures are needed here. In its very end, this question depends on the cause-and-effect chain on which these risks and possible harm to collective legal interests such as the security of critical infrastructures, the principle of democracy and solidarity or a functioning public discourse are based. In its decision on the 1983 Census Act ("Volkszählungsurteil"), for example, the German Federal Constitutional Court considered it an indispensable prerequisite for a democratically constituted society that its individual members, i.e. each individual citizen, remain in a position to make autonomous decisions and act accordingly.[126] The functioning of a democratic system is therefore conceptually based on the ability of individual citizens to make autonomous decisions. Similar relationships are constructed in German competition law (Unfair Competition Act – UWG). Even though most of the regulations are now based on European harmonising directives, their implementation in Germany still follows its basic distinction between a micro-economic and a macro-economic level: The protection of autonomous consumer purchasing decisions on a micro-economic level leads to fair competition on a macro- or at least meso-economic level.[127] Of course, German competition law does not stop there, but finds further entry points for regulation that goes beyond this individual decision-centred approach (see in particular the Act against Restraints of Competition – GWB) applying a more structural approach.

However, as to whether (European) data protection law should be conceived in a more individualistic way with subjective rights and then protect collective interests as kind of an annex by means of objective duties for the data controller or, conversely, whether data protection law should primarily be understood as an objective obligation of data controllers, from which individual subjective rights of consumers are then derived, is in

[120] BSI, Cyber-Angriffe über Online-Werbung, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/Adblocker-Tracking/adblocker_tracking.html?nn=130950#doc504232bodyText3.

[121] Dachwitz/Meineck, Datenhändler verticken Handy-Standorte von EU-Bürger*innen, Netzpolitik, 17.1.2024.

[122] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 78 et seq.

[123] Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, p. 5.

[124] Iversen/ Rehm, Big Data and the Welfare State: How the Information Revolution Threatens Social Solidarity, 2022, pp. 188 et seq.

[125] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 89 et seq.

[126] Federal Constitutional Court, 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83, para. 127 - Volkszählungsurteil.

[127] V. Grafenstein/ Hölzel/ Irgmaier/ Pohle, Nudging - Regulierung durch Big Data und Verhaltenswissenschaften, 2018.

any case a rather theoretical dispute.[128] In practice, the legislator usually implements both approaches anyway, either in a single law or by way of different laws. The GDPR, for example, not only protects the interests of data subjects (see Art. 1 sect. 2 GDPR), but also those of society as a whole (see, for example, the interests of the public to be respected in Art. 6 sect. 1 lit. f GDPR).[129] The same applies to the new AI Act, which not only protects the fundamental rights of the consumers, but also the democracy and security of society as a whole (Art. 1 sect. 1 AI Act). The Digital Services Act also protects both the individual users of the platforms and general interests such as the public discourse (Art. 34 sect. 1 DSA). Similarly, the Political Advertising Regulation protects both the individual voter from the manipulation of their vote and the democratic system as a whole (Art. 12 et seq. as well as recitals 4 and 6 PTR). The Data Governance Act also helps individuals to share their data, but it also aims to exploit the innovation potential of the European data space more effectively for the benefit of society as a whole (Art. 12 et seq. as well as recitals 1 et seq. DGA). Similarly, the Digital Markets Act protects individual consumers from the abuse of market power by so-called gatekeepers, while safeguarding free competition (Art. 1 and 5 sect. 2 DMA). We will return to this later in our analysis of possible alternative or supplementary regulatory approaches for the personalisation of advertising (see chapter 5).

2.4 CONCEPTUAL AND PRACTICAL LIMITATIONS OF THE CONSENT MODEL

The above comments on the various risks for consumers, third parties and society as a whole suggest that consent as a protection instrument is not a magic bullet, but is subject to limitations. Some of these restrictions already exist at a conceptual level, but several result from inadequate practical implementation.

2.4.1 Conceptual limitations: How to transform consent from a privacy tool into a risk management tool?

On a conceptual level, many problems with consent result from the fact that it is intended as a tool to protect against privacy intrusion. However, the protection of privacy is not the only area of application of consent. In fact, in many cases today, consent must also function as a tool for controlling numerous other risks for consumers. This makes it necessary for consent to have additional conceptual functions and therefore to be designed accordingly in practice.

With respect to privacy protection, measures are usually aimed at ensuring that such intrusion is made transparent to the data subject in good time, so that they may shield themselves from such an intrusion if they do not want it. **Informed consent is the classic mechanism for privacy protection** by which consumers can decide to whom they disclose which insights into their private lives and which they do not. How comprehensive the information must be for consent to be considered informed, and how strict the requirements for giving consent must be for it to be considered a conscious decision by the consumer, depends on the extent and intensity of the (expected) invasion of privacy. With regard to the previously described structures of the online advertising ecosystem (see chapter 2.2., esp. 2.2.6.), it is obvious that – as found out by the APD – there is hardly any transparency about which actors have

[128] Britz, Informationelle Selbstbestimmung - zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, 2010, pp. 594, 595.

[129] EDPB,Guidelines 1/2024 on processing of personal data based on Article 6 (1) (f) GDPR, para. 128.

access to which personal data and in what way.[130] **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.[131] We will go into more detail on the practical challenges of implementing consent in practice in the following chapter (see chapter 2.4.2.).[132]

The requirements for the function and design of consent in relation to other individual risks for consumers are different. In these cases, the question arises as to how the consumers may be most effectively protected against the risk of manipulation, discrimination, material or mental harm. Is the appropriate safeguard here, similar to privacy protection, a consent mechanism by which consumers may agree to be manipulated (just as they agree to an intrusion into their privacy)?[133] With this function, consent makes no sense: **After all, who would voluntarily agree to discrimination, loss of freedom, material or mental harm if they were really informed about it?** In these cases, consent does not have the function of shielding one’s privacy from others, but rather of enabling the data subject to understand and control in a self-effective manner the risk that the processing of their data will limit their scope of social freedoms, will lead to unequal treatment or material or health damage. One would only agree to such a risk if it were outweighed by a sufficiently large benefit – or at least if one believed that one could sufficiently control the risk and thus change the risk-benefit ratio in one's favour. **This requires**, first of all, **the necessary information about the risks and also the benefits.** Secondly, the ‘consent process’ must be designed in such a way that consumers can change the risk-benefit ratio in their favour in the respective context of use and at the right time. Consent to the intrusion into privacy logically occurs before the data is collected, because the data collection generates the insights into private life. However, the risks of manipulation, discrimination, and material and health harm are realised later, after the data has been collected. These risks arise from the way in which the data is processed and used. In the case of personalised advertising, this is usually the moment when the advertising is displayed to the consumer, i.e. when the consumer sees the advertising and interacts with it. The **information and control options for consumers must therefore focus on this moment when the advertising is displayed**, so that consumers can effectively protect themselves. This is why traditional consent is conceptually not the most

[130] Cf. Belgian Data Protection Authority wrt TCF, APD, 2.2.2022, DOS-2019-01377, para. 465 et seq.; on the extent of the data sets processed, see Ryan, Report - Behavioural advertising and personal data, 2018 as well as ICCL, The Biggest Data Breach, 2022.

[131] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 31: “In such a context, the sophisticated disclosure and consent obligations of [...] the GDPR cannot wash away the fact that mandated disclosure and other provisions aimed at increasing consumer data awareness have failed”; Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 248: “It is questionable whether consent could be actually the appropriate tool to optimally secure the interests of digital consumers, given that the obvious cognitive and informational asymmetry between the user and the publisher usually leaves a user exposed to the circulation of his/her personal data to an unspecified number of ad intermediaries and advertisers, without knowing in advance how, where, when and why his/her information will be processed”.

[132] v. Grafenstein/ Heumüller/ Belgacem/ Jakobi/ Smieskol, Effective regulation through design - Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach, 2021, pp. 8 et seq.

[133] Cf. the debate on waiving fundamental rights through consent, for example at Lynskey, The Foundations of EU Data Protection Law, pp. 188-190, with further references; Ohly, Die Einwilligung im Privatrecht, pp. 94 and 95 and v. Grafenstein, The Principle of Purpose Limitation in Data Protection Law, pp. 572 et seq.

important component of effective protection against the manipulation risk, and in no way a sufficient one.[134]

However, **effective implementation of such a broadened understanding of the consent model would require a number of technical and organisational measures**: Here too, the actors involved would therefore have to coordinate in such a way that consumers receive the necessary information even if this can only come from actors who do not have a direct end-user interface with consumers, but are active further down the data value chain.

Last but not least, the limitations of consent as an effective protection mechanism arise even more clearly when it is not about risks for individual consumers or groups of consumers, but about **risks for third parties or structural risks for society as a whole**. Whether one wants to adhere to consent at all in the face of these risks depends on whether one makes the autonomous decisions of individual consumers a prerequisite for social legal interests. In the case of collective legal interests such as a functioning democracy, public discourse and fair competition, this is certainly conceivable. It might be more questionable in the case of other collective legal interests such as security or the environment. In any case, this mechanism only works if the relevant information is available. In this context, it should be emphasised that it is not even so much about the information that individuals need to have about these structural risks (they need the information too, but not only they). The main thing rather is that actors who represent societal interests are able to measure these structural risks at all. This is possible, for example, if the data controllers are forced to disclose the information, such as how many people in total are exposed to which advertising, how much money is spent by which interest groups on which advertising; where the money ultimately ends up, etc. **This information can be given, for example, by means of access rights for individual actors (such as journalists, scientists and supervisory authorities) or public registers**. Only on this basis of information can suitable metrics and methods then be used to determine which risks really exist for which collective legal interest. The fact that numerous laws already provide for such rights of inspection and public registers will be discussed in more detail in chapter 3 on the current legal framework.

2.4.2 Practical limitations: Consumer perceptions between fatalistic risk control and vague value expectations

The conceptual limitations of the consent model go hand in hand with some, mostly serious, problems of informed consent in practice. In presenting these practical problems, we focus on the consumer perspective, since it is ultimately the consumers who decide whether one or another consent mechanism effectively informs them about the risks and allows them to control these risks effectively. In summary, it can be said that the problems that consumers see in the current practice of personalised advertising are so serious that there has been a widespread loss of trust in this form of data processing; consumers feel caught between powerlessness and fatalism. The problems of consent as it is currently designed in practice can ultimately be categorised into three broad groups: opaqueness and deception; consent fatigue; data misuse.

[134] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 78 et seq.

2.4.2.1 Opaque, deceptive and manipulative designs of current consent forms

The starting point here are empirical studies, in which an overwhelming **majority across Europe spoke out against tracking and personalised advertising** anyway.[135] Globally, user acceptance of tracking – often linked to advertising – is notably low. In a large-scale study, Kozyreva et al. highlight the low acceptance of data collection for personalisation among users in Germany and Great Britain and emphasise the need for transparent algorithmic personalisation (2021).[136]

At the same time, there is a **very limited understanding of tracking and its scope amongst consumers**. Thode et al. (2015) exposed non-technical users to tracking technologies and found that many were surprised by the extent of tracking they experience during everyday online activities.[137] These users generally oppose online tracking, citing distrust in protection measures and concerns over privacy and control. The study underlines the significant lack of awareness among non-technical users regarding the scale and prevalence of tracking technologies, reinforcing the need to improve digital literacy and raise awareness about online privacy issues. Further, the mental models users have of how tracking works online vary widely and are often inaccurate. Yao et al. (2017) identified the diverse and often mistaken beliefs people hold about how personalised advertising functions.[138]

Another reason that is very often mentioned negatively by consumers is the **deceptive and manipulative design of consent processes** that encourage consumers to give their consent rather than refuse it.[139] Even though the situation is improving thanks to the growing number of statements and recommendations published by data protection authorities,[140] there are still numerous such practices. These are based not least on

[135] European Interactive Digital Advertising Alliance, Your Online Voices: What consumers told us about their perceptions, needs, hopes, and expectations of data-driven advertising, p. 9; McCann/ Stronge/ Jones, The future of Online Advertising, 2021, pp. 75 et seq.; Forbrukerrådet, Surveillance-based advertising - Consumer attitudes to surveillance-based advertising, 2021, p. 3.

[136] Kozyreva/ Lorenz-Spreen/ Hertwig/ Lewandowsky/ Herzog, Public Attitudes towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States, Humanities & Social Sciences Communications 8/2021, p. 1.

[137] Thode/ Griesbaum/ Mandl, "I Would Have Never Allowed It": User Perception of Third-Party Tracking and Implications for Display Advertising, 2015.

[138] Yao/ Re/ Wang, Folk Models of Online Behavioral Advertising, 2017.

[139] Bauer/ Bergstrøm/ Foss-Madsen, Are you sure, you want a cookie? - The effects of choice architecture on users' decisions about sharing private online data, 2021.

[140] AEPD, Guía sobre el uso de las cookies, Mai 2024; APD, Cookies et autres traceurs, April 2020; APD/La Commission de la protection de la vie privée, Recommandation n° 01/2015 du 4 février 2015; Autoriteit Persoonsgegevens, Handleiding privacyvriendelijk instellen van Google Analytics, 13.1.2022; Autoriteit Persoonsgegevens, Cookies FAQ, 2022; CNIL, Délibération n° 2020-092 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux „cookies et autres traceurs" 17.9.2020; CNIL, Délibération n° 2020-091 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux „cookies et autres traceurs") et abrogeant la délibération n° 2019-093 du 4 juillet 2019, 17.9.2020; CNIL, Questions-réponses sur les lignes directrices modificatives et la recommandation „cookies et autres traceurs" de la CNIL, 18.3.2021; CNIL, Délibération n° 2013-378 du 5 décembre portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, 5.12.2013; CNPD, Lignes directrices en matière de cookies et autres traceurs,, 20.10.2021; Datatilsynet, Behandling af personoplysninger om hjemmesidebesøgende – Vejledning Feb. 2020; Datatilsynet, Quick-guide til at sætte cookies, 12.2.2021; DPC, Report by the Data Protection Commission on the use of cookies and other tracking technologies, 6.4.2020; DPC, Guidance Note: Cookies and other tracking technologies, April 2020; ÖDSB, FAQ zum Thema Cookies und Datenschutz, 2023; DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021; EDPB, Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023, EDPB, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, 14.3.2022; GPDP, Guidelines on the use of cookies and other tracking tools, 10.6.2021; GPDP, Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies, 8.5.2014; HDPA, Recommendations on controllers' compliance with the specific legislation on electronic

technical progress and the additional possibilities for these practices that this development creates.

This suggests that most consent notices do not inform consumers effectively, at least not effectively enough to meet the requirements of the law. Art. 6 sect. 1 lit. a and Art. 25 sect. 1 GDPR require the controller to implement consent in a way that effectively informs the consumers about the risks caused by the processing of their data, and to effectively control these risks by giving consent or not. Such effective control is barely the case with the consent forms currently in use. This finding is confirmed in a quantitative study by Grassl et al., according to which **consent, even designed according to current best practices, hardly meets the requirements of Art. 6 sect. 1 lit. a and Art. 25 sect. 1 GDPR.** In an online study with 985 participants an interdisciplinary research group tested on a fictitious plant webshop how well a cookie banner that has been designed according to best practice rules enabled the participants to understand and control the processing of their data.[141] The cookie banner was designed in accordance with best practice rules,[142] and contained the following processing purposes (see a screenshot of the cookie banner used for the study in **Annex 1**):

1) *Statistics to improve the website*;

2) *Personalisation of the website*;

3) *Personalisation of Online Advertising*.

The results of this study show that the participants were hardly able, due to the currently given information in the cookie banner, to correctly assess the right risks (not even the benefits) to the respective purpose. The participants hardly recognised any differences between the purposes. The results also show that the majority of participants sees themselves hardly able to control the handling of their data through the cookie banner. In particular, the best practice cookie banner barely achieved the objectives of the Art.-29 Working Party, in its ‘Opinion 03/2013 on purpose limitation’, according to which the processing purposes must be specified in such a way that the data subjects may assess the scope of the data processing, whether they find the data processing appropriate and whether they agree with the data processing or not.[143] The participants were also hardly able to recognise the impact of consenting to one or the other purpose on their lives. As a result, 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.

However, other recent studies also suggest that consent processes can in fact be designed in such a way that they do inform consumers better about the risks and enable them to control them more effectively. However, a **more effective design requires the application of interdisciplinary methods**, in particular from data protection law, user experience, visual and textual design, as well as from the social

communications, 25.2.2020; ICO, Guidance on the use of cookies and similar technologies, 2019; ICO, Cookies and similar technologies, 2019; LfDI BW, FAQ - Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, März 2022.

[141] Grassl/ Gerber/ v. Grafenstein, How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? EDPL 2024, pp. 96 et seq.; see also the extended version of this paper including charts and images online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012997.

[142] EDPB, Report of the work undertaken by the Cookie Banner Taskforce, 2023; ConPolicy, Good Practice Initiative for Cookie Banner Consent Management, Design Guidelines, 26 January 2023.

[143] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, p. 11.

and behavioural sciences. These methods must be synchronised in their understanding of problems, objectives, solution concepts, methods and processes.[144] Such a synchronisation requires a considerable amount of coordination, not only organisationally but also intellectually. The current practical problems therefore do not mean that the consent model should be abandoned as a whole because the practical problems could not be solved. Rather, there is evidence to suggest that consent should even be retained, at least under certain conditions, in order to allow consumers to realise their individual preferences. We will discuss this in more detail in chapter 4.

2.4.2.2 Consent fatigue caused by the multitude of consent forms

A second serious problem is what is known as consent fatigue. This results from the fact that consumers had to read privacy policies around 244 hours per year to give their informed consent on the internet.[145] Thus, even if these consent banners were designed in such a way that they most effectively inform consumers about the risks and most effectively control them, **the high number alone still leads to a fatigue effect, which in turn causes consumers not to read the information and not to exercise their control options**.[146]

In this context, too, we would like to point out that the problem is not unsolvable. One approach is to establish the requirement to obtain informed consent in a slightly less comprehensive way by law, or to switch from opt-in to opt-out processes for low-risk processes so that consumers are less forced to click. The conceptual rationale behind this is that an opt-in process based on Art. 6 sect. 1 lit. a GDPR and an opt-out process based on Art. 6 sect. 1 lit. f GDPR are actually both default settings prescribed by law. Depending on which result the data subjects prefer, one or the other default setting means more or less effort for them to achieve this result: Those who do not agree with a certain processing purpose have less effort with an opt-in process because they can simply (but also have to) click away the cookie banner. Those who agree with one or more purposes, on the other hand, have more effort with an opt-in process because they now have to take action and explicitly switch each individual toggle to ‘on’. For this second group of people, an opt-out process would mean less effort. Of course, which default setting means more or less effort for the data subjects in order to achieve their goal can only be answered reliably on the basis of empirical data. Without such data, the discussion is based on guesswork. We believe it is at least possible that a clear majority of data subjects will agree to a processing purpose if the benefits for them are significantly higher than the risks. Taking this restriction into account, we believe it is at least possible that a clear majority of data subjects will agree to a processing purpose if the benefits for them are significantly higher than the risks. For these cases, we therefore bring into play the possibility of switching from an opt-in to an opt-out process. Finally, if it can even be determined on the basis of empirical data that the

[144] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review 2024, pp. 1 et seq.; v. Grafenstein/ Jakobi/ Stevens, Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods, Computer Law & Security Review 2021.

[145] McDonald/ Cranor, The Cost of Reading Privacy Policies, A Journal of Law and Policy for the Information Society, 2008, pp. 543 et seq.; see also more recently cf. Forbrukerrådet, Deceived by Design – How tech companies use dark patterns to discourage us from

exercising our rights to privacy, 2018.

[146] Kulyk/ Gerber/ Hilt/ Volkamer, Has the GDPR hype affected users’ reaction to cookie disclaimers?, Journal of Cybersecurity 2020.

overwhelming majority of data subjects agree or disagree with a purpose, consent could even be dispensed with altogether and the respective purpose either completely authorised or prohibited by law. Because then there is obviously no need for consent to reflect different needs for privacy amongst the data subjects.[147]

As far as one wants to stick to consent processes, the second approach comes into play, namely involving so-called Personal Information Management Services (PIMS) to solve the problem of consent fatigue. Especially so-called consent agents can be an important building block for countering consent fatigue, as they enable users to specify their privacy preferences in advance and in a centralised manner. After users made their preferences, the consent agent communicates these preferences to the respective website visited, whereby users usually have the opportunity to adapt their preferences to the specific data processing circumstances of the website. By giving users the opportunity to familiarise themselves with the processing of their data within their consent agent in advance, there is more space, more time and more attention available for the users to process the information. Most importantly, users are no longer forced to give their consent on every single website they visit, which avoids the resulting consent fatigue.[148] We will discuss the role of PIMS in more detail below, in particular the legal, technical and organisational requirements that must be met if they are to be used to provide consumers with truly more effective protection (see chapter 4).

2.4.2.3 Data misuse caused by non-specific purposes and insufficient data use controls

The third problem can be identified against the background of the aforementioned issues: consumers have little or no trust that the data will not be used in a way that is unfavourable for them.

This problem ultimately stems from an **inadequate implementation of the principle of purpose limitation**. The principle of purpose limitation is a cornerstone of data protection law and requires data controllers to specify their processing purposes with sufficient detail and not to process the data later in a way that is incompatible with this original purpose specification. As mentioned above, the Art. 29 Data Protection Working Party points out that the purposes must be specified in such a way that the data subjects may assess the scope of the data processing, whether they find the data processing appropriate and whether they agree with the data processing or not.[149] Ultimately, the purpose limitation principle is about identifying risks of data processing in good time so that they can be effectively controlled.[150]

In a relatively large qualitative study, an interdisciplinary team of researchers asked consumers about their views on how well the principle of purpose limitation is currently being implemented in practice. To do this, the research team first determined the ways in which the data collected could be used that were unfavourable (i.e. risky) for them, using the example of the use of three technologies (namely using websites, voice assistants and connected cars). In a second step, the research team showed

[147] Cf. on the function of consent Masing, Herausforderungen des Datenschutzes, 2012.

[148] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review 2024, pp. 20 et seq.

[149] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, p. 11.

[150] V. Grafenstein, Refining the concept of the right to data protection in Article 8 ECFR – Part II, EDPL 2021, pp. 190 et seq.

consumers various purpose formulations that the respective technology providers typically make to consumers and asked the consumers for their opinion on how well these purpose specifications explain or exclude the risks. In the opinion of the consumers surveyed, the purpose statements did not exclude the risks. On the contrary, in view of the purpose formulations, the consumers had to expect that in principle all risks could occur and sooner or later would occur.[151]

Even if controllers specify their processing purposes in a way that better explains and excludes the risks, there is still the additional **problem that the controller may not use the data in a manner that is incompatible with these purposes**, that is, in any way that leads to other or higher risks.[152] One reason for why purpose limitation is often only weakly implemented in practice is that the necessary documentation of the original purposes is lacking. If the original purpose is no longer known or has not been sufficiently documented, it may not be possible to verify whether the respective planned or current use is incompatible with this original purpose. This applies in particular to longer data processing chains or networks, where there is a particularly high risk that knowledge of the original purpose will be lost due to the continuous transfer of data. Thus, the controllers must ensure to pass on, together with the data, the documentation of the original use and the conditions for the new use to the respective data recipient. However, even where the purposes are sufficiently documented, there are often hardly any technical or organisational measures implemented in practice to prevent the use of data in a way that is not compatible with the original purpose of data collection. The fact that the principle of purpose limitation is, so far, insufficiently implemented, especially in the online advertising ecosystem today, is shown by the above example of the IAB's Transparency and Consent Framework (see chapter 2.2.4.3.).

However, here again, we would like to point out that these results do not mean that the principle of purpose limitation could not be implemented more effectively (and should therefore be abandoned[153], or replaced by another instrument[154]). Rather, empirical studies suggest that the purposes can indeed be formulated in such a way that they more clearly explicate and exclude the risks.[155] Furthermore, certification processes can provide an important anchor for consumer trust that the data will not be misused, later on, in a way that leads to risks beyond those originally indicated.[156] As described, the TCF of the IAB Europe has actually already provided for such a certification process; however, for the reasons of governance mentioned above, this mechanism is too weak in practice and cannot avoid data misuse (see chapter 2.2.4.3.). Thus, certification

[151] V. Grafenstein/ Jakobi/ Stevens, Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods, Computer Law & Security Review 2021.

[152] V. Grafenstein, Refining the concept of the right to data protection in Article 8 ECFR – Part II, EDPL 2021, pp. 190 et seq.

[153] See Moerel/ Prins, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, 2016.

[154] See Nissenbaum, Respect for Context as a Benchmark, 2015.

[155] V. Grafenstein/ Jakobi/ Stevens, Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods, Computer Law & Security Review, 2021, pp. 21 et seq.; and on this basis, v. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review, 2024, p. 10.

[156] Smieskol/ Jakobi/ v. Grafenstein, From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. Computer Law and Security Review, 2024.

mechanisms would have to be made more effective, for example on the basis of Art. 42 GDPR (see in more detail chapter 2.5.8.3.).

2.4.2.4 Inability of consumers to weigh the benefits against the risks

Interestingly, consumers generally see added value in the personalisation of advertising, provided that this really makes the advertising more relevant to them.[157] The main problem is that they cannot check for themselves whether the advertising is actually more relevant. The fact that consumers cannot experience the promised added value of personalised advertising, let alone verify it, combined with the impression that the risks are concealed and that they are therefore deceived or manipulated into giving their consent anyway, leads to the feelings of fatalism described above and the widespread loss of trust.

In this context, it should be pointed out one last time that this does not mean that it is impossible to design consent processes accordingly. Rather, the studies mentioned above show that it is indeed possible to design consent processes in such a way that consumers can compare different forms of advertising for themselves in terms of the relevance of the advertising type and its risks.[158] Only then will consumers be able to understand the consequences of data processing and thus the significance of their decision. However, it is just not currently implemented in this way (see chapter 4 for a discussion on how this could be implemented better).

2.4.2.5 Need to take up with technological development

There is another practical problem that is more procedural in nature. The question is how the design of consent processes can keep pace with technological developments. This challenge is both negative and positive: on the one hand, the question is how to ensure that consent processes can be designed in such a way that they can also be effectively designed for new risks that were not yet foreseeable at the time of the first design. On the other hand, the same question arises if a better, even more effective design of consent processes should emerge while the risks remain the same. In both cases, a mechanism is needed to ensure that the design is open to future developments on the one hand and demands a kind of design optimisation of what is possible in each case on the other. Readers will now rightly expect that there are already solutions for this as well, which we will discuss in detail later (see chapter 3.1.2.6.).

[157] McCann/ Stronge/ Jones, The future of Online Advertising, 2021, p. 15; Smieskol/ Jakobi/ v. Grafenstein, From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. Computer Law and Security Review, 2024.

[158] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review 2024, pp. 17 et seq.; Smieskol/ Jakobi/ v. Grafenstein, From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalised and non-personalized content through an On/Off toggle. Computer Law and Security Review, 2024.

2.4.3 Interims conclusion: Objective controls to complement and/or replace the consent model to make risk protection more effective

The previous chapters showed with respect to numerous risks that the consent model is subject to considerable conceptual and practical limitations. However, these constraints could be overcome and compensated by appropriate objective measures:

- Effectively informed consent to the intrusion into consumers' private lives would require that consumers would 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 (see in more detail chapter 4.3.).

- With the risks of manipulation, discrimination, material and health harm, one should speak less of consent and more of control. Effective control of these risks should shift the focus to the context and the point in time at which these risks actually occur, i.e. usually at the moment when the consumer is shown the advert and interacts with it. Here too, this would require appropriate coordination between the actors involved in the personalised advertising processes (see in more detail chapter 5.5.).

- Effective consent processes not only require consumers to understand the risks, but also to be able to understand the benefits of personalised advertising, and to weigh up the benefits against the risks. Furthermore, the consent processes must be designed in such a way that they can compare different forms of advertising, for example personalised or not, in terms of these benefits and risks of each type of advertising. Only then will consumers be able to truly understand the consequences of data processing and thus the significance of their decision.

- The effective design of informed consent and control processes requires the application of interdisciplinary methods, in particular from data protection law, user experience, visual and textual design, as well as from the social and behavioural sciences; these processes must enable the design of consent processes to be adapted to technological developments in such a way that they ensure the best possible protection against risks (see in more detail chapter 4.3.).

- Even the most informative and effective consent and control processes cannot prevent consent fatigue in the face of the extremely high number of consents consumers are asked to provide on a daily basis. One approach is, of course, to completely abandon the legal requirement to obtain informed consent, or at least cut it down, or at least to switch from opt-in to opt-out processes for low-risk processes so that consumers are less forced to click. As far as one wants to stick to consent processes, so-called consent agents are an important building block for countering consent fatigue, as they enable users to specify their privacy preferences in advance and in a centralised manner. However, this also requires a number of legal, technical and organisational requirements to be met in order for this solution to actually lead to more effective consent processes in practice (see in more detail chapter 2.5.1.).

- To counter the justified concern of consumers that the data will be used for all kinds of purposes anyway and that sooner or later all kinds of risks will likely materialise, effective (not only legal, but also technical and organisational) measures would have to be implemented to control the subsequent use of the data. Certification processes, such as those already provided for by the TCF, are one example that springs to mind here. However, these would have to be designed more effectively, for example on the basis of Art. 42 et seq. GDPR (see in more detail chapter 2.5.8.3.).

- Last but not least, some of the structural risks for society can also be eliminated with more effective decision-making processes at the individual level. This applies above all to collective legal interests such as a functioning democracy, public discourse or solidarity. However, to be able to measure structural risks at all, additional objective measures are needed to ensure the necessary information (e.g. which advertisement was played to whom and how often, who paid how much and where did the money go). This can be done, for example, through access to information rights for representatives of the public interest (e.g. journalists, scientists, law enforcement authorities), and more comprehensively through public registers (see in more detail, for example, the chapters 3.3., 3.4. and 3.5.).

2.5 CURRENT AND CURRENTLY FORESEEABLE DEVELOPMENTS: RISK CONTROL APPROACHES FROM CIVIL SOCIETY AND INDUSTRY, AS WELL AS FURTHER RISK AGGRAVATIONS

Against the background of the preceding risk analysis, it is now interesting to examine the extent to which current developments already address or perhaps even intensify these risks. Behavioural advertising most widely relies on large amounts of personal data being processed. Over the last few years, there have been visible major changes when it comes to the development of less intrusive alternatives. More and more consumers become aware – and sensitive – about the risks outlined in the previous chapter which is why they are pushing for more privacy-preserving (tech) solutions.[159] At the same time, the regulatory framework changes significantly. In addition to the GDPR various new laws have been adopted that force actors related to the advertising ecosystem to change their practices and be more transparent about how they process user data.

Efforts have been made from this situation by the industry, civil society and scientific community over the last years to evolve methods, techniques and commitments for providing more effective privacy solutions and its technical and organisational pre-conditions.[160] One approach is the involvement of PIMS at a higher level, meaning that (neutral) services are integrated into websites, apps or browsers to help users manage their choices (see below 2.5.1.). Other developments concentrate more on the technical-organisational conditions. Among these, we will discuss server-side tracking (see 2.5.2.), cohort-based and interest-based personalisation of advertising (2.5.3. and 2.5.4.), anonymised conversion measurement (2.5.5.) as well as contextual advertising (2.5.6.). We will further take a look at consent under the influence of subscription models, like pay-or-okay (2.5.7.), as well as co-regulatory initiatives evolving from

[159] Fouad/ Santos/ Laperdrix, The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, PoPETS 2024, p. 450.

[160] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 138.

cooperations between state and private stakeholders (2.5.8). The chapter concludes with an outlook on developments that may, however, also counteract a more effective implementation of data protection requirements through power concentrations by quasi-monopolies and AI (2.5.9).

2.5.1 Personal Information Management Services: Whose interests do the designs of PIMS reflect?

Personal Information Management Systems (PIMS) aim to help data subjects manage their personal data. Such assistance may take the form of central login solutions, central consent management services or solutions for the central exercise of data subject rights (such as data access, data correction and data deletion). The aim in each case is therefore to provide an overview and reduce the effort that would otherwise be required for the data subject to separately log in to various websites and give their consent or to exercise their data subject rights each time again.[161]

However, centralisation also makes it possible for providers of PIMS to use the service itself as an identifier to track the data subjects across websites and services, to obtain their consent more easily or to make it more difficult for them to exercise their data subject rights. Whether a PIMS really protects the interests of consumers or actually pursues the interests of the various industrial competitors, therefore depends on who the service provider is or – less actor-oriented and more facts-oriented – how the respective service is specifically designed. Against this background, we currently observe three different interest groups that offer PIMS and where the interests could manifest themselves in different designs.

2.5.1.1 Solutions provided by the European industry

The first group includes providers that represent the interests of European traditional media companies and telecommunications providers. An example of the former is the NetID Foundation, which offers the single sign-on service NetID.[162] The NetID Foundation is an association of European media companies that aimed to create a European alternative to the American single sign-on solutions from Facebook, Google and others. If a user signs into a service of a partner of the NetID Foundation using an email address of one of the (equally) partnering email providers, the user can use this login, a so-called NetID, for signing into all other partner services. On this basis, a user can control, centrally, either in her email account or on the platform of NetID itself, which data usage rights she wants to remove, eventually, from which partner companies. Thus, the NetID claims to facilitate the management of data usage rights providing the users for a central portal for the management of these rights. In any case, even if the NetID is organised by a (not-for-profit) foundation, its members are driven by their (for-profit) goal to get the users' consent for their tracking and online advertising purposes. Due to the interests of its members, the question arises as to whether the NetID Foundation is shaping the NetID designs in favour of its own interests rather than the interests of consumers. Of course, this question cannot be analysed in detail here. At the very least, it might be assumed that NetID does not go beyond the current best practice rules, which, as described above, have been proven not to represent effective consent processes for those affected.

[161] EDPS, Personal Information Management Systems, TechDispatch 3/2020.

[162] See for the following explanation at https://netid.de/.

An example in the telecommunications sector is Utiq (during its test phase known as TrustPID). Since its merger approval by the European Commission on 10 February 2023,[163] Utiq is operated as a joint venture by the leading European telecommunications companies Deutsche Telekom, Vodafone, Telefónica and Orange.[164] Utiq offers an Ad ID solution primarily for mobile browsing to supplement conventional tracking mechanisms. In doing so, the telecommunications providers aim to fill a gap left, in particular, by the announcements of OS and browser providers to significantly restrict tracking by third-party cookies. When users open a website via their smartphone, an additional banner is displayed, asking for consent to involve the users telecommunications provider as well as subsequent tracking processes. In the case that users agree, Utiq (or the publisher) forwards the visitors IP-address to the respective telecommunications provider, who subsequently identifies the subscriber (incl. its phone number). By using this complementary knowledge that only telecommunications providers are able to connect with the IP-address, the provider generates a pseudonymous identifier (called network signal) that can be permanently linked to the website visitor, regardless of (the lifespan of) any cookies. The telecommunications provider forwards the network signal to Utiq who uses it to create two further IDs, which Utiq passes on to its customers. Utiq enables participating publishers to create profiles of users that can either be used to personalise advertising or to tailor websites. The difference between the two IDs lies in their lifespan - the advertising ID remains valid for 24 hours, the website personalisation ID for 90 days.[165] The involvement of telecommunications providers and subsequent personalisation processes take place across all websites visited by the user that use Utiq's tracking service. Similar to NetID, users basically benefit if they only have to give consent once for tracking on many different websites. As with NetID, the question arises as to whether Utiq is shaping the designs in favour of its own interests rather than the interests of consumers, due to the interests of the providers. Of course, this question cannot be analysed in detail here either. At the very least, it appears that the designs do not go beyond the current best practice rule.

Utiq´s approach of involving telecommunications providers has already been criticised for different reasons.[166] Due to their unique position at the interface to the public telecommunications network and their contractual relationship with the subscriber, telecommunications providers have complementary knowledge that no actor in the advertising ecosystem has. The processing of this knowledge regarding the connection between IP-address and subscriber is generally subject to a special relationship of trust as well as strict requirements under telecommunication law. Therefore, it is already doubtful on the merits, whether this position is compatible with advertising related tracking.[167] Beyond that, it has already been noted that the information text in the Utiq consent banner uses a very positive framing, which could make it unclear to inexperienced users that Utiq, like other tracking methods, is used to track and profile the users online behaviour. At present, there is also a lack of detailed descriptions of all data flows within the Utiq system, which is all the more crucial to fully understand, as it

[163] European Commission, press release, 10.2.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_721.

[164] See in more detail https://utiq.com/.

[165] Dachwitz, Neue Tracking-Firma Utiq: Wie Telekom, o2 und Vodafone im Datengeschäft mitmischen, Netzpolitik, 15.5.2024.

[166] D64, Utiq unter der Lupe: Zukunft des Trackings oder Bedrohung für die digitale Privatsphäre?, Mai 2024.

[167] BfDI, FAQ zu TrustPID: “Andererseits kommt gerade Telekommunikationsanbietern eine besondere Vertrauensstellung zu, die für die BfDI nur schwer mit einem Tracking ihrer Nutzerinnen und Nutzer vereinbar ist.”, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/FAQ-TrustPID.html.

includes pre-processes that significantly differs from the current advertising system.[168] Finally, Utiq is (so far) just a system that supplements conventional tracking mechanisms, but (by now) does not preclude that “normal” cookie banners are still displayed to users on every website.

2.5.1.2 Solutions provided by the Silicon Valley industry

The second group includes solutions that are being driven forward by browser providers. These solutions are characterised by the fact that, like the first group, they also purport to give users control. However, at least in the case of market-dominating browsers, the aim behind this appears to not only give their users control, but also eliminate competitors. This comes to the benefit of users in that the browser providers are not primarily concerned with obtaining data for their own purposes with this consent. The consent mechanism is usually designed in such a way that users are hardly encouraged to make a real decision and therefore tend not to give their consent. However, this design does not imply that users should really make such a decision. Rather, it benefits the browser providers when users refuse their consent, because this means that their competitors in the advertising market are not allowed to collect data about users. One example is the new feature introduced by Apple, with which the iPhone browser Safari can delete annoying content on websites, such as cookie banners. The browser then simply hides the cookie banner, whereby all requested consent is deemed to have been refused.[169] Recently, Google has announced a similar function. After the long-announced Third Party Cookie Phase Out was ordered by the British competition authority to pause because of several related competition concerns, Google will now leave it to the users of its Chrome browser to block third-party cookies via a central consent form.[170] Here, too, at least in view of the interests involved, it is unlikely that the design of the consent form will aim to enable users to make a genuine balancing decision.

2.5.1.3 Solutions coming from civil society and science

Finally, in the third group, we categorise approaches that come from civil society or science. These approaches currently show the most promising specific designs, given their consumer-oriented or scientifically neutral objectives. However, most of them only exist as a proof of concept or at least have not yet found widespread use. An early example is the many approaches that have emerged from the My Data Movement (see in particular the My Data Operator approaches).[171] A more recent example, specifically for consent agents, is the Advanced Data Protection Control developed by the University of Vienna together with the not-for-profit organisation Noyb.[172] Here, at least a technical specification exists, however, the solution so far only exists as a proof of concept. Further examples are the research projects SolidLab Flanders[173] as well as Secure in Data Traffic (SiD)[174] at the Alexander von Humboldt Institute for Internet and Society in Berlin, which builds upon ADPC. Here there are already some developed

[168] D64, Utiq unter der Lupe: Zukunft des Trackings oder Bedrohung für die digitale Privatsphäre?, Mai 2024, pp. 6 et seq.

[169] Geiger, iPhone-Funktion erstaunt, Chip, 15.9.2024, https://www.chip.de/news/iPhone-Funktion-erstaunt-Neues-iOS-18-Feature-raeumt-den-Bildschirm-auf_185407846.html.

[170] Chavez, A new path for Privacy Sandbox on the web, 22.7.2024.

[171] For more details see https://mydata.org/.

[172] https://noyb.eu/de/neues-browser-signal-koennte-cookie-banner-ueberfluessig-machen.

[173] https://solidlab.be/.

[174] https://www.hiig.de/project/sid/.

applications in specific areas. However, they are not yet widespread enough to solve the problem across the board.

A decisive disadvantage that these civil society initiatives have compared to solutions from the industry is that they are dependent on the cooperation of the industrial actors from the advertising ecosystem, such as publishers, browser and advertising service providers. This is because there is a certain risk that these economic players will not cooperate with the civil society initiatives voluntarily. Even the most ambitious **PIMS may only work if the other actors along the data value chain provide the technical and organisational pre-conditions to document and share the information necessary for more effective transparency and control measures and to monitor compliance among themselves**. The industrial solutions do not have this problem, as they already provide this co-operation, whether in the form of collaborations, as in the case of the NetID Foundation or Utiq, or in the form of quasi-monopolies based on their horizontal and vertical integration of the various stages of the value chain. Civil society initiatives, on the other hand, still have to do the necessary work to convince publishers to voluntarily accept the signals from their PIMS and for browsers to voluntarily transmit these signals. For further details on the German regulation on PIMS, which – after pressure by the online industry – only provides a voluntary participation instead of an obligation when it comes to the forwarding and consideration of signals from consent agents, see chapter 3.2.4.1.

2.5.2 Server Side Tracking: Who controls who collects which data for which purposes?

As with PIMS, the question of who has control over server side tracking is ultimately about who controls who collects what data for what purposes and, if necessary, forwards it to third parties. However, server-side tracking is about control of the underlying technology that may be used to collect data in the first place. The conflict over this control takes place between the browser provider on the one hand and the publisher on the other.

The concept of server side tracking dates back to the 1990s and the beginnings of web analytics. Despite the technical possibilities, the method was not popular for a long time because it is more complex and therefore more expensive than its counterpart, the client side tracking. The changing environment, such as the growing awareness of users and the increasing prosecution of data protection violations, have led to a paradigm shift.[175] In August 2020 Google introduced its first tool using server side tracking, namely a new version of their Tag Manager, which led to growing popularity of the method.

When visiting a website using **client side tracking**, the browser will load third party resources directly from an external source, meaning that data flows take place directly between the user's browser (the so-called client) and a third-party server, e.g. from an actor from the advertising ecosystem.[176] This data flow generally is easy to detect by opening the network traffic analysis within a browser, which shows every connection to third-party servers when a website is called up (provided that no measures have been taken to cover up the source, e.g. through CNAME cloaking).

[175] Fouad/ Santos/ Laperdrix, The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, PoPETS 2024, p. 450.

[176] In more detail including figures, see Fouad/ Santos/ Laperdrix, The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, PoPETS 2024, p. 452.

With **server side tracking**, an instance is interposed into the data stream so that data does not flow directly from the user's browser to a third party, but through a tunnel called proxy. Tracking events will therefore only be sent to the third-party server indirectly. Server side tracking can be used in different variants, namely as server side tracking with a third-party proxy or server side tracking with a first-party-collector, where the transport tunnel is self-operated by the visited website.

The proxy has the effect that third parties from the advertising system don't have access to all data of a user, but only those made accessible via the proxy. If data is shortened, aggregated or similar on its way through the proxy, it is less possible for the third party to (re-)identify and profile the user. Ultimately, what is at stake with server side tracking is a shift in technical control regarding which data is collected by whom, for what purposes and in what way, and forwarded to third parties: from the user's browser to the website visited by the user (or the third party proxy). However, a recent university study demonstrates how server side tracking entails non-compliant practices, inter alia lack of transparency as well as a rising number of website operators abusing the technology to pass third party content as first party.[177]

Whether server side tracking represents a gain for the user's privacy protection (or represents a loss of control for the user) depends on the specific design used by the publisher (or third party proxy). The conversion of formerly very clear tracking requests, which were executed by the browser on the client side, into masked and hidden requests on the server side has, on the one hand, a data protection-friendly effect. Likewise it becomes more complicated for users to protect themselves, because the method is suitable for bypassing browser restrictions. Common blocking tools are not adapted to this hidden form of tracking and won't recognize requests via the proxy as third party content. For regulators, it likewise gets harder to verify and audit who's performing tracking in the background.

2.5.3 Cohort-based personalisation (“Synthetic audiences”): Minimised privacy insights, same risk of manipulation

Discussions about advertising based on cohorts or on “synthetic audiences” often give the impression that no personal data is being processed and that therefore no data protection risks will arise.[178] In fact, however, these methods only reduce the insights into the behaviour of the users being observed to create interest profiles. This is already a major benefit for these users. However, cohort-based advertising cannot prevent the other risks from arising, such as being manipulated or discriminated against or suffering health or financial disadvantages; these risks just arise for another group of users.

Cohort-based advertising separates the phases of data collection and analysis on the one hand and the attribution of the inferred buying interests to specific consumers on the other, therefore affecting two basically different groups of data subjects. As said, the first group consists of consumers whose behaviour is observed and analysed. However, cohort-based advertising does not create profiles of individual consumers, but instead statistical interest groups, so-called cohorts. Based on cross-consumer observation and statistical analysis, these cohorts assign certain typified characteristics of observed consumers to certain purchasing interests. For example, consumers who buy book A are likely to also buy book B; or newcomers to Prenzlauer Berg between

[177] Fouad/ Santos/ Laperdrix, The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, PoPETS 2024, pp. 450, 458 et seq.

[178] See for example, the White Paper by Emetriq at https://www.emetriq.com/wp-content/uploads/2024/03/EMQ-Whitepaper-Synthetic-Audience-240313.pdf.

the ages of 25 and 40 with a medium to high income are likely to buy latte macchiato. As the observation data is aggregated statistically, the insights into the private lives of the observed consumers are therefore limited. If the processing procedures are designed properly, the risk of someone else gaining access to the observation data may actually be fairly low.[179]

However, cohort-based advertising should not obscure the fact that the attribution of these statistical interest profiles to specific consumers, i.e. potential buyers, now poses a risk to the fundamental rights of these other consumers. Of course, the attribution of interests on the basis of observed characteristics of this second consumer group is, in principle, less intrusive than the creation of real profiles about them. For example, the observation that a consumer who buys book A is also likely to buy book B provides little insight into the private life of this consumer. However, the second aforementioned example shows that the insights may go further, depending on

- how many characteristics of the second consumer group are used to attribute the statistical attributes to them (in the example, the new place of residence, age and income),
- how comprehensive the attributed characteristics are and
- how much this information affects the social, private or intimate sphere.

In this context, it also does not matter that the attributed interests are only based on probability calculations. This is because it does not come down to whether this information is true or not when it comes to the protection of personality rights safeguarded by the right to privacy. For a person's need for privacy it is irrelevant whether the information that another person reveals about her private life is true or not (see also the right to correct false data, which would otherwise come to nothing).

In addition to the right to privacy, cohort-based advertising also poses a risk of being manipulated or discriminated against or suffering health or financial disadvantages; as mentioned before. The main effect of cohort-based advertising therefore is to reduce the risk for the consumers’ private life. However, this is a very good start.

2.5.4 Interest-based personalisation (incl. enhanced user controls): Google’s Topics for Chrome

Since 2019 Google has kept the industry in suspense with announcements like “we will soon block the use of third-party cookies in the Chromium browser”[180] and plans to “phase out” third-party cookies in Chrome.[181] Many stakeholders within the advertising industry raised concerns that this could have a negative impact on the way that ads are targeted and measured. However, Google provided reassurances that its Privacy Sandbox Initiative would “sustain a healthy, ad-supported web in a way that will render third-party cookies obsolete”.

The Privacy Sandbox Initiative includes a number of proposals. Google´s first public effort to go beyond classical tracking based on cookies has been the Federated Learning of Cohorts (FLoC), a cohort-based approach. In FLoC, users are clustered in cohorts according to the interests inferred by each user´s browser based on the user's

[179] However, see the criticism below that ignited on Google's cohort-based sales FLoC because it apparently came with both a certain risk of re-identification and a weak statistical accuracy.

[180] Schuh, Building a More Private Web, Google Blog, 22.8.2019.

[181] Schuh, Building a More Private Web: A Path towards Making Third Party Cookies Obsolete, Chromium Blog, 14.1.2020.

recent activity. When visiting a website, third parties were offered the user´s cohort, which presents information on the interests of the cohort. Supporters emphasised that this solution would prevent tracking, as every user was „hidden" in his or her cohort. However, critics argued that while a user could hide inside a cohort for a short period of time, the sequence of cohorts they belonged to could work as an increasingly unique identifier over time.[182] As a response to the criticism towards FLoC, Google retired the project and presented a new proposal in January 2022 called Topics.[183]

The Topics API also does not require the storage of cookies on end devices but analyses the browsing history of users at the end of each week to infer interests based on the websites that a user visited. For this purpose, the Topics API assigns certain topics from a taxonomy, which currently includes around 469 topics, to each crawled website based on its hostname. In a second step, the browser observes which websites the user visits and which of the topics associated with the website the user is obviously interested in for a week at a time. In this way, the five most relevant topics for a user are determined each week. One topic is then randomly selected from these five topics and made available to advertisers (alongside other measures designed to further reduce the probability of a user being identified). Advertisers may now choose from the pool of interests that Google assigns to all its users week after week, the interests under which they think they will achieve the highest user interest in their advertising. Topics stores the interests assigned to individual users for only three weeks, after that deletes the interests, and the assignment process starts all over again. Furthermore, users may up-rank and down-rank the interests assigned to them, delete them and also switch off Topics altogether.[184]

Topics in general received positive feedback from various stakeholders,[185] even if there were also prominent critics for both privacy and competition reasons, of course.[186] Among others the system has been recognized as „having the potential to become the new standard for behavioural advertising".[187] However, latest studies and evaluations raise concerns about the offered privacy guarantees.[188] Based on real browsing traces some studies demonstrate that Topics API algorithm mitigates but cannot prevent re-identification.[189]

Meanwhile the organisation NOYB filed a complaint with the Austrian data protection authority in June 2024 regarding the Topics API.[190] The complainant considers it misleading when Google calls the system a „Privacy"-tool.[191] NOYB admits that Chrome

[182] Rescorla/ Thomson, Technical Comments on FLoC Privacy, 10.6.2021.

[183] Jha/ Trevisan/ Leonardi/ Mellia, On the Robustness of Topics API to a Re-Identification Attack, PoPETs 2023, p. 76.

[184] For more details see https://developers.google.com/privacy-sandbox/private-advertising/topics?hl=de.

[185] Muttach/ Köppel/ Hornung, Google Topics als Ausweg aus dem Cookie Dilemma?, CR 2023, 644, para. 62.

[186] Claburn, Shot down: Google's grand fancy plan for pro-privacy targeted ads, The Register 18.1.2023; Schräer, Google und Aufsichtsbehörden ignorieren Kritik an Cookie-Ersatz Topics, Heise Online, 19.1.2023; Wolford, Google's Privacy Sandbox is privacy quicksand, Proton Blog 30.11.2023.

[187] Jha/ Trevisan/ Leonardi/ Mellia, On the Robustness of Topics API to a Re-Identification Attack, PoPETs 2023, p. 66.

[188] Thomson, A Privacy Analysis of Google's Topics Proposal, 6.1.2023; Alvim/ Fernandes/ McIver/ Nunes, The Privacy-Utility Trade-off in the Topics API, CCS 2024, with reference to further studies.

[189] Beugin/ McDaniel, Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving), PoPETs 2024, pp. 1 et seq.; Beugin/ McDaniel, A Public and Reproducible Assessment of the Topics API on Real Data, SPW 2024, p. 5; Jha/ Trevisan/ Leonardi/ Mellia, On the Robustness of Topics API to a Re-Identification Attack, PoPETs 2023, pp. 67 et seq.: the authors assume a re-identification rate of 15-17% for users in a pool of 1000, but point out that the attack time of several weeks required for this makes the scenario impractical.

[190] NOYB, complaint no. C-083, 13.6.2024, https://noyb.eu/sites/default/files/2024-06/Google%20Sandbox%20Complaint%20DE_geschw%C3%A4rzt.pdf.

[191] Klosowski, How to turn off google's privacy sandbox ad tracking – and why you should, Electronic Frontier Foundation, 28.9.2023.

browsers indeed block some third-party cookies now – but other browsers such as Safari from Apple and Firefox from Mozilla have done so by default already since 2017 resp. 2019.[192] According to NOYB the system behind Topics still tracks a user's browsing history for targeted advertising. The most important change seems to be that this is only done by the browser of one company (Google) and no longer by countless third-party tracking systems.[193]

As with purely cohort-based advertising, the mixed-methods applied with Google's Topics approach cannot eliminate the emergence of data protection risks. But it may reduce the risks for the right to privacy by limiting the profiles of users to certain topics (instead of collecting the raw data, namely the users' behaviour on the websites), stores these topics only for three weeks and only shares part of this knowledge with advertising partners. Topics API still creates interest profiles of individual users, but to a significantly lesser extent than before. In addition, Topics also reduces the other risks such as manipulation and, to some extent, discrimination, as well as health and financial disadvantages, by allowing users to upvote and downvote the topics that are suggested to them, delete them, or switch off Topics as a whole.

2.5.5 Encrypted and aggregated conversion measurement: Mozilla's Privacy-Preserving Attribution for Firefox

Finally, since July 2024 Mozilla offers a feature for its Firefox browser called Privacy-Preserving Attribution (PPA). The technology doesn´t serve for the actual process of personalising advertising, but for measuring the success of personalised advertising. There are various indicators for measuring the success of advertising, of which only reach, number of impressions, number of clicks and number of conversions are mentioned here.[194] In order to measure the number of conversions, i.e. how many users clicked on an advert and then performed an action on the target website that is relevant for the advertiser (e.g. actually purchased the advertised item), it is necessary to observe a user's specific reaction to the advert.

To minimise the intrusion into users' private lives regarding the conversion rate, Mozilla's PPA takes three steps: First, when a user interacts with an ad or advertiser, an event is logged in the browser about the details (e.g. viewed, clicked, purchased) and subsequently encrypted using the Distributed Aggregation Protocol (DAP) on a Mozilla server. Second, the encrypted conversion data is then aggregated with encrypted data of other users who, from the advertiser's point of view, have similar characteristics. Third, noise is added to the aggregated data using the differential privacy model to further reduce the probability of individual users in this data being identified. It is only in this form that the reports are given to the advertising partners, who may use them to measure the success of their advertising.[195]

In this scenario the recipient can no longer draw conclusions about individual users. However, the PPA was immediately subject to criticism. Firstly because it is switched on by default when updating the Firefox browser, which is why the organisation NOYB

[192] Wolford, Google's Privacy Sandbox is privacy quicksand, Proton Blog 30.11.2023; Jha/ Trevisan/ Leonardi/ Mellia, On the Robustness of Topics API to a Re-Identification Attack, PoPETs 2023, p. 66.

[193] Klosowski, How to turn off google's privacy sandbox ad tracking – and why you should, Electronic Frontier Foundation, 28.9.2023.

[194] See the different key parameters at https://www.netzdenke.de/blog/online-marketing/erfolgsmessung-im-online-marketing-diese-kennzahlen-solltest-du-kennen/.

[195] Tiwari, Privacy-Preserving Attribution: Testing for a New Era of Privacy in Digital Advertising, Mozilla Blog, 22.8.2024.

– filed a complaint with the Austrian DPA in September 2024.[196] And secondly because user data leaves the computer onto the aggregation server which – depending on a wider or narrower definition – serves as part of an advertising network.[197]

As with the other technologies described, PPA does not prevent the personalisation of advertising and thus the processing of personal data. On the contrary, the technique helps to measure the success of personalised advertising. However, PPA does this in a way that minimises the insights that would arise from this measurement.

2.5.6 Contextual advertising in its various forms: It's a matter of definition

Contextual advertising in its most basic form pursues the approach to reduce the privacy impact of digital advertising by targeting ads based purely on content being viewed - without using personal data of the individual viewing the content.

Most commonly this is done either by an analysis based on URL embeddings.[198] Or by identifying specific keywords within the content using linguistic methods in order to correctly classify contexts of meaning. For this method specific algorithms recognize and analyse the content with the help of databases and determine the main topics. Both methods aim to place thematically appropriate advertising when a user is dealing with the relevant topic.

Some hoped contextual advertising ist the cure for privacy-invasive advertising since the method might eliminate the need for cookies, identifiers and processing of other personal data.[199] Especially as examples have already been reported in which website operators have even increased their revenue with context-based advertising.[200] However, in practice the privacy benefits of contextual advertising is questionable, because no standard industry definition exists - sometimes industry players simply label it as “not behavioral/ non-personalised”.[201] In consequence, a lot of methods that are described as contextual advertising often do involve the processing of personal data. Hence the term is used for a kind of „privacy-washing“. Some critics even claim that advertisers and others use “browser and page-level data, device data, IP address, location data and whatever other info they can get their hands on to model the potential user, framing it as “contextual 2.0.”[202]

A similar phenomenon is known with „audience measurement“, a term which was often used to give tracking methods the appearance of being harmless and non-invasive. In fact, however, this term is so vague and indeterminate that inter alia the German data protection authorities have refused to assess the use of audience measurement.[203] The

[196] NOYB, complaint no. C-089, 25.9.2024, https://noyb.eu/sites/default/files/2024-09/C089%20Firefox%20Beschwerde%20Redacted.pdf.

[197] Förster, Für Werbung: Firefox sammelt ab sofort standardmäßig Nutzerdaten, Heise,15.7.2024; Förster, Firefox verteidigt sich: Alles richtig gemacht, nur schlecht kommuniziert, Heise, 16.7.2024.

[198] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 142, 143.

[199] Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy Press, 26.9.2023.

[200] Deutschlandfunk Nova, Auf Cookies verzichtet – trotzdem viel Geld mit Online-Werbung verdient, 6.8.2020.

[201] For an overview of different approaches of definition and the evolving understanding of the term, see Bleier, On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web, 2021, pp. 8 et seq; AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 141, 142.

[202] Hercher, The Royal Rumble Is On For Who Wins Contextual Advertising, AdExchanger, 13.2.2023.

[203] DSK, Orientierungshilfe Telemedien, 2022, para. 85.

term audience measurement originates from the age of analog media and press and since then has developed into an audience analysis with an undefined scope that might be supplemented by various criteria using numerous, often individualised information. A determination of the lawfulness of audience measurement within a digital service can at best be made for a precisely defined configuration and purpose.

The same issues apply to (the term) contextual advertising. Without a comprehensive and up-to-date definition of contextual advertising the privacy benefits of contextual advertising are limited. In fact there have been attempts to narrow down the meaning and conditions of contextual advertising. One example is a public report of the US Federal Trade Commission (FTC) from 2009 in which the authority has taken a stand on the definition of contextual advertising. The FTC endorsed the industry's interpretation as the „delivery of ads based upon a consumer's current visit to a single web page or a single search query, without the collection and retention of data about the consumer's online activities over time".[204] At the same time the FTC stressed that where a practice involves the collection and retention of consumer data for future purposes beyond the immediate delivery of an ad or search result, the practice does not constitute contextual advertising.

In its opinion 1/2010 the EDPBs predecessor, the Art. 29 Working Party, referred to contextual advertising as "advertising that is selected based on the content currently being viewed by the data subject. In the case of a search engine, content may be derived from the search keywords, the previous search query or the user's IP address if it indicates their likely geographical location".[205] According to the Working Party it´s a kind of advertising that (only) uses 'snap shots' of what data subjects view or do on a particular web site.

Both definitions were already questionable at the time they were published, as they did not categorically exclude the processing of personal data. This not only left space for the claim that session data is not about tracking, but only about the active session and usage at one point in time.[206] Moreover it has given some market players, such as Uber, the leeway to claim that even location-based targeting is considered contextual.[207] In light of the technical advancements and evolving market practices, not least due to the use of advanced AI analysis (see chapter 2.2.5.), these definitions are outdated in any case.

Rather than analysing one article at a time or one single URL, by using AI driven tools advertisers can analyse a vast range of content and URLs and profile it along very finely tuned classification schemes. The possibilities arising from this have fueled a trend towards neuroprogrammatic advertising. While contextual advertising in the narrower sense means matching ads to content based on topics, neuroprogrammatic advertising contextually targets ads based on emotion and a granular understanding of the moods of the audiences they want to reach. By using natural language processing neuroprogrammatic can categorise the feelings in an ad and the sentiments of the

[204] FTC Staff Report, Self-Regulatory Principles for Online Behavioral Advertising, February 2009, p. 30.

[205] Art. 29 Working Party, Opinion 2/2010 on online behavioural advertising, p. 5; it seems the Art. 20 Working Party put contextual advertising on the same level as segmented advertising, meaning "advertising based on known characteristics of the data subject (age, sex, location, etc.), which the data subject has provided at the sign up or registration stage".

[206] Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based "Behavioral" Advertising?, Tech Policy Press, 26.9.2023.

[207] Schiff, When Does Contextual Targeting Cross The Line Into Something … Else?, AdExchanger, 28.8.2023.

content the audience consumes and subsequently pair ads to emotional contexts that make emotional and topical sense.[208]

To sum up, contextual targeting is a promising alternative to personalised advertising not only because it is privacy-oriented. Nevertheless, if contextual data is used as a proxy for (sometimes sensitive) personal data, people are still profiled and monitored, not based on what they do, but the content they view.[209] Thus, the method can be more manipulative and privacy invasive as it seems, just thinking about contextual ads on weight loss programs placed alongside content related to dieting and eating disorders.

2.5.7 Consent under the influence of subscriptions: Pay-or-okay models and potential social consequences

Another development that began a few years ago in the German media sector and has since been copied throughout further industries all over Europe is noteworthy are so-called pay-or-okay models. These models, also called consent-or-pay models, are strictly speaking no privacy-preserving solution in favour of users, but an approach by the industry to solve the issue of the voluntary nature of consent as a legal basis for personalised advertising or, more fundamentally, the financing of media content on the internet.

The EDPB defines the phenomenon of pay-or-okay models “as models where a controller offers data subjects a choice between at least two options in order to gain access to an online service that the controller provides: the data subject can 1) consent to the processing of their personal data for a specified purpose, or 2) decide to pay a fee and gain access to the online service without their personal data being processed for such purpose”.[210]

The background to this development is the headwind that the common design of banners has experienced since 2018. After the GDPR came into force and following rulings by national courts[211] and the ECJ[212], supervisory authorities and plaintiffs in civil actions[213] have increasingly questioned the validity of consent for advertising-related processes gained via website banners. In case it is more complicated to refuse consent in such a banner than to accept it, inter alia by hiding the reject button on a second visual level, then ultimately it is not possible to gain voluntary and unambiguous consent with it.[214]

The discussion originates from an economic problem regarding digital services, in particular the media industry. The media industry has traditionally financed the production of its content and technologies on two pillars: on the one hand, through a usage fee and, on the other, through advertising. This was already the case in the offline world, but with the internet there were two developments: First, most content providers made their content available for free, so that the financing of this content was limited to advertising revenue. Second, however, with technical development,

[208] Cantu, Neuroprogrammatic Is the Future of Contextual Advertising, AdMonsters, 19.4.2023.

[209] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 141.

[210] EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, para. 14.

[211] German Federal Court of Justice, 28.5.2020, I ZR 7/16 – Cookie-Einwilligung II (Planet49).

[212] ECJ, 1.10.2019, C-673/17 - Planet 49.

[213] See as an example Regional Court Munich,29.11.2022, 33 O 14776/10 - focus.de.

[214] See inter alia EDPB, Report of the work undertaken by the Cookie Banner Taskforce, 2023, para. 6 et seq.; DSK, Orientierungshilfe Telemedien, 2022, para. 48 and 54 et seq.; for further publications regarding cookie banner design, see footnote 140.

advertising increasingly relied on personalisation and thus on the processing of personal data. This development brought data protection law into play and, in particular, made it necessary to obtain the consent of consumers. Either the media industry obtains valid consent, charges a usage fee again or finds completely new ways of financing their content. The pay-or-okay model was subsequently developed with the above-mentioned requirements for effective consent in mind.

The Datenschutzkonferenz (DSK), a committee consisting of all German supervisory authorities, were the first to comment on the pay-or-okay model and emphasised the requirements for valid consent when using subscription models. Inter alia the DSK has clarified that if there are several processing purposes that differ significantly from one another, the requirements for voluntary consent must be met to the effect that consent can be given on a granular basis. This means, among other things, that users must be able to actively select the individual purposes for which consent is to be obtained (opt-in). Only if purposes are very closely related can a bundling of purposes be considered. A blanket overall consent for different purposes - as an alternative to the subscription - is not suitable to obtain valid consent.[215]

Starting in August 2021, the organisation NOYB filed complaints with various German as well as the Austrian supervisory authority regarding seven media websites, stating that users cannot freely decide whether to consent, but must take out a subscription if they do not want to.[216] NOYB inter alia refers to a statement from the industry, according to which 99.9% of visitors agree to tracking if they are confronted with a fee of 1.99 Euro.[217] Saying "no" is not only time-consuming (since users need to disclose name, address and credit card details), but also unreasonable costly: According to NOYB users would sometimes have to pay ten, twenty or a hundred times as much to stop their data being passed on, than publishers earn with personalised advertising. This makes it highly questionable if it is about a fair alternative to consent or selling expensive subscriptions: "Many media companies have surrendered to the whims and standards of the advertising technology industry. They sell their readers' data and their trust for a few cents. The big profits go to the advertising technology industry - just like the data*"*.[218]

While some aspects have already been dealt with by the authorities (the Austrian DPA ruled that in the specific case the consent lacked granularity, as it was not possible to select yes or no for each data processing operation[219]), the financial aspect is still subject of debates. Here, the question arises as to whether the pay-or-okay-model will lead to data protection becoming a privilege of the wealthy in society as a whole, i.e. for those who can afford it financially.

Starting from German-language media websites, the use of such pay-or-okay models has spread to other sectors (weather services, databases for recipes etc.) and member states.[220] Ultimately Meta also introduced this model in November 2023 for Facebook

[215] DSK, Bewertung von Pur-Abo-Modellen auf Websites, 2023, p. 2.

[216] NOYB, press release, 13.8.2021, https://noyb.eu/de/news-seiten-leserinnen-sollen-eigene-daten-zum-wucherpreis-zurueckkaufen.

[217] NOYB, press release, 28.11.2023, https://noyb.eu/de/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay.

[218] NOYB, press release, 13.8.2021, https://noyb.eu/de/news-seiten-leserinnen-sollen-eigene-daten-zum-wucherpreis-zurueckkaufen.

[219] Austrian DPA, 29.3.2023, D124.4574 2023-0.174.027, https://noyb.eu/sites/default/files/2023-04/Standard_Bescheid_geschw%C3%A4rzt.pdf.

[220] At the same time, the first civil lawsuits for damages arise, Regional Court Regensburg, 15.4.2024, 75 O 1040/23.

and Instagram,[221] followed by an EDPB Opinion on valid consent in the context of pay models implemented by large online platforms.[222] The EDPB considers that, in most cases, it will not be possible for such platforms to comply with the requirements for valid consent, if they confront users only with a choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

Currently, the use of the model by Meta is subject of an investigation by the European Commission, which so far assumes that the design of the subscription model does not allow for voluntary consent and (since Meta is a gatekeeper under the Digital Markets Act) violates Art. 5 sect. 2 DMA (see chapter 3.6.3.). It remains to be seen how the proceedings will end and whether the reasoning will undermine the model as a whole.[223]

On top of that, even if the lack of granularity and unreasonable pricing were resolved, a current study shows that publishers do not even deliver what they promise. The collection of data from 341 websites and subsequent analysis showed that while websites reduce tracking for paying users, 32.9% of the websites fail to uphold the privacy promise declared in their cookie banner.[224]

Ultimately, 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).

2.5.8 Co-Regulation: Voluntary commitments, public initiatives, certifications & codes of conduct

In addition to the developments described above, which are emerging more or less voluntarily from the economy, civil society or research, a few co-regulatory approaches should also be mentioned. In contrast to purely voluntary or self-regulatory initiatives (like the TCF, see chapter 2.2.4.), co-regulatory initiatives are characterised by the fact that they emerge through cooperation between public authorities and private actors, be it that public authorities initiate them or at least play a major role in shaping them for example by accrediting them.[225]

2.5.8.1 Cookie Pledge Initiative and Good Practice Initiative for Cookie Consent Management

Among these, the **Cookie Pledge Initiative**[226] at EU level and the **Good Practice Initiative for Cookie Consent Management**[227] in Germany are particularly relevant for the present report. As in the two examples mentioned, voluntary commitments are informal interactions that are usually initiated by the state and that the private actors

[221] The introduction of the pay-or-okay model within Metas services had been preceded by measures taken by the Irish supervisory authority, as Meta did (respectively planned) to base advertising-related processes on the performance of contracts (respectively its legitimate interests).

[222] EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.

[223] For a comprehensive analysis of Metas subscription model, see also D'Amico/ Pelekis/ Santos/ Duivenvoorde, Meta's Pay-or-Okay Model - An analysis under EU Data Protection, Consumer and Competition Law, TechReg 2024.

[224] Müller-Tribbensee, Privacy Promise Vs. Tracking Reality in Pay-or-Tracking Walls, APF 2024, pp. 173 et seq.

[225] See Voßkuhle/ Eifert/ Möllers/ *Eifert*, § 19 Regulierungsstrategien, E.) cip. 52 et seq.

[226] See, in more detail, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en; Pfeiffer/Muttach, EU-Kommission: Initiative zur freiwilligen Cookie-Selbstverpflichtung, ZD-Aktuell 2024, 01520.

[227] ConPolicy, Good Practice Initiative for Cookie Banner Consent Management - Design Guidelines, 26.1.2023.

making the commitments use in an effort to avert formal state regulation. Both initiatives are relevant for this report for two reasons: **Firstly, both initiatives failed**, i.e. the voluntary commitments were either not taken up at all or at least not by all the important stakeholders. Such a failure often results in the state reacting with a formal regulatory initiative. For such a possible formal regulatory initiative, the present report aims to identify various regulatory options.

The second reason is even more important for this study. **On closer inspection, even these state-initiated approaches are only partially suitable for effectively addressing the regulatory deficits**, i.e. the problems described above. In line with the objectives of the cookie pledge initiative, the eight draft pledging principles can be categorised into three categories: 1) simplify consumer choices (principles A, E and F); 2) reduce the cookie fatigue (principles G and H); and 3) enable consumers to clearly decide for or against advertising-based models (principles B, C and D).[228]

Even though these principles contain numerous important specifications to enable consumers to make an informed decision, the principles cannot completely resolve the problems described above with respect to the ineffective implementation of consent. This is important to emphasise, because the success of the voluntary commitment or of a corresponding formal regulation would in all likelihood make these specifications the benchmark that hardly any actor would exceed. The effectiveness of consent would thus be fixed at the level set by these principles.

In practice, this would lead to the following three shortcomings: First, the principles seem to suggest that their implementation should enable consumers to reject consent as easily as possible. This is at least suggested by the wording in principle H, that ‘Consumers should have their say if they decide that they want to systematically refuse certain types of advertising models” (underlining by the authors of this study). Commissioner Reynders' stated the aim of respecting “the wish of the majority of consumers not to be tracked for advertising purposes” goes in the same direction. Thus, **it seems that the primary concern of the principles is to enable consumers to easily refuse consent, rather than to make a genuine decision for or against the benefits and risks** of personalised advertising. This tendency may also be the reason why the industry has not adopted the principles. However, according to the rationale of the law, it is not simply a matter of enabling consumers to simply refuse consent (which Reynders seems to assume), but rather consumers should be able to make real decisions in favor of or against the processing of their data for the specific purposes.[229] This is in line with numerous empirical studies, according to which consumers would like to be able to better assess the benefits against the risks of the respective processing purpose, and according to which consumers increasingly decide in favor of one or the other purpose the better they understand the respective benefit-risk ratio for themselves (see in more detail in chapter 4).

Secondly, **the principles seem to use the business model of personalised advertising as a proxy for consumers**, on the basis of which they are to be able to recognise the consequences of giving their consent. This lumps together all variants of personalised or tracking-based advertising, regardless of the specific risks and benefits for the consumers, and only distinguishes it from non-tracking-based advertising. However, the above analysis has not only shown that there are meanwhile numerous

[228] See European Commission, Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, Discussion Paper for Stakeholders´ Roundtable, p. 2.

[229] See Masing, Herausforderungen des Datenschutzes, 2012.

differences in the way tracking and personalisation are carried out and the risks (and advantages in terms of relevance for consumers) that they may entail. Empirical studies furthermore suggest that these differences are important, if not crucial, for consumers when deciding whether or not to consent to one or another type of personalised advertising (see chapter 4.4.1.). The implementation of the principles are thus **threatening to freeze development** in the direction of even more data protection-friendly methods at the current level, insofar as advertisers or publishers no longer seem to be able to present differences in their methods to consumers. A success of the Cookie Pledge Initiative would therefore likely have meant that the industry would have lost any incentive to develop privacy-enhancing technologies and thereby reduce the risks of their processing operations for consumers. The examples given above show that even in the current situation, which is not perceived as very satisfactory (see chapter 2), the industry itself has such incentives and is developing risk-reducing technologies. In chapters 4 and 5, we will present regulatory options that will significantly strengthen these incentives to further lower the risks for consumers.

Finally, a third weakness of the principles leads in a similar direction. Although the principles contain numerous specifications, they are far from exhaustive. There is still a great deal of leeway in terms of how exactly the consent forms are designed, both textually and visually. Not only do data protection authorities now provide a great deal of guidance in this regard, going far beyond the Cookie Pledge principles.[230] Even if the Cookie Pledge principles referred to the application of these regulatory requirements, the scope will never be fully utilised. The principles therefore lack two essential prerequisites for ensuring the effective design of consent processes also in the long term: Firstly, the principles **do not contain any requirements that ensure** or at least clarify that and **how the designs of consent processes are adapted to technological developments in the best possible way** to protect against the risks; **and** secondly, **there are no guidelines or clarifications on how the actors involved in the data processing processes must cooperate** so that all necessary information is passed on along the data value chain and the conditions of consent are complied with (see above chapter 2.4.2.). However, both requirements are essential for the effective design of consent processes. As long as no such specification or clarification is made, it can be assumed that the design of consent processes will remain at the level laid down in the principles, i.e. far from ensuring truly effective protection.

The **Good Practice Initiative for Cookie Consent Management** of the German Federal Ministry of Justice and Consumer Protection goes, on the one hand, beyond the Cookie Pledge Principles, but on the other hand, also falls short of them, and for the rest, suffers from the same deficits. On the other hand, they also fall short of the cookie pledge principles because they do not specify how to overcome consent fatigue (e.g. by integrating PIMS). In particular, the initiative does not require any empirical methods to ensure the effectiveness of the consent processes. The aforementioned recent quantitative study showed that even a cookie banner created according to the guidelines of the Good Practice Initiative for Cookie Consent Management provides only limited information about the risks of data processing, so that it may hardly be regarded as effective consent.[231] This is not to say that these initiatives were wrong in the first place, on the contrary. But in order for these initiatives to have a better effect, at least in favour of consumers, **interdisciplinary methods should be applied** more

[230] See footnote 140.

[231] Grassl/ Gerber/ v. Grafenstein, How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights?, EDPL 2024, pp. 96 et seq.

consistently here. For consent banners to be more effective, it is simply not enough to apply purely legal methods. Rather, these legal methods must be combined with methods from visual design, user experience design and empirical social sciences.[232]

As mentioned initially, both initiatives did not achieve the commitment of all necessary stakeholders anyway. And even if this commitment had been achieved, the requirements would only have made a limited contribution to a significant improvement since the guidelines have no binding effect. This issue has also been identified in a recent study to support the fitness check of EU consumer law on digital fairness that has been prepared for the European Commission. The authors of this fitness check therefore recommended for additional legislative guidance on how to avoid common pitfalls in website and interface design leading to dark patterns.[233]

2.5.8.2 Altruistic consent form according to Art. 25 sect. 1 Data Governance Act

Using the right methods is extremely important, especially if the state, be it the European Commission, national ministries or data protection authorities, should not only develop binding guidelines but also technical and organisational solutions themselves. One example here may be the **altruistic consent form** for which the European Commission is authorised. According to Art. 25 sect. 1 Data Governance Act (DGA), “the Commission shall adopt implementing acts *establishing and developing* a European data altruism consent form” in order to “facilitate the collection of data based on data altruism”.

Indeed, Art. 25 DGA only refers to the “sharing of data (…) for **objectives of general interest as provided for in national law**, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest”. However, as with the state-led Cookie Pledge Initiative, there is a reasonable concern that the basic consent design and the underlying methods will be used as a benchmark for the design of consent in other areas as well, such as personalised advertising.

To avoid such a ‘freeze effect’, the competent authority must therefore ensure that it sets the optimal standard for the methodology and the visual, technical and organisational requirements when complying with Art. 25 sect. 1 and Art. 6 sect. 1 GDPR. To this aim, it is essential that the developers address all limitations as analysed in chapter 2.4. providing for the corresponding solutions. The same applies to other technical and organisational solutions, such as anonymisation solutions in the field of data minimisation.[234]

2.5.8.3 Certification schemes and codes of conduct according to Art. 40 et seq. GDPR and Art. 46 DSA

Last but not least, we would also like to mention the **certification programmes and codes of conduct** that Art. 40 et seq. GDPR as well as Art. 46 DSA envisage. These

[232] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review, 2024.

[233] CSES, Study to support the Fitness Check of EU consumer law on digital fairness, 4.10.2024, p. 348.

[234] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 177 et seq.

mechanisms were discussed for some time as a promising mechanism for establishing more legal certainty and a higher level of protection in practice. Unfortunately, these mechanisms have also had little effect so far. At least, a relatively small number of certification programmes have been approved by the relevant authorities to date.[235] An important reason for this is certainly that they are voluntary. Data controllers and processors are free to submit to such mechanisms (and participate in their development) or not. Another reason might be the complicated coordination processes, at least, in Germany. In Germany, the situation is complicated by the fact that another actor, the German Accreditation Body (DAkkS), is authorised to participate in the decision-making process. The different goals of these different bodies as well as the resulting coordination threaten to be so complex that only a few companies might consider the additional legal certainty to be worthwhile. After all, Art. 40 sect. 1 and Art. 42 sect. 1 GDPR contain the requirement that the needs of small and medium-sized enterprises must be taken into account when designing these mechanisms. As it is unclear in what form this should take place, this requirement has not been reflected except in the data protection authorities' fee tables. In summary, it can be said that the online advertising sector will probably avoid these proceedings simply because many companies are counting on the high enforcement deficit anyway. Similarly weak effects are to be expected with Art. 46 DSA, provided that the responsible authorities or the legislator do not take countermeasures.

2.5.9 Aggravation of the risks, especially through power concentrations

2.5.9.1 Accumulation of additional information power by quasi-monopolies

One very complex problem is the increasingly observable trend whereby very large companies are best able to exploit the application of data protection as a competitive advantage, and are increasingly doing so. The problem is complex because different dimensions of protection interact here.[236] Although data protection law was originally conceived as a legal safeguard against the accumulation of information power by the state or by companies that were already strong due to their size and organisational structure, today it is precisely the large companies that benefit more and more from the application of data protection law. There are several reasons for this:

First of all, the larger the company, the better it is able to comply with legal requirements (especially if these are complex and costly to comply with). The reason for this is that they are able to build up the necessary resources to implement the legal requirements. Secondly, the more functions (or services) a company integrates vertically and horizontally, the lower the coordination effort. An illustrative example of this is the TCF. Here, a total of over 600 different players had to coordinate and agree on a common standard in legal, organisational and technical terms. The result is a ‘lowest common denominator’ that almost inevitably falls short of the legal minimum standard. In this respect too, quasi-monopolies, which are characterised by the vertical and horizontal integration of many different functions, have a clear advantage. Silicon Valley companies are a clear example of this. A third aspect that should be emphasised

[235] At the time of publication, five certification schemes are listed in the EDPB's Register of certification mechanisms, seals and marks, two of which are from Germany, https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_de.

[236] EDPS, Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data, 2014, p. 6: “EU approaches to data protection, competition and consumer protection share common goals, including the promotion of growth, innovation and the welfare of individual consumers”.

is that these companies have generally also integrated the end user interface. This not only puts them in a position to monitor end users directly without having to rely on the involvement of third parties. Via the end-user interface, these companies are also able to obtain consent themselves (and for all subsequent data processing steps).[237]

Finally, and this is the most interesting aspect, some companies are using data protection to eliminate competitors. The most obvious example of this is Apple, which has focussed from the outset on offering all services from a single source, thus making it easier for it to guarantee a high level of quality. But other companies, even those that have long promoted the open source and associated community concept, are also making increasing use of this mechanism. This can be illustrated using the latest update of Apple's mobile operating system iOS 18.0 and the operating system macOS Sequoia 15.0 that offers a new feature for ‘Distraction Control’, which allows users to simply block ‘unwanted content’ on websites, such as cookie banners, with a single click in the default settings.[238] Google Chrome has since announced a similar feature that will allow Chrome users to block third-party cookies via a preference setting in the browser.[239] Since this function, announced as a privacy feature, puts competitors in the advertising market in a significantly worse position than Apple or Google itself, it is doubtful whether Apple and Google have the intention of designing these default options in such a way that users can really weigh up the benefits and risks for themselves. Instead, based on the economic interests at stake, it is likely that these default settings are designed to enable users to simply click away cookie banners without understanding the significance of the processing purposes behind consent.

For consumers, this anti-competitive behaviour ultimately becomes relevant in two ways: Firstly, these practices can (and will) lead to even fewer competitors and thus even less competition in terms of privacy-friendly technologies, alongside the already powerful companies.[240] Of course, in view of the dire current situation, one may doubt whether there can or will be any such market dynamics in the direction of privacy-friendly technologies. However, the argument is theoretically valid and the above-mentioned consumer studies show that consumers do make a distinction between more and less privacy-friendly technologies.[241] Secondly, the concentration of economic power also leads to a further accumulation of data and knowledge on the part of the already powerful companies. However, such a further accumulation of information power is exactly what data protection actually wants to prevent.[242]

[237] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 6: „the market power of the large digital firms, which force the consumers to consent“.

[238] Apple, 17.9.2024, https://support.apple.com/en-us/120682.

[239] Chavez, A new path for Privacy Sandbox on the web, 22.7.2024, https://privacysandbox.com/news/privacy-sandbox-update/

[240] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 47; Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 6: „The correct policy conclusions are […] to deal effectively with the economic power of the large digital firms instead of weakening the standards of data protection law“.

[241] Acquisti/ John/ Loewenstein, What Is Privacy Worth?, The Journal of Legal Studies 2013, pp. 249 et seq.; Cisco, Consumer Privacy Survey - Privacy Awareness: Consumers Taking Charge to Protect Personal Information, 2024, pp. 11 et seq.; Cisco, Consumer Privacy Survey - Building Consumer Confidence Through Transparency and Control, 2021, p. 5.

[242] See Pohle, Datenschutz und Technikgestaltung, 2016, p. 253: ”Datenschutz heißt, informationell begründete soziale Macht in der Informationsgesellschaft unter Bedingungen zu stellen, sie zu zwingen, sich zu verantworten, und sie damit (wieder) gesellschaftlich verhandelbar zu machen. Seine Funktion besteht darin, dass kontingente Sozialstrukturen sich auch unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverarbeitung und gegen die „überlegen standardisierende Strukturierungsmacht von Organisationen reproduzieren können”.

2.5.9.2 Aggravation of power concentration through AI

The problem of market concentration is further exacerbated in connection with the use of AI. When looking at the current utilisation of AI in the online advertising market it is crucial to recognize that particularly programmatic advertising has incorporated automation as a fundamental component from the very beginning. The integration of AI-based technologies leads to efficiency gains without having a disruptive effect on learned processes in online advertising (see chapter 2.2.5.).

The development and training of AI-based technologies, for example, for profiling and prediction purposes, largely depends on the amount of available data. Due to exclusive data access, those big actors within the advertising market that operate closed ecosystems with business models designated to create strong incentives for users to share data, are at an advantage compared to publishers and advertisers regarding data availability.

While all players in the advertising ecosystem benefit from AI-driven efficiency gains, the big actors have a better starting point for developing innovative AI solutions. This advantage on the one hand stems from substantial and early investments and development capacities. On the other hand, regulatory challenges lead to an increased barrier to entry in the AI market. While the big actors in the advertising ecosystem have market-leading solutions in all areas of use cases, and a significant advantage in being able to integrate AI solutions directly into their comprehensive advertising services, publishers and advertisers, on the other hand, currently mainly use AI to improve internal process efficiency.

2.5.10 Interims conclusion: remarkable variety of approaches, but no comprehensive solution

Over the last years, numerous approaches have been developed by the industry, civil society and research to evolve methods, techniques and commitments for providing more effective privacy solutions and its technical and organisational pre-conditions. The different approaches each address different risk areas or causes of risks of personalised advertising and function at different technical and organisational levels. In doing so, the approaches highlight the various areas and levels through which the risks described above may be addressed. However, they are far from forming a coherent system that would provide comprehensive and effective protection against the risks of personalised advertising.

Let's start the summary with the initiatives that directly affect the effective organisation of consent processes: These include firstly the state-driven Cookie Pledge initiative at EU level and the Good Practice Initiative for Cookie Consent Management in Germany. Unfortunately, both initiatives had only a limited impact. Of course, both initiatives correctly aim to standardise cookie banners, increase transparency and, in some cases, even combat consent fatigue. However, both initiatives did not achieve the commitment of all stakeholders involved on a voluntary basis. And even if this commitment had been achieved, the requirements would only have made a limited contribution to a significant improvement in effective transparency and user control. One reason for this is due to the fact that the guidelines have no binding effect. Another reason is that they are far from exhaustive and, in particular, do not contain any specification or clarification on how to ensure that the consent processes are as effective as possible in view of the technical development. Due to these deficits, the initiatives threaten to practically fix a level of protection that has already been proven to be ineffective.

PIMS are another important initiative because with their help consumers have more space, more time and more attention available to process the information and exercise their controls. Most importantly, the consumer is no longer forced to give their consent on every single website they visit, which avoids the resulting consent fatigue. But here it comes down to whose interests the specific design of a PIMS reflects, those of the European media industry who try to collect as many consents as possible, those of quasi-monopolies from Silicon Valley who also use data protection and their "users' control" at least to eliminate their competitors, or really those of consumers. Less focused on the interests of the different actors and more on the specific design, clear metrics and methods are needed to ensure that PIMS enable consumers to make informed balancing decisions about the benefits and risks that are associated with consenting to personalised advertising. The most promising approaches currently appear to be those developed by civil society and researchers, even if these currently only exist as proof of concepts and prototypes in certain areas.

The pay-or-okay models that have recently become increasingly widespread are being discussed controversially, at least to the extent that they call into question the voluntary nature of consent. This model may even prove to be detrimental to effective control. Indeed, based on a pay-or-okay model, the individual consumer has a clear choice between paid website content without personalised advertising and free website content in return for personalised advertising. Consumers may also hardly expect to always receive such content or services on the internet free of charge, since they have to pay for media content and services alike as well in the offline world. However, the question arises as to whether this will lead to data protection becoming a privilege of the wealthy in society as a whole, i.e. for those who can afford it financially. Here again, this risk 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).

As far as the technical and organisational pre-conditions for more effective transparency and user control measures are concerned, the various approaches highlight the different areas and modes of operation. Server side tracking is actually primarily about the question of who controls who collects what data for what purposes and discloses it to whom: the publisher or the user's browser? Since the publisher does not necessarily have less (or does have even more) interest in collecting the personal data of its visitors than the provider of a browser, this change in control may hardly be considered as a privacy preserving technology.

The same applies to cohort-based personalisation of advertising (or personalisation based on 'synthetic audiences'). Here, the debate often overlooks the fact that the statistical interest profiles generated in this way are ultimately also assigned to individual consumers, causing the risks of manipulation, discrimination and health and financial disadvantages typical of personalised advertising. Nevertheless, cohort-based advertising may contribute to a significant reduction in insights into consumers' private lives, at least in comparison to the classic profile-based personalisation of advertising.

Mozilla's PPA for the firefox browser is ultimately a form of encrypted and aggregated performance measurement for personalised advertising. It is therefore only one, albeit very important and in our opinion convincing, component in a more data protection-friendly online advertising ecosystem. The most comprehensive approach is probably Google's Privacy Sandbox, although we have only focussed on one of several components here, namely the Topics API. The Topics API is characterised by several privacy-enhancing features: Topics API still creates interest profiles of individual users, but to a significantly lesser extent than before. Furthermore, compared to the practice of the TCF, Google only releases a considerably smaller proportion of these profiles to its advertising partners. Last but not least, Topics also reduces the other risks such as manipulation and, to some extent, discrimination, as well as health and financial disadvantages, by allowing users to upvote and downvote the topics that are suggested to them, delete them, or switch off Topics as a whole. The Topics API is indeed a major step forward. However, as with most other privacy-friendly technologies of the quasi-monopolies from Silicon Valley, it is accompanied by a considerable disadvantage for the competitors on the online advertising market and a corresponding increase in information power in favour of the quasi-monopolies. From a consumer perspective, this further economic concentration of power leads to a smaller range of products for consumers. This will be particularly relevant in terms of data protection law if, at some point in the future, the hoped-for competition in favour of constantly data protection-friendly advertising services should actually materialise. Furthermore, this resulting increase in information power asymmetries is actually what data protection wants to prevent. In this respect, we will therefore ultimately speak of a ‘from the frying pan into the fire’ phenomenon.

These information power asymmetries are likely to become even stronger in the future due to the use of AI in the area of personalised advertising. Even if the European economy and economic policy still saw AI as an opportunity to make up for lost ground in the field of digitalisation, it is becoming increasingly clear that it is actually only a matter of not being completely left out of the digital economy race. As the development of AI generally requires massive investment and its use is increasingly being deployed in the hyperscaling clouds of the Silicon Valley companies, it is very likely that these quasi-monopolies will accumulate even more information power through the use of AI.

Ultimately the use of AI also plays its part when assessing the – supposedly – least intrusive method to personalise ads, namely contextual advertising. While it is indeed a promising alternative that is worth taking a closer look at from a regulatory perspective, it is no sure-fire success since the understanding of “contextual” has been highly blurred by the industry. Only in its most basic form, which means without using personal data of the individual viewing content, this method constitutes a solution to escape several problems and risks posed by personalised advertising, not only for users but also advertisers and publishers. Nevertheless, even “zero data” methods are not automatically and absolutely risk-free for users since AI driven tools enable very finely tuned context schemes leading to new methods with profiling effects.

With this in mind, we cautiously conclude that comprehensive protection against the risks of personalised advertising is most likely to be provided by the big tech companies if (we are aware: once again) the European legislator does not step in. As such comprehensive protection by the Big Tech companies will ultimately lead to a further increase in their already enormous economic and information power asymmetries, we cannot help but clearly recommend appropriate legislative steps. Because, at least from a data protection perspective, this further increase of economic and informational power asymmetries is exactly what consumer and data protection actually wants to prevent.[243] Instead of reducing data protection overall – because the risks are far too great for that, at least in the area of personalised advertising (see above in chapter 2) – the aim should therefore be to specify and, if necessary, supplement the existing data protection law in such a way that its application does not lead to a further concentration of information power, but to an actual containment of such information power and the resulting risks for consumers and society as a whole (including fair competition).

2.6 CONCLUSION: THE COMPLEXITY AND RISKS OF THE ONLINE ADVERTISING ECOSYSTEM DEMANDS A CROSS-DATA PROCESSING AND CROSS-ACTORS REGULATORY FRAMEWORK

The current ecosystem of personalised online advertising is very complex; on closer inspection, the underlying data processes and even payment flows appear messy and chaotic. The risks are correspondingly numerous and severe, both for individuals and for society as a whole. The current situation from a consumer perspective, especially with regard to the effectiveness of consent, is – there is no other way to put it – catastrophic.

In view of the risks discussed among experts, the consumer perceptions, and the conceptual and practical limits of consent, it almost seems obvious to abandon the regulatory focus on consent and replace it with a ban on personalised advertising altogether. On the other hand, such a ban would leave out the heterogeneous privacy attitudes of consumers completely and the fact that on an individual basis they theoretically see added value in the personalisation of advertising, provided that this would really make the advertising more relevant to them. Thus, consent might, at least for certain areas, function as an appropriate regulatory instrument (for solutions on this conflicting field of protection and interests see chapter 5).

In fact, due to the increased awareness of these risks and the associated legislative improvements, numerous approaches have been observed in industry, civil society and research in recent years that aim to both create these technical and organisational pre-conditions and improve the design of consent in favour of consumers. However, these approaches still seem rather eclectic when viewed as a whole. Thus, they do not reveal a systemic approach that spans all data processing phases and actors, which is necessary for a comprehensive and effective addressing of the aforementioned risks.

Although the IAB Europe appears to be pursuing such an overarching approach with its TCF, as a voluntary initiative it is thrown back to the best possible compromise of all its participants. However, these participants of the TCF are only industry representatives and not consumer or data protection representatives. Therefore, this industry standard falls short of the consumers' need for protection and, correspondingly, of legal expectations. So far, only the big tech companies appear to be in a position to provide such comprehensive protection due to their own end-user interface, horizontal and vertical integration of the various advertising services and their gatekeeper function. However, this would in turn lead to a further increase of the already large economic and information power asymmetries in favour of these quasi-monopolies – what consumer and data protection laws actually seek to prevent.

Therefore, it seems reasonable to establish the needed systemic approach across (personal) data processing phases and actors by means of a regulatory framework.

[243] See Pohle, Datenschutz und Technikgestaltung, 2016, p. 253.

However, before we propose the essential building blocks of such a regulatory framework, we have to take a closer look at the current legal situation.

3 REGULATORY APPROACHES

Usually, the lawfulness of personalised advertising is dealt with as a data protection issue, since the lifecycle of such ads is based on a large range of data processing operations, in particular matching a user's specific characteristics after a profile has been created by observing the individual's interaction with digital content and combining, analysing and sharing their personal data. However, data protection legislation is only a piece of the puzzle when it comes to the regulatory framework applicable to such practices.[244]

As presented below, a handful of other EU laws include provisions aiming at regulating personalised advertising aspects beyond data protection law, including the ePrivacy Regulation, the AI Act, the Political Targeting Regulation, the Digital Services and Digital Markets Act. In this chapter, the report turns to the regulatory aspects by raising the following questions: To what extent does existing law provide suitable building blocks to adequately protect consumers from the risks described above? What gaps and problems still exist? Which regulatory approaches or elements might be transferred from other laws to close these gaps or solve these problems?

To answer these questions, this chapter draws on the previous results, in particular from the analysis of individual and societal risks, and examines the current legal situation on the basis of three sub-questions or criteria:

1) To what extent do current laws provide effective individual-subjective rights for consumers to protect their individual – and, as a possible consequence, societal – interests from the aforementioned risks?

2) To what extent do the current laws place structural-objective obligations on the various actors operating in the area of personalised advertising in order to effectively protect consumers and societal positions from the stated risks?

3) To whom do the current laws assign the responsibility to guarantee these subjective rights and objective obligations, and how effectively is this assignment of responsibility being realised in current advertising practice?

These questions are answered in brief for each individual law we identified as relevant in the context of the advertising ecosystem. In doing so, we occasionally refer to similar or alternative regulatory approaches in order to highlight the deficits of the current laws and pinpoint possible solutions. Interestingly, an analysis of the laws reveals a learning curve on the part of the legislator. With the GDPR, the legislator has created a law that is not only comprehensive but also flexible and can theoretically be effectively applied to the online advertising sector. However, due to the high level of legal uncertainty, the complexity of the online advertising ecosystem and the lack of enforcement, the GDPR is proving to be almost ineffective in online advertising practice. Against this background, the following actor-, technology- and sector-specific laws can be read as a reaction to these uncertainties through increasingly specific requirements not only at the legal level, but also at the technical and organisational level.

[244] Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice, EuCML 2023, p. 243.

3.1 EU GENERAL DATA PROTECTION REGULATION

3.1.1. Scope of application and regulatory objective

The General Data Protection Regulation (GDPR) regulates the processing of personal data, i.e. information that relates to an identified or identifiable person (Art. 4 no. 1 GDPR). In this context, processing means any operation, whether or not by automated means, from the collection of personal data, to its storage, further processing and disclosure, and finally to its deletion (Art. 4 no. 2 GDPR). The primary regulatory goal of the GDPR is to protect individuals (referred to as data subjects) from the risks of data processing, or more precisely, to prevent uncontrolled, non-transparent and non-intervenable data processing from undermining the autonomous exercise of their fundamental rights (Art. 1 sect. 1 and Art. 24 GDPR).[245]

With respect to personalised advertising, this means that all its possible processing phases constitutes the processing of personal data: from observing consumers, i.e. data subjects, across different devices and social contexts, collecting information about their behaviour in all these contexts, creating profiles of possible buying interests based on this data, aggregating this data into statistical interest cohorts and classifying consumers into such interest cohorts, up to displaying online advertising based on these interests. The requirements of the GDPR for the processing of personal data aim at protecting data subjects from such insights into their private life, ensuring that they are able to make autonomous purchasing decisions, are not discriminated against, and do not suffer financial harm or health damage (see above chapter 2.3.1.). So far, the data protection assessment of personalised advertising is straightforward. However, challenges in applying the GDPR arise when it comes to the question of what risks are actually present in a specific case or phase of the processing, and who is actually supposed to protect the data subjects from these risks and how exactly.

3.1.2. Objective obligations, subjective rights and responsibilities

To protect consumers against the risks, the GDPR establishes an arsenal of objective requirements and subjective data subject rights.[246] The objective-structural requirements include, among other things, specifying and documenting the purpose of the data processing (Art. 5 sect. 1 lit. b and Art. 30 GDPR), making this purpose transparent to the data subjects (Art. 5 sect. 1 lit. a and Art. 12 et seq. GDPR), designing the processing procedure lawfully (Art. 5 sect. 1 lit. a and Art. 6 et seq. GDPR) and fairly by providing them with options for intervention (Art. 5 sect. 1 lit. a and Art. 16 et seq. GDPR), using the data adequate and accurate (Art. 5 sect. 1 lit. c, d and e GDPR) and not for other purposes if these are incompatible with the original purpose (Art. 5 sect. 1 lit. b and Art. 6 sect. 4 GDPR) and securing the data against respective misuse (Art. 5 sect. 1 lit. f and Art. 32 GDPR). In turn, on the basis of their intervention rights, the data subjects may, depending on the case, refuse to consent to the processing or revoke their consent (Art. 7 and 8 GDPR), object to the processing (Art. 21 GDPR), access the data collected (Art. 15 GDPR), correct it (Art. 16 GDPR) and/or delete it (Art. 17 GDPR). Last but not least, the GDPR also regulates who is responsible for applying the aforementioned data subjects rights and objective obligations. However, all these obligations are, unfortunately, quite ineffectively implemented in practice, if at all.

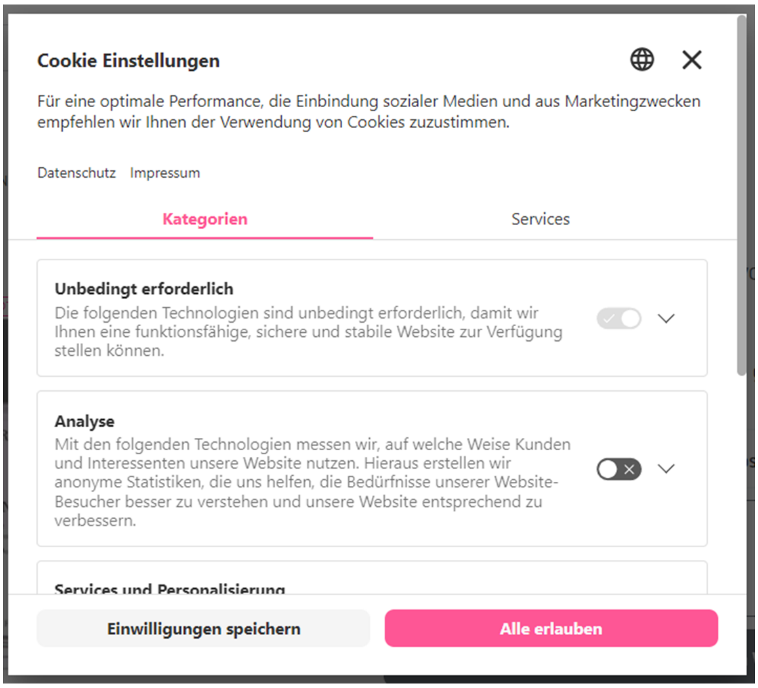
[245] Regarding the conceptual underpinning, see for example, v.Grafenstein, Refining the concept of the right to data protection in Article 8 ECFR – Part II, EDPL 2021, pp. 195 et seq.

[246] See Bieker, The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law, 2022.

3.1.2.1 Purpose specification and transparency

Ambiguities in the implementation of these provisions begin with the specification of the processing purposes. Purpose specification (combined with purpose compatibility, see in more detail below) is one of the cornerstones of data protection law.[247] The conceptual debate recognised early on that with the advent of IT, the relevance of data can no longer be judged solely on the basis of the type and context of its collection, but that relevance depends above all on the manner and purpose of its use. For this reason, many, if not most, of the other legal requirements are organised around the correct specification of the purpose.[248] For data subjects, purpose specification combined with the transparency and purpose compatibility requirements ensures that they can assess whether they find the processing of their data appropriate or objectionable.[249] For this reason, it is decisive for the effective protection of data subjects that the controller specifies its purposes of the data processing correctly. However, this is where the central problem arises in practice.

In the context of personalised advertising, it is remarkable how differently purposes are defined and described. The spectrum becomes visible if you simply place a few common consent banners (that do not participate in the TCF). For example, the two banners below come from different websites that are not related. The publishers use the same CMP, same colour, same sizing etc. In all likelihood, they also process the visitors personal data for the same purposes in order to personalise advertising. Nevertheless, the specification of the three purposes is not identical in a single point:



Cookie Einstellungen

Für eine optimale Performance, die Einbindung sozialer Medien und aus Marketingzwecken empfehlen wir Ihnen der Verwendung von Cookies zuzustimmen.

Unbedingt erforderlich
Die folgenden Technologien sind unbedingt erforderlich, damit wir Ihnen eine funktionsfähige, sichere und stabile Website zur Verfügung stellen können.

Analyse
Mit den folgenden Technologien messen wir, auf welche Weise Kunden und Interessenten unsere Website nutzen. Hieraus erstellen wir anonyme Statistiken, die uns helfen, die Bedürfnisse unserer Website-Besucher besser zu verstehen und unsere Website entsprechend zu verbessern.

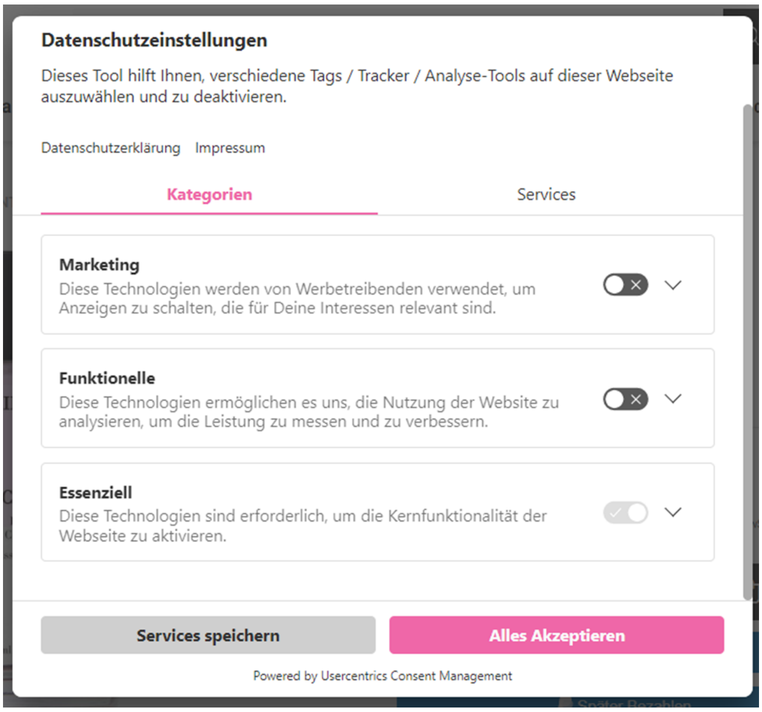
Services und Personalisierung

Figure 3: Cookie Banner 1

[247] Bygrave, Core Principles of Data Privacy Law, Data Privacy Law: An International Perspective, 2014.

[248] V. Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I: EDPL 2020, p. 513.

[249] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, pp. 11 et seq.



Datenschutzeinstellungen

Dieses Tool hilft Ihnen, verschiedene Tags / Tracker / Analyse-Tools auf dieser Webseite auszuwählen und zu deaktivieren.

Datenschutzerklärung Impressum

Marketing ○
Diese Technologien werden von Werbetreibenden verwendet, um Anzeigen zu schalten, die für Deine Interessen relevant sind.

Funktionelle ○
Diese Technologien ermöglichen es uns, die Nutzung der Website zu analysieren, um die Leistung zu messen und zu verbessern.

Essenziell ●
Diese Technologien sind erforderlich, um die Kernfunktionalität der Webseite zu aktivieren.

Figure 4: Cookie Banner 2

Is there a difference between “unbedingt erforderlich” (absolutely necessary) and “essenziell”, between “Analyse” and “Funktionelle” or between “Services and Personalisierung” and “Marketing”? And apart from that, what does marketing actually mean?

If the term is interpreted in favour of the consumer, it refers only to the compilation of marketing statistics. In fact, however, the term also covers the display of advertising, not only on the basis of such statistics, but even personalised on the basis of individual advertising profiles. This distinction is important because each of the three sub-purposes mentioned above threatens the autonomous exercise of the fundamental rights of the data subjects with varying degrees of intensity: The creation of (marketing) statistics only carries, in principle, a relatively low risk that other people will gain insights into the purchasing behaviour of the data subjects. However, when advertising is displayed, there is an added risk of manipulation of the data subject's purchasing decision. Finally, advertising is displayed in a personalised manner, this is based on relatively extensive personality profiles with significantly increased insights into the data subject’s private life and a much higher risk of manipulation.[250] Accordingly, the legal requirements of these different forms of ‘marketing’ vary and data subjects may assess them differently.

As early as 2013 the EDPB´s predecessor, the Article 29 Working Party, already emphasised that “a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', [...] will - without more detail - usually not meet the criteria of being ‘specific’.[...] In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required. The fact that the information must be precise does not mean that longer, more detailed specifications are always necessary or helpful. Indeed, a detailed description

[250] Cf., for example, Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, pp. 5 et seq.

may at times even be counter-productive".[251] In order not to be accused of "vagueness", the industry has reacted to this with so-called purpose hierarchies or cascades. At the top of such a cascade is a relatively broadly formulated purpose, which is then further and further differentiated. The most exaggerated example for such a purpose cascade is the TCF that currently differentiates 19 different (sub)purposes (see chapter 2.2.4.2.). This approach is not to be criticised per se, even the Art. 29 Working Party recommends layered notices. Nevertheless it is questionable which of the main or sub-purposes must be made explicit to the data subjects in what exact manner so that they can assess the consequences of the data processing for themselves.

The industry usually falls back on claiming that the GDPR is too vague and there is too little guidance by the authorities when it comes to specifying purposes, which is why there is uncertainty about differentiating them. 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.

In general, the problem of legal uncertainty is evident in various parts of the GDPR and will in some cases lead to years of legal clarification proceedings. Vague legal terms and requirements for consideration are part of the regulatory model chosen by the legislator.[252] The flexibility achieved in this way is justified in view of the rapid pace of technical developments, especially since it can lead to greater justice in individual cases. However, the uniformity of application of the law, which is also desired by the legislator, can only be achieved if there are sufficient specifications.

In principle, this need has been recognized by the legislator, which is why the EDPB has been instructed in Art. 70 sect. 1 lit. d-m GDPR to issue guidelines, recommendations and best practices on procedures. However, the guidelines often remain at a superficial level, leaving (too) much leeway in practice. At the same time, it often takes a long time to finalise them, not least due to lengthy coordination processes between the parties involved. It is rightly criticised that the resulting need for clarification of legal issues by authorities and courts takes too long, partly because the authorities are too reluctant to enforce potential violations and therefore it takes time for more court decisions to be issued. One consequence of this is the existence of many legal grey areas that are exploited by controllers and ultimately tolerated by the authorities.[253] In order for the GDPR to be effectively enforced and to avoid creating facts through practice that can only be reversed with great effort, it is imperative that the EDPB and the supervisory authorities provide specific guidance – in due time. This is a decisive factor for the success of the GDPR.[254]

3.1.2.2 Legal basis: From contract to consent

Art. 6 sect. 1 GDPR governs that six different legal bases can legitimise the processing of personal data. These are all of equal significance and are not ranked in order of importance. However, in the context of personalised advertising, only three of them are of practical relevance: A data subject has given consent to the processing of his or her personal data for one or more specific purposes (Art. 6 sect. 1 lit. a GDPR), the processing is necessary for the performance of a contract (Art. 6 sect. 1 lit. b GDPR) or

[251] Art. 29 Working Party, Opinion 03/2013 on purpose limitation, pp. 15 et seq.

[252] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 97.

[253] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 38.

[254] Simitis/ Hornung/ Spiecker gen. Döhmann/ *Schiedermair*, Art. 70 GDPR, para. 8.

the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (Art. 6 sect. 1 lit. f GDPR).

There have been major disputes about which of these legal bases can be considered in connection with personalised advertising. Due to the various formal requirements for the validity of consent and its more cumbersome opt-in procedure for data subjects the industry has an interest to circumvent consent as legal basis and instead favour the contract or legitimate interests as the legal basis,[255] since here the data subjects can generally only object to the processing of their data (‘opt-out’), which in effect considerably expands the data controller's ability to process the data. In contrast, the data protection authorities generally seem to consider consent with its opt-in process to be the only correct legal basis also for low risk purposes, such as for statistics for website improvement.[256] The ECJ has confirmed this requirement at least for the processing of personal data for marketing purposes, without distinguishing more precisely between the possible sub-purposes mentioned above.[257]

The legal basis chosen makes a considerable difference for consumers, not only because they have different options for avoiding the processing of their data in specific cases. The categorisation also has a significant impact on how many consents consumers have to click on or off every day. To counteract consent fatigue, a differentiated approach would therefore be preferable, which sets stricter requirements for the decision-making process of the consumers, the more risks are associated with the processing purposes, and vice versa.

With respect to the design of consent in the form of cookie banners, the authorities meanwhile provided several guidelines on how these are to be designed.[258] Nevertheless, such guidelines are not suitable but also not intended to ultimately clear out all ambiguities, since the possible application scenarios are too diverse. One particular challenge here is that these guidelines must also remain open to future developments. Another challenge is of a methodological nature; in order to be able to make more specific design proposals, they themselves would have to be able to provide the necessary interdisciplinary concepts, methods and processes, i.e. the corresponding personnel (see above chapter 2.4.). Indeed, most data protection authorities already have numerous IT specialists in their departments alongside lawyers. However, additional staff with knowledge of textual, visual and user experience design as well as social and behavioural sciences are currently (at best) in the process of being recruited. One decisive reason for this is the limited financial resources (see also chapter 3.1.3.1. on reasons for enforcement deficits within the authorities).

3.1.2.3 Data minimisation and accuracy

The GDPR provides controllers to use personal data limited to what is necessary in relation to the purposes for which they are processed and accurately according to Art. 5 sect. 1 lit. c and d GDPR. The principle of data minimisation requires the controller to limit the collection of personal data in question to what is strictly necessary in the light

[255] See, for example, in ECJ, 4.7.2023, C-252/21 para. 86 et seq. - Meta vs Bundeskartellamt.

[256] See footnote 140.

[257] ECJ, 1.10.2019, C-673/17 - Planet 49.

[258] See footnote 140.

of the objective of the envisaged processing.[259] This requirement applies on various levels, inter alia, to the amount of personal data collected, the extent of their processing and the period of their storage.[260] In consequence even initially lawful processing of data may over time become incompatible with the GDPR where those data are no longer necessary in the light of the purposes for which they were collected or further processed.[261]

Regarding the use and storage of personal data of users of a social media platform for the purpose of personalised advertising, the ECJ recently emphasised limitations on two levels. Firstly, "the indiscriminate use of all of the personal data held by a social network platform for advertising purposes, irrespective of the level of sensitivity of the data, does not appear to be a proportionate interference with the rights guaranteed by the GDPR to users of that platform".[262] The controller may not engage in the collection of personal data in a generalised and indiscriminate manner and must refrain from collecting data which are not strictly necessary having regard to the purpose of the processing.[263] Secondly, the storage of such data for an unlimited period must be considered to be a disproportionate interference in the rights guaranteed to those users by the GDPR. The court held, such processing is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user and may give rise to the feeling that his or her private life is being continuously monitored.[264]

Accordingly – without uncertainties – the GDPR has mechanisms in place to actually ensure that data within the advertising ecosystem is up to date and only processed to the minimum extent necessary. However, this has not prevented data subjects in the past from, on the one hand, a great deal too much data and, on the other hand, an enormous amount of incorrect data being processed.

An impressive example of this is Xandr, a data management platform owned by Microsoft (formerly known as AppNexus), that maintains extensive advertising profiles with numerous identifiers of millions of consumers.[265] There are clear indications that much of this data is incorrect. In July 2024, the organisation NOYB filed a complaint with the Italian data protection authority against Xandr. NOYB criticised that according to Xandr´s data supplier, the complainant is both male and female and is estimated to be between the ages of 16-19, 20-29, 30-39, 40-49, 50-59 and 60+. He also has an income between €500 - €1,500, €1,500 - €2,500 and €2,500 - €4,000. In addition, the same person is a jobseeker, employed, a student, a pupil and works in a company. This company, in turn, simultaneously employs 1-10, 1,000+, and 1,100-5,000 people.[266] It is hard to imagine how these data categories can be used for accurate

[259] ECJ, 24.2.2022, C-175/20 para. 79 - Valsts ieņēmumu dienests.

[260] ECJ, 4.10.2024, C-446/21 para. 60 - Schrems vs. Meta.

[261] ECJ, 20.10.2022, C-77/21 para. 54 - Digi.

[262] ECJ, 4.10.2024, C-446/21 para. 64 - Schrems vs. Meta.

[263] ECJ, 24.2.2022, C-175/20 para. 74 - Valsts ieņēmumu dienests.

[264] ECJ, 4.10.2024, C-446/21 para. 58, 62 - Schrems vs. Meta; ECJ, 4.7.2023, C-252/21 para. 118 - Meta vs Bundeskartellamt.

[265] Xandr acts on several positions within the ecosystem, including SSP, DSP, AdExchange and cookie sync services, see chapter 2.2.3.

[266] NOYB, complaint no. C-084, 9.7.2024, para. 33, https://noyb.eu/sites/default/files/2024-07/Xandr%20Complaint-EN_redacted.pdf.

advertising targeting. Although the source is not Xandrs' only data supplier, it seems to be very likely that this information is used for advertising targeting.[267]

It is obvious that the chaos described, in the way personal data is organised and stored, is in direct contrast to the principles to continuously maintain the quality of the data and to keep the data relevant and limited to what is necessary for the marketing purposes. It is likely that this case is not an exception in the marketing business, but the rule. In this context, it is important to point out the risks to the fundamental rights of the data subjects if data controllers do not meet the principle of data minimisation and quality. On the one hand, such incorrect data may significantly reduce the risk of manipulation. After all, incorrect data means that the advertising industry does not recognise the actual interests, needs and weaknesses and therefore may not make any convincing or even manipulative offers to buy. The same applies to the risk to the health of the persons concerned and the risk of financial damage, as such advertising is not aimed at actual vulnerabilities or the inclination of the person concerned to pay a higher price. On the other hand, the attribution of false interests etc. to individual consumers interferes with their right to privacy, because it does not matter whether the observation leads to correct or false facts from their private lives. Finally, the risk of discrimination may even be categorised as greater because unequal treatment based on false data can hardly be objectively justified. An excessive or incorrect data basis therefore does not mean that there are no longer any risks to the fundamental rights of the data subjects, but merely that the risks occur differently.

3.1.2.4 Data subject rights

The situation is even more disappointing with regard to the effective implementation of data subject rights. There are numerous studies that show how ineffective or meaningless the implementation of data subject rights is from the perspective of the data subjects.[268]

These are still the positive examples, because in many other cases the rights of data subjects are completely denied. One example is the aforementioned data management platform Xandr. According to NOYB, in the period between January 1, 2022, and December 31, 2022, Xandr received 1,294 access requests and 600 deletion requests – and denied every single one.[269] Xandr justifies this denial with the fact that the data is pseudonymous and therefore cannot identify the data subjects in its data set, although Art. 11 GDPR provides a specific procedure for identifying the data subjects for precisely this purpose.[270] Here too, it is likely that this case only represents the tip of the iceberg in the online advertising ecosystem.

Even where the right to information is granted, there is a lack of knowledge, or even of will, how this right must be provided so that it becomes a meaningful and effective control instrument for the data subject.[271] Based on our own observations in practice,

[267] NOYB, complaint no. C-084, 9.7.2024, para. 34 et seq.

[268] Pins/ Jakobi/ Stevens/ Alizadeh/ Krüger, Finding, getting and understanding: the user journey for the GDPR'S right to access, Behaviour and Information Technology 2022, pp. 2174 et seq. with further references.

[269] NOYB, complaint no. C-084, 9.7.2024, para. 11 et seq.

[270] Lomas, Microsoft-owned adtech Xandr accused of EU privacy breaches, Tech Crunch, 8.7.2024, with further references to the EDPB Guidelines 01/2022 on data subject rights - Right of access.

[271] Cf., also Alizadeh/ Jakobi/ Boldt/ Stevens, GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies, Proceedings of Mensch und Computer 2019, pp. 811 et seq.

we do not currently assume the other data subject rights, such as the right to erasure or data portability, are significantly better implemented.

3.1.2.5 Purpose compatibility, confidentiality and security

The principles of purpose limitation and compatibility, as well as confidentiality and security, are closely related. Ultimately, all these principles are about using technical and organisational measures to prevent data from being used in a way that is incompatible with its original purpose: whether the data is used for other purposes or is no longer available in a form suitable for the original purpose, whether this happens from within or outside the data controller's organisation, through authorised or unauthorised access. In particular, the limitation principle essentially aims to identify risks in good time and implement the necessary protective measures. By effectively implementing the purpose limitation principle, data subjects can be confident that no further risks will arise than were indicated to them before the data was collected. This is important because it is the only way they can reliably decide whether and under what circumstances they agree or disagree with the original collection of their data (see above chapter 2.4.2.3. with further references).

In many cases, as shown previously, effective purpose limitation already fails because the purposes are formulated too broadly. If the data processing purpose is described only with the term ‘marketing’ and the term is not interpreted narrowly in favour of the consumer, the above-described differences in risk cannot be adequately addressed by technical and organisational measures against unauthorised access or use. A second reason why purpose limitation is often only weakly implemented in practice is that the necessary documentation of the original purposes is lacking. If the original purpose is no longer known or has not been sufficiently documented, it may not be possible to verify whether the respective planned or current use is incompatible with this original purpose.[272] Even where the purposes are sufficiently specified and documented, there are often hardly any technical or organisational measures implemented in practice to prevent the use of data in a way that is not compatible with the original purpose of data collection. An example of this again is the TCF, which does not even oblige participating parties to report any misuse, even if they have passed on personal data to a third party and observe such misuse (see above chapter 2.4.2.3.).

3.1.2.6 Data protection by design and security of processing

The previous subchapters have shown that a recurring problem is the uncertainty as to how the generally formulated requirements of the GDPR must be *effectively* implemented in a specific case, such as that of personalised advertising and all its sub-forms. This problem is actually addressed by Art. 24 and 25 GDPR, whereby the latter has a greater significance in supervisory practice, since only Art. 25 GDPR is mentioned in Art. 83 sect. 4, 5 GDPR as directly being subject to a fine. Taking a closer look at Art. 25 GDPR, from a legal point of view the requirement is remarkable in three respects:

- Firstly, Art. 25 sect. 1 GDPR clarifies that an essential building block of effective protection is the appropriate design of the technical and organisational systems both at the moment of data collection and (!) later processing (the existence of legal requirements *per se* is therefore not enough for effective protection);

[272] Forgó/ Krügel/ Rapp, Zwecksetzung und informationelle Gewaltenteilung, 2006, pp. 53 to 58.

- secondly, Art. 25 sect. 1 GDPR demands empirical proof of effective implementation, which needs methods that lawyers have not been genuinely trained for and which they must therefore acquire (either by acquiring it themselves or by collaborating with the corresponding experts) and integrate into their legal thinking and implementation processes;
- thirdly, Art. 25 sect. 1 GDPR aims to create, by referring to the so-called state of the art, a market dynamic towards an even higher level of data protection in practice.

Art. 25 GDPR with its data protection by design approach is the central provision that forces controllers to implement all the provisions of the GDPR in the technical and organisational design of its processing. The requirement is central, not least, to the area of personalised advertising because the requirement clarifies that effective protection requires the appropriate technical-organisational building blocks. The TCF does go in this direction to some extent, by presenting a technical-organisational system for obtaining and passing on consent. However, this system was designed primarily to serve the interests of the advertising industry. As a result, the TCF falls short of the requirements of the GDPR and, in particular, of Art. 25 sect. 1 GDPR, which primarily protect the interests of data subjects. The same conflict of interest in how to design a system specifically can be seen, to a greater or lesser extent, in other technical-organisational building blocks, such as PIMS and other privacy-enhancing technologies as discussed above (see above chapter 2.5.1.).

Against this backdrop, even more interesting is that Art. 25 sect. 1 GDPR requires the controller to implement the legal requirements in a way that *effectively* protects the data subjects from the risks of the specific processing in question. Thus, the controller must provide for an empirical proof of the effectiveness of its implementation. This reference to empirical evidence is legally the most effective approach to ensure that all those phenomena for which there is uncertainty as to how they are to be implemented achieve the regulatory objective: How purposes should be specified so that data subjects can really foresee the consequences; or how opt-in or opt-out mechanisms must be designed so that data subjects can adequately control the risks; what deceptive designs or dark patterns are and what are not. All of this can ultimately be empirically verified using appropriate metrics and methods to determine how effectively they protect data subjects from risks to their fundamental rights. The effectiveness requirement is therefore a suitable mechanism for ensuring that the technical and organisational building blocks are not designed unilaterally in favour of industry, but are actually focused on protecting the interests of the data subjects.

Furthermore, Art. 25 of the GDPR does not only state that the implemented protection must be effective, but rather that the controller must also take into account the state of the art as well as the costs of implementation. This is interesting because the state of the art is understood as the scientifically proven *most effective* implementation of a legal provision that is available on the market.[273] Thus, the controller must additionally consider the most effective implementation available on the market, so to speak, as a benchmark. Briefly said, the controller does not have to implement the most effective implementation available on the market only if the implementation costs are disproportionate.[274] This dynamic reference to the market-development can hence turn

[273] Cf. Martini, Integrierte Regelungsansätze im Immissionsschutzrecht, pp. 210 et seq.

[274] Ehmann/ Selmayr/ *Baumgartner*, Art. 25 GDPR, para. 22.

out to be a powerful legal mechanism to constantly push the data protection level in practice because as soon as someone has advanced the state of the art, everybody else must take it into account.[275]

With these requirements, Art. 25 sect. 1 GDPR is an extremely powerful tool to respond to the practical constraints of informed consent identified above (see chapter 2.4.). The provision supplements and specifies how all provisions of the GDPR must be implemented so that across the entire data value chain: 1) data subjects understand and control the complex processes that provide insights into their private lives; 2) they understand and can effectively control the risks of manipulation, discrimination and material and health damage; and 3) the actors involved in the data processing must coordinate for effective protection so that the protection for data subjects and society as a whole is as effective as possible.

However, in practice, this mechanism runs dry due to a lack of conceptual and methodological knowledge. The EDPB has taken a stance on this matter in its Guidelines 4/2019 on Data Protection by Design and by Default.[276] Unfortunately the opportunity to explore the requirements for proof of effectiveness in greater depth, including the need to provide it empirically was not seized. Beyond that, even if there were more clarity about which methods should be used for effective implementation, controllers require special knowledge in order to meaningfully evaluate the de facto efficiency as well as its state of the art. In fact, very few lawyers have been trained in empirical qualitative and quantitative methods, which may be the greatest challenge for the effective implementation of Art. 25 GDPR in practice.

Understanding this conceptual and methodological problem is extremely important both to achieve effective protection for data subjects and to prevent disproportionate regulatory burdens on data processors. The reason for the former observation is that the risks can only be controlled by designing the technical and organisational processing procedures accordingly if personalised advertising is not to be banned completely. If the processing of personalised data is prohibited, the problem does not arise. In this case, the technical and organisational processes do not need to be adapted at all, but may not be used for personalised advertising in the first place. However, if one attempts to control the risks by designing the data processing processes accordingly, this requires coordination of the actors involved at all data governance levels - legal, technical and organisational. This coordination is highly complex because the various objectives, problems, solutions, methods and processes have to be synchronised.

Understanding this conceptual and methodological problem is also important to prevent disproportionate regulatory burdens on data controllers. Legislators seem to be losing patience time and again (sometimes rightly so). Instead of waiting for the industry to finally adapt its technical and organisational systems, the legislator gives the impression of being able to simply solve the problem with more and more new laws. However, that is not always the case. In view of the comprehensive regulatory approach of the GDPR, new laws only help in many cases insofar as they clarify the

[275] V. Grafenstein, Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the “state of the art” of data protection-by-design, 2022, referring to Gawel, Technologieförderung durch „Stand der Technik“: Bilanz und Perspektiven, 2009, p. 204.

[276] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

legal uncertainties. To do this, these new laws must be harmonised conceptually. Without such harmonisation, however, new laws merely threaten to create additional regulatory pressure without providing effective protection against the risks. New laws must therefore be scrutinised and designed to determine the extent to which they fill actual regulatory gaps or eliminate legal uncertainties. This requires a thorough analysis of existing laws. If it turns out that the risks cannot be contained by further supplementary or more specific requirements, but only by adapting the technical and organisational processing procedures, such an adjustment of the technical and organisational processing procedures should be the focus of all government and societal efforts. This is also what this report attempts to do.

3.1.2.7 Responsibility and accountability

Last but not least, the GDPR also clarifies who is responsible for compliance with these provisions. This is, first of all, the data controller (Art. 5 sect. 2 and 24 GDPR), i.e. the person who determines the purpose and means of the processing (Art. 4 no. 7 GDPR). Insofar as the data controller passes on the data to other recipients, the extent of their responsibility depends on whether they process the data only for the purposes of the controller (e.g. data processors, Art. 28 GDPR) or also process the data for their own purposes (joint controller, Art. 26 GDPR) or completely independently from the first controller (then the receiver is another controller, but independently). In the first case, the processor must support the data controller in fulfilling its duties, and only bear a reduced level of own responsibility. In the second case, the joint controllers must clarify who fulfils which rights and obligations and how, so that the protection for the data subjects is effective.[277]

The GDPR places an obligation on all controllers and processors to document their data processing activities in a processing record, Art. 30 GDPR. This includes, in particular, the types of data processed, the purposes of the processing, the data subjects concerned and the recipients of the data. Such documentation is crucial, not only because it is an important basis for an assessment by the data protection authorities (Art. 30 sect. 4 GDPR), but also because such documentation is a pre-condition for the company's own compliance with subjective rights and objective obligations.[278]

Furthermore, it should be noted that the GDPR addresses only the controller and processor of personal data, not the manufacturer of information technology. This is surprising given that Art. 24, 25 and 32 GDPR oblige the controller to implement all the provisions of the GDPR in the technical and organisational design of its processing activities. In case the controller does not develop the technologies itself, there is a gap between legal responsibility and technological capacity. A draft version of the GDPR has still envisaged producer liability as an additional paragraph in Art. 25 and 32 GDPR. However, under pressure from industry, the European Council later prevailed in the trilogue negotiations and producer liability was deleted.[279] Today, this gap between legal responsibility and technological capacity can only be closed by a market in which IT producers design their IT in such a way that their business customers, i.e. the controllers, could easily comply with the GDPR. In practice, however, this usually results in a cat-and-mouse game, because although the producer promises that its

[277] See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[278] See Art. 29 Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 (5) GDPR.

[279] Sydow/ Marsch/ *Mantz*, Art. 25 GDPR, para 11.

technology can be used in a GDPR-compliant manner, it usually does not want to take responsibility for this.[280] To a lesser extent, the same gap between legal necessity and technical ability exists between controller and processor. On the one hand, Art. 32 GDPR places an equal obligation on the processor and the controller to take security measures, and according to Art. 28 GDPR, the processor must support the controller in implementing the controller's obligations. However, on the other hand, this also results in a game of cat and mouse, whereby the processor does not want to guarantee to the controller that the latter may use the processor's technology in a GDPR-compliant way.

Against this background, it gets clear that the same ambivalences arise with regard to the question of how the various actors in the advertising industry need to coordinate their activities in order to provide effective protection for consumers. Here, it is often not clear whether some of the actors who present themselves as mere processors do not use the data for their own purposes after all.[281] Nor does it seem clear which of the actors is an independent and which is a joint controller and must therefore coordinate with the others when implementing the protective measures.[282] In the current online advertising ecosystem, this question is put to the extreme by the fact that the collaboration between the various actors is extremely complex and encompasses more than hundreds of actors. The lack of clarity ultimately boils down to the fact that the actors do not organise themselves according to the principle of how to achieve most effective protection for the data subjects, but rather how the individual actors can best avoid any protection measures.

The GDPR actually provides several co-regulatory instruments to clarify such legal issues. These include, in particular, codes of conduct and certification mechanisms according to Art. 40 et seq. GDPR. By submitting to such procedures, controllers and processors can demonstrate compliance with the provisions of the GDPR (Art. 24 sect. 3 and Art. 25 sect. 3 as well as Art. 32 sect. 3 GDPR). However, for various reasons, these methods have hardly been used to date, at least in the online advertising ecosystem (see chapter 2.5.8.3.).

3.1.3 Reasons for enforcement deficits

In 2018 there has been great hope that the GDPR brings a new era in taking effective action against international players, large data markets and high-risk businesses that harm data subject rights.[283] Yet, years later there is constant criticism of the authorities´ enforcement practice.[284] Some former supporters even warned that the gap between the law on the books and the law in action appears to be so great that it risked becoming a "fantasy law".[285] In fact, Art. 57 and 84 GDPR provide the data protection authorities (DPAs) with powers that enable them to - supranational - impose very high fines and other incisive measures to enforce the GDPR. With regard to the online

[280] v. Grafenstein, Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework, HIIG Discussion Paper Series, 2022, pp.14 et seq.

[281] See, for example, the case of Facebook Fanpage, however, which has now been clarified by the ECJ, 5.6.2018, C-210/16.

[282] See, for example, the case of the IAB Europe with respect to the TCF, however, which has now been clarified by the ECJ, 7.3.2024, C-604/22.

[283] Golla, Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, JIPITEC 2017, pp. 74 et seq.; Hoofnagle/ van der Sloot/ Zuiderveen Borgesius, The European Union general data protection regulation: what it is and what it means, Inf. & Com. Tech. Law 2019, p. 92.

[284] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 17; Thiel, Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene, ZD 2021, p. 468; Wagner/ Ruhmann, Irland: Das One-Stop-Shop-Verfahren, ZD-Aktuell 2019, 06546.

[285] Satariano, Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates, New York Times, 27.4.2020.

advertising ecosystem, nevertheless, the force and impact reached so far has been low.[286]

The reasons why DPAs can't or don't use their enforcement powers as vigorously as necessary to counter the shortcomings are diverse. A fundamental problem is the supervisory structure itself. Several obstacles that hinder smooth law enforcement already become apparent with view to individual authorities, their tasks, organisation and equipment (see 3.1.3.1). Looking at the bigger picture, the cooperation mechanism between the dozens of DPAs and the delimitation of competence show further impediments for efficient enforcement (see 3.1.3.2.).

Apart from such structural deficits, the situation is framed by procedural challenges, including those of administrative law, proof of evidence or quite simply: the controllers (financial) man and market power (see 3.1.3.3.).

3.1.3.1 Within the authorities: Capacity and capability

The most obvious cause in data protection enforcement results from being chronically underfunded. The poor equipment relates not only to the number of employees, but also to technical resources. This is despite the fact that Art. 52 sect. 4 GDPR actually obliges the Member States to ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers. While the risk of underfunding is inherent to all public institutions, data protection supervision combines a mix of technology and law, an unlimited group of addressees, a diverse portfolio of essential tasks and proximity to citizens in a unique way that is not comparable to any other authority.

In terms of enforcement resources, fining capacity and other regulatory tools the legislators attempted to put data protection on par with antitrust law.[287] Systematically, of course, this approach is plausible, since both competition and (online) violations of data subject rights mostly take place behind the scenes. Unlike antitrust, however, the addressees of data protection laws are (not) just a small subset of corporations that possess market power, but potentially: everybody. The GDPR establishes a range of complex rights and obligations that apply across the economy to businesses of every size, non-profit organisations, public authorities and even Individuals that fall under the definition of “controller”.[288] The group of people that the data protection authorities shall supervise is therefore in a completely different league in terms of quantity.

The situation is equally special with regard to tasks and prioritisation. Art. 57 sect. 1 GDPR lists a total of 22 tasks of every data protection authority, ranging from generally monitoring the application of the GDPR to specifically conducting the accreditation of a body for monitoring codes of conduct. By far the biggest item among these 22 is lit. f, namely to “*handle complaints lodged by a data subject, [...] and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is*

[286] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR. 2022,p p. 61 et seq.: A survey of a total of 26 empirical studies analysing the effects of the GDPR and the California Consumer Privacy Act (CCPA) on the data processing of website operators and advertisers pointed to underwhelming results so far. None of the independent studies surveyed found meaningful compliance on the ground in the first two years after the GDPR came into force.

[287] Hoofnagle/ van der Sloot/ Zuiderveen Borgesius, The European Union general data protection regulation: what it is and what it means, Inf. & Com. Tech. Law 2019, p. 67.

[288] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 52.

necessary". European DPAs receive several thousand complaints every year,[289] which they have to handle inhouse or accompany as part of the so-called one-stop-shop (**OSS**) procedure.[290] In 2023, 1023 proceedings were initiated in connection with the OSS alone.[291]

One reason for the sheer volume of complaints is - apart from the fact that data protection law is actually violated in many cases - the low threshold for submitting them. According to Art. 57 sect. 2 GDPR, the DPAs are obliged to facilitate the submission of complaints, e. g. by providing a complaint submission form. Because submitting a complaint takes no more time than writing an email, data subjects make extensive use of it. The topics of the complaints more or less reflect the deficits that data subjects perceive in their everyday lives - an unwanted newsletter from an online shop, a camera in the neighbour's garden, an open email distribution list, an unanswered access request with the employer etc. Although this low-threshold option for submitting a complaint is not objectionable, it means that even the most minor violations are reported on a massive scale, tying up considerable human resources in processing them.

The annual reports and organisational charts of the DPAs demonstrate that the majority of employees are involved in handling such complaints and therefore focus on enforcing the issues that complainants notice in their day-to-day life. With regard to the online advertising sector this means complaints are mostly limited to cookie banners on websites that are not suitable to obtain effective consent. As a consequence the regulatory focus is primarily on publishers.

Furthermore the GDPR offers hardly any options to escape this dilemma of prioritising complaint handling. Art. 57 para. 1 lit. f GDPR demands that a complaint needs to be investigated "to the extent appropriate". However, even most minimal measures per case tie up enormous amounts of capacity with view to the mass of individual cases. The problem becomes clearer when one realises that only a few complaints are really well prepared - the ones that are publicly known, like from NOYB, are an absolute exception. Rather, the information and documents submitted by the complainants are often very short, incomplete or even incomprehensible.

Given the large number of complaints, a pragmatic approach to complaint handling seems urgently required in view of the supervisory authorities' human resources and the need to set priorities in terms of cases with systemically relevant character. The ECJ's recent ruling on the discretionary powers of supervisory authorities is therefore to be welcomed. In the decision, the ECJ deals with the question of whether a supervisory authority is obliged under the GDPR to always take corrective powers when a violation is identified. The ECJ concludes that it cannot be inferred from either Art. 58 sect. 2 GDPR or Art. 83 GDPR "that the supervisory authority is under an obligation to exercise, in all cases where it finds a breach of personal data, a corrective power, in particular the power to impose an administrative fine, its obligation being, in such circumstances, to react appropriately in order to remedy the shortcoming found".[292] The

[289] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, pp. 53 et seq.: "Yet, their workload is all but endless - it took European data protection agencies only eighteen months to trigger the same amount of EU-wide potential cooperation requests that their antitrust counterparts issued in more than fourteen years". In the first nine months of GDPR enforcement, European data protection authorities received 94.622 complaints of potential violations, see EDPB, First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, 2019, p. 12, https://www.edpb.europa.eu/sites/default/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

[290] Figures for the individual supervisory authorities can be found in the EDPB´s Annual Report 2023, pp. 38 et seq.

[291] EDPB, Annual Report 2023, p. 33.

[292] ECJ, 26.9.2024, C-768/21 para. 41 - TR/Land Hessen.

ECJ expressly states that data subjects do not have a subjective right against the DPA to impose a fine.[293] At the same time, the ECJ emphasises that the supervisory authority is required to take actions where the exercise of one or more corrective powers is appropriate, necessary and proportionate. However, the ECJ also states - for the first time in such clarity - that a supervisory authority may exceptionally refrain from exercising a corrective power - depending on and taking into account the circumstances of the specific case - even if an infringement is identified. This may particularly be the case if the infringement has ceased and there is no risk of repetition.[294] Even though this ECJ ruling does not change the volume of complaints and as a result the compliant-driven working environment of the DPAs, it hopefully creates opportunities to build up capacity for enforcing more systemically relevant cases.

Another consequence of the described complaint-driven environment is that, "hidden" intermediaries without direct customer contact rarely come to the attention of the DPAs. Actors within the online advertising ecosystem get into the focus of the authorities only when data subjects with a particularly high level of expertise in the subject matter submit complaints or deficits in the depths of the network are subject to a press article.[295] Indeed, ex officio proceedings in which DPAs take a general look at an industry do take place. But to a relatively small extent. One example is the investigation into data protection compliance in the direct marketing data broking sector by the UK data protection authority. In 2020, the authority published a report on its investigation in which it focussed on offline marketing services offered by the three largest credit reference agencies in the UK.[296]

However, for such ex officio proceedings resources are essential. But this is what most DPAs lack. In fact several DPAs have grown significantly since the enactment of the GDPR. For example the Irish Data Protection Commission (DPC) grew from 70 to 201 personnel between 2016 and 2023.[297] The German Federal Data Protection Commissioner (BfDI) grew from 90 to 327 employees between 2015 and 2023.[298] Nevertheless, the existing personnel resources are far from sufficient.

Due to limited financial resources and the ongoing shortage of specialists, the supervisory authorities also have serious difficulties in recruiting well-qualified staff in sufficient quantity. In addition, a large proportion of the supervisory authorities seem to set the wrong priorities when filling the positions that are actually available, as only a comparatively small proportion of the positions are earmarked for technical specialists. Germany had the most tech specialists in 2020 compared to other member states, from which half of the European DPAs had only five tech specialists or less.[299] Even at the DPC, which is the lead supervisory authority for almost all big tech companies, the

[293] ECJ, 26.9.2024, C-768/21 para. 42 - TR/Land Hessen.

[294] ECJ, 26.9.2024, C-768/21 para. 43 - TR/Land Hessen.

[295] Dachwitz, Werbetracking: Wie deutsche Firmen am Geschäft mit unseren Daten verdienen, Netzpolitik, 8.6.2023.

[296] The investigation covered only direct marketing services and did not extend to the core credit referencing function of these companies. Also, it did not involve data collected about individuals' online behaviour, see ICO, Investigation into data protection compliance in the direct marketing data broking sector, https://ico.org.uk/action-weve-taken/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector/.

[297] DPC, Annual Report 2016, p. 2; DPC, Annual Report 2023, p. 90.

[298] BfDI, Annual Report 2017/2018, p. 124; BfDI, Annual Report 2023, p. 133.

[299] Ryan/ Toner, Europe's governments are failing the GDPR - Brave's 2020 report on the enforcement capacity of data protection authorities, p. 4.

proportion of tech specialists was only 15% in 2020.[300] However, in many areas, particularly in the field of online advertising, data protection investigations require a high degree of technical expertise and in-depth knowledge of the industry. Both authorities and courts are generally unable to provide this.

The so-called EDPB Support Pool of Experts (SPE) is one attempt to mitigate this situation. The program was developed as part of the EDPB Strategy 2021-2023 to help DPAs increase their capacity to enforce by developing common tools and giving them access to a wide pool of experts.[301] Inter alia the SPE launched a project in 2022 to develop a documented tool for website inspections, building on the Website Evidence Collector.[302] The EDPB aims to carry out approximately 10 projects per year with pre-eminent external experts in a given field. However, the SPE focusses on larger projects, rather to cope with individual enforcement procedures. When dealing with day-to-day business the supervisory authorities are essentially left to their own.

3.1.3.2 Between the authorities: OSS and structure of competence

In cases of cross-border processing according to Art. 4 no. 23 GDPR, where the processing of personal data takes place in the context of establishments in more than one Member State or where data subjects in several member states are affected, the one-stop-shop (OSS) mechanism applies. In short, this means that a controller only has to deal with one (lead) supervisory authority within the EU, which is competent to investigate potential violations and impose measures, but in turn has to cooperate with authorities from other Member States. Initially this instrument was considered to be the most practically significant innovation in the context of cooperation between European DPAs.

In fact, the number of cases handled in a cooperation procedure has risen continuously in recent years.[303] At the same time, the cooperation procedures, in which coordination between many DPAs has to be managed, are (too) time-consuming and complex.[304] Over the years, it has become apparent that the OSS mechanism is at the centre of cumbersome and slowed-down case processing. The aim of ensuring harmonised enforcement of the GDPR throughout the EU by coherent interpretation and implementation of data protection regulations is now faced with a number of dispute resolution proceedings between the DPAs. Years lasting proceedings, in which several authorities lodge objections against the draft decision of another DPA, are the order of the day.[305]

To understand the criticism, it is essential to understand the OSS mechanism itself: According to Art. 56 sect. 1 GDPR the lead supervisory authority (LSA) for cross-border cases is the authority of the main establishment or the single establishment of the controller or the processor. An exception to this are local cases according to Art. 56

[300] Ryan/ Toner, Europe’s governments are failing the GDPR - Brave’s 2020 report on the enforcement capacity of data protection authorities, p. 9.

[301] EDPB, Report on the use of SPE external experts, 16.4.2024.

[302] https://www.edps.europa.eu/node/5452_de.

[303] All final OSS decisions - for which the national law of the LSA does not prevent publication - can be accessed via the EDPB website, https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

[304] Thiel, Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene, ZD 2021, p. 468.

[305] All EDPB binding decisions regarding dispute cases can be accessed via the EDPB website, https://www.edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en.

sect. 2 GDPR, which, however, play a minor role in practice.[306] The LSA´s counterpart are supervisory authorities concerned (CSA) according to Art. 4 no. 22 GDPR, meaning all authorities that are affected by the processing because there is either another establishment in their territory, the processing in question affects data subjects in their Member State or the complaint was lodged with them

The cooperation between the LSA and the CSAs is governed by Art. 60-62 GDPR. In cross-border cases the LSA heads the investigation, communicates with the controller and ultimately prepares a draft decision to be submitted to the CSAs. The CSAs have the opportunity to file a "relevant and reasoned objection" within four weeks (Art. 60 sect. 4 GDPR). If no objection is raised, the draft decision is deemed to have been adopted and all authorities involved are bound by it (Art. 60 sect. 6 GDPR).[307]

If a CSA objects to the draft decision, be it because the facts appear incomplete, the legal assessment is not convincing or the measure does not appear suitable, it is up to the LSA whether or not it classifies the objection as relevant and reasoned and accordingly revise the draft decision.[308] If the LSA decides not to follow the objection, it is obliged to submit the matter to the consistency mechanism referred to in Art. 63 GDPR. In such cases of dispute regarding an objection the EDPB gets involved in the decision-making process and - after a formal procedure laid down in Art. 65 GDPR - decides about the conflict by issuing a binding decision (Art. 65 sect. 1 lit. a GDPR). The LSA subsequently shall adopt its final decision on the basis of the EDPBs binding decision.[309] However, the dispute may go one step further as a lawsuit demonstrates that was brought up by the Irish data protection authority (DPC) against the EDPB for allegedly exceeding its powers in one of the binding decisions.[310]

One key factor why this OSS mechanism does not achieve its goals is the lack of harmonised administrative procedural law in the EU.[311] The GDPR does state that national DPAs shall work together. However, the details of the procedures and what this cooperation looks like are left to the Member States. There are no clear rules as to which national law applies to which elements of the procedure. The elements of EU law are limited to certain steps of the cooperation procedure. In the past, this has led to time-consuming disputes at various levels. For example some SAs wanted to apply the instrument of so-called amicable settlement in order to close OSS procedures - a procedural step which is alien to most domestic legislations. The EDPB addressed these circumstances in its Guideline on the practical implementation of amicable

[306] Local cases are cases in which the subject matter relates only to an establishment in one Member State or substantially affects data subjects only in one Member State. In this case, the respective authority may handle the complaint, provided that the LSA does not exercise its right to deal with the matter itself in accordance with Art. 56 sect. 4 of the GDPR ("Selbsteintrittsrecht").

[307] See an overview of the procedure at Herbort/ Reinhardt, PinG 2019, pp. 28, 29.

[308] If a revised draft decision is issued, it must be resubmitted to all CSAs, not just the CSA that filed the objection, to ensure that the other CSAs also support the changes.

[309] If the LSA does not take action at all, the other SAs have various options at their disposal, particularly the initiation of urgency procedure according to Art. 66 sect. 3 GDPR. All existing options ultimately provide for a decision by the EDPB, which, however, always requires the cooperation of the DPAs due to a lack of powers under Art. 58 of the GDPR. If the SAs do not cooperate, the only option is to initiate infringement proceedings under Art. 267 TFEU. See in detail Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, pp. 105, 106 with further reference.

[310] The action was brought up on 17.2.2023, T-84/23: The DPC claims that the Court should annul parts of the Binding Decision 4/2022 of the EDPB on the dispute submitted by the DPC regarding Meta and Instagram, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62023TN0084.

[311] Thiel, Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene, ZD 2021, p. 468.

settlements, seeking to provide best practices for a consistent application of the GDPR.[312]

To streamline cooperation between DPAs when enforcing the GDPR in cross-border cases, the European Commission furthermore proposed a “Regulation laying down additional procedural rules relating to the enforcement of GDPR” in July 2023.[313] The proposal, inter alia contained a provision on the prioritisation of complaints and includes further details on a (narrow) definition of what constitutes “relevant and reasoned objections”, the parties' rights to be heard and the urgency procedure. After several comments on the proposal,[314] it was discussed in the European Parliament in April 2024 followed by further proposals for amendments.[315] One point of criticism is that the proposal may curtail the rights of users and merely stuff individual holes in the system instead of taking a systematic approach.[316] It remains to be seen whether and to what extent the planned regulation will actually lead to an increase in efficiency in the OSS procedure.

In addition to the challenges of the OSS mechanism just mentioned, a perennial criticism to the OSS procedure is that individual data protection authorities lack enforcement efforts, which is not only due to the shortage of human resources and certainly not because of too few enforcement powers.[317] In particular, the DPC has been criticised for delaying enforcement of the GDPR whereby the cause for the restraint of the DPC is seen in the importance of digital markets to the Irish economy.[318] Some experts are therefore discussing and calling for the creation of a European Data Protection Authority, which should be financially adequately equipped and competent for the data processing by very large online platforms.[319] However, this proposal, as good as it sounds, seems rather utopian in view of the current legal situation.

Irrespective of any obstacles within the OSS mechanism, questions of competence create its own difficulties. Even in cases in which GDPR violations are the only subject, intense disputes about competences may arise, both vis-a-vis the authorities or the controller. One case that was the subject of heated debate was the decision of the German Federal Cartel Office (FCO) in 2019, in which the FCO prohibited Facebook from merging user data from various services, such as Facebook, WhatsApp and Instagram, assuming that this would constitute a violation of § 19 para. 1 of the German

[312] EDPB Guidelines 06/2022 on the practical implementation of amicable settlements, p. 4

[313] European Commission, press release, 4.7.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609.

[314] EDPB-EDPS, Joint Opinion 01/2023, p. 5: The EDPB and the EDPS generally welcome the proposed regulation, while also making clear that the regulation will lead to a further workload for the supervisory authorities and can only be effectively enforced if the EDPB and the national supervisory authorities are provided with sufficient resources, https://www.edpb.europa.eu/system/files/2023-09/edpb_edps_jointopinion_202301_proceduralrules_ec_en.pdf; European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report of 9.11.2023 and Amendments 219 – 454 of 14.12.2023, https://www.europarl.europa.eu/doceo/document/LIBE-PR-755005_EN.pdf and https://www.europarl.europa.eu/doceo/document/LIBE-AM-757368_EN.pdf.

[315] Council of the European Union, General Approach, 18.6.2024, 11214/24, https://www.parlament.gv.at/dokument/XXVII/EU/189379/imfname_11386418.pdf; EDPB, Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR, para. 2: The EDPB maintained its demand for further resources right at the beginning of the statement. Overall, the EDPB has welcomed the amendments to the draft regulation, although further adjustments are still needed, particularly due to the fact that there are still too many references to national law, which would obstruct further harmonisation.

[316] https://noyb.eu/de/gdpr-procedures-regulation-stripping-citizens-procedural-rights.

[317] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, pp. 103, 104.

[318] Vinocur, One Country Blocks the World on Data Privacy, Politico, 24.4.2019; Kobie, Germany Says GDPR Could Collapse as Ireland Dallies on Big Fines, Wired UK, 27.4.2020.

[319] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 107.

Competition Act (abusive exploitation of a dominant market position). The FCO argued that freely given consent was necessary for the practice of Facebook. The choice between agreeing to the data collection or not using the social network at all was, however, not permissible.[320]

This was the first time that a competition authority had issued a ban on a particular behaviour based on data protection regulations.[321] This sparked a dispute over whether national competition authorities may investigate GDPR violations or whether this examination is reserved for data protection authorities only. After a back and forth between the instances of several German courts, among others, this question was referred to the ECJ. [322] The ECJ ultimately answered this question in the affirmative - meaning it took four years for the question of competence to be conclusively confirmed.[323]

3.1.3.3 Procedural issues: Lengthy proceedings and sideshows

Regardless of the financial and capacity issues, administrative and court proceedings may take years since some controllers seem to go out of their way to deliberately drag them out by complaining about (alleged) procedural errors. This can be seen from a few examples. Among other things, the Belgian data protection authority has devoted an entire chapter of its decision regarding IAB Europe to procedural objections raised by the defendant.[324] In a case of the Dutch authority, the Autoriteit Persoonsgegevens (AP), the controller objected to procedural errors, arguing that the investigation was unlawful because the authority had entered the virtual premises of the controller without the controller's consent or knowledge.[325]

It goes without saying that a controller is entitled to defend itself in the administrative proceedings or in court by all legally permissible means. There is also nothing to prevent a controller – which may benefit from a delay in the proceedings – from raising some spurious legal objections. However, focussing on side issues may lead to significantly prolonging the proceedings.

Beyond that, large, financially strong companies do not shy away from either fines or legal proceedings. They not only act in their own interests, but often as representatives of the entire industry. That means: Once a case has been sufficiently investigated and a decision has been made by the supervisory authority, these decisions - at least by financially strong companies - are very often challenged in court using all available means.[326] The challenge for the supervisory authorities is then to uphold the decision in court once it has been made. Here, too, the unequal balance of power becomes clear. A David versus Goliath battle begins. While an army of top lawyers fights on one side and produces pages of written pleadings, the authorities often have very good legal arguments, but hardly any capacity to put them on paper. Unlike many big tech companies, additional capacity cannot be bought in on the supervisory side ad hoc

[320] FCO, press release, 7.2.2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[321] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, pp. 56-57.

[322] Higher Regional Court Düsseldorf, order for reference, 24.3.2021, Kart 2/19 (V).

[323] ECJ, 4.7.2023, C-252/21.

[324] APD, 2.2.2022, DOS-2019-01377, para. 194 et. seq., https://www.edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf.

[325] AP, 2.5.2024, z-2021-14274, para. 34-35, https://autoriteitpersoonsgegevens.nl/system/files?file=2024-07/Besluit%20boete%20A.S.%20Watson%20-%20Kruidvat.pdf.

[326] Lancieri, Narrowing Data Protection's Enforcement Gap, MLR 2022, p. 41.

when it is needed. In addition, these proceedings require a very thorough collection of evidence in advance, which also ties up considerable resources for the authorities. This leads to a situation in which - even when wrongdoing is clear - DPAs might hesitate to use their powers against major companies because they can not afford the cost of legally defending their decisions against 'Big Tech' legal firepower.[327]

Since the GDPR came into force in 2018 several European data protection supervisory authorities have conducted proceedings in the context of online advertising. However, the number is rather small. See **Annex 2** for a table of 12 particularly noteworthy cases.

3.2 DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS

When displaying personalised advertising, processes such as the use of cookies to track the behaviour of users will regularly be at issue, where both the scope of the GDPR and the Directive on privacy and electronic communications (ePrivacy Directive - ePD)[328] apply.[329] While the GDPR and ePrivacy Directive have different objects and purposes of protection, they have overlapping areas of application, partly complement each other and cannot be considered in complete isolation from each other when it comes to the access of terminal equipment.

For this case, Art. 95 GDPR contains a conflict rule. According to this rule, the GDPR does not impose any additional obligations on data processors if they are subject to special obligations set out in the ePrivacy Directive that pursue the same objective. This conflict rule also applies to the national implementations of the Directive. Consequently, the specific provisions of the ePrivacy Directive take precedence over the provisions of the GDPR insofar as personal data is processed when storing and accessing information in a terminal equipment.[330] For the subsequent processing of personal data, which is only made possible by accessing this data, the general provisions of the GDPR come into effect.

3.2.1 Scope of application and regulatory objective: Protection of users' terminal equipment as part of the private sphere against unauthorised access

As early as 2002 the European legislator reacted to the fact that access to the internet became available and affordable for the general public on the one hand and the increasing use of tracking technologies on the other hand. These new options provided increasing capacities and possibilities for processing personal data. The successful cross-border development of these services inter alia depended on the trust of users that their privacy will not be compromised. In this new environment the ePrivacy Directive created specifications to protect the usage of terminal equipment against third party access without authorization. Although this is indirectly related to the protection of the user's privacy, the starting point of the Regulation is not the processing of personal

[327] Ryan/ Toner, Europe's governments are failing the GDPR - Brave's 2020 report on the enforcement capacity of data protection authorities, p. 1.

[328] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[329] ECJ, 5.6.2018, C-210/16, see in particular paragraphs 33-34 - Wirtschaftsakademie; EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, para. 33.

[330] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, para. 38.

data, but the storage of information in a user's terminal equipment or gaining access to the terminal equipment. Art. 5 sect. 3 ePD lays down that both actions are only allowed on the basis of consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. In consequence Art. 5 sect. 3 ePD sets high hurdles directly at the gateway of a process chain, which usually develops like a domino effect on subsequent data processing.

3.2.2 Objective obligations, subjective rights and responsibilities

Online advertising is generally displayed within digital services - like social media platforms, websites and apps - that can only be accessed via terminal equipment. Therefore Art. 5 sect. 3 ePD is relevant regarding the whole lifecycle of the advertising delivery process to users.

3.2.2.1 Technology-neutral and independent of personal data

A “user” in the meaning of Art. 5 sect. 3 ePR is everyone using terminal equipment, meaning a device that is connected to the internet and provides access to apps or website content.[331] This includes common electronic devices such as laptops, tablets and smartphones.[332] In contrast to data protection law, no subjective “affectedness” is required. Instead the ePrivacy Directive refers to any person who objectively uses the terminal equipment, regardless of whether the information accessed or read from the device is personal data within the meaning of GDPR.[333]

Storing information or gaining access can be independent operations, and performed by independent entities.[334] In consequence, information that is stored by one party (including information stored by the user or device manufacturer) which is later accessed by another party is therefore within the scope of Art. 5 sect. 3 ePD.[335]

When the directive was adopted, the legislator had in mind to regulate so-called spyware, web bugs, identifiers, cookies and similar instruments that can be used to store hidden information or to trace the activities of users and may seriously intrude upon the privacy of these users without their knowledge.[336] With cookies, for example, the accessing entity instructs the terminal equipment to proactively send information on each subsequent HTTP call order to receive back the targeted information. That is equally the case when the accessing entity distributes software on the terminal equipment of the user that is stored and will then proactively call an API endpoint over the network.[337] Regarding the storage of information, it is typically not stored in the terminal equipment through direct access by another party, but rather by instructing

[331] Art. 5 sect. 3 ePD builds on the definition used in Art. 1 no. 1a of Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications, saying that “terminal equipment means equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network”.

[332] But also connected cars or connected TVs and smart glasses, EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 17.

[333] ECJ, 1.10.2019, C-673/17 para. 70 - Planet 49; German Federal Court of Justice, 28.5.2020, I ZR 7/16 para. 61 – Cookie-Einwilligung II (Planet49).

[334] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 30.

[335] Art. 29 Working Party, Opinion 9/2014 on the application of ePrivacy Directive to device fingerprinting, p. 8.

[336] See recital 24 f. of the ePrivacy Directive 2002 and recital 66 of the ePrivacy Directive 2009.

[337] Additional examples would include JavaScript code, where the accessing entity instructs the browser of the user to send asynchronous requests with the targeted information, EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 32, 33.

software on the terminal equipment to generate specific information[338] There is no upper or lower limit regarding the length of storing time or amount of information stored. Similarly, the notion of storage does not depend on the type of medium on which the information is stored.[339]

Early on the Art. 29 Working Party emphasised that even if cookies were the most prominent way of accessing a terminal device to date, Art. 5 sect. 3 ePD does likewise apply to fingerprinting and similar technologies.[340] Hence, the law was designed to be technology-neutral in order to cover all technologies and procedures by means of which information can be stored and accessed in terminal equipment. However, the technical landscape has been evolving during the last decade. In the context of personalised advertising the increasing use of identifiers embedded in operating systems, as well as the creation of new tools allowing the storage of information in terminals, led to disputes regarding the laws application.[341]

The transition from less stateless to more stateful tracking methods led to the question, whether some of the new techniques involve end device access or storage at all. Among other things the replacement of existing tracking tools and development of new business models was driven by the (announced) discontinued support for third-party cookies by some browser vendors.

In view of the EDPB the ambiguities regarding the scope of application of Art. 5 sect. 3 ePD have created incentives to implement alternative solutions that have a tendency to circumvent the legal obligations, which is why the EDPB decided to publish a supplementary analysis in order to complement its previous guidance.[342] In its “Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive” the EDPB specifically commented on five methods that raised concerns: (1.) URL and pixel tracking, (2.) local processing, (3.) tracking based on IP only, (4.) Intermittent and mediated Internet of Things (IoT) reporting and (5.) Unique Identifier. The EDPB states that all these approaches fall within the scope of application or that this cannot be ruled out per se, depending on the specific utilisation.[343]

During a consultation phase, several stakeholders and civil society organisations commented on the first draft, mostly criticising that the EDPBs interpretation extends the scope of application beyond the purpose of protection. Some argue that Art. 5 sect. 3 ePD is not sector-specific data protection law but does protect a different type of privacy, namely the informational integrity of personal IT devices. As long as this informational integrity is left untouched, Art. 5 sect. 3 ePD shall not apply. In consequence some argue that information that is “sent” by terminal equipment such as the information contained in GET requests sent by web browsers, this shall not fall within the scope of this provision. It therefore remains to be seen whether the guidelines provide clarity and remedy in practice.

[338] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 36.

[339] Like hard disc drives (HDD), solid state drives (SSD), electrically-erasable programmable read-only memory (EEPROM) or random-access memory (RAM), see EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 37, 38.

[340] Art. 29 Working Party, Opinion 9/2014 on the application of ePrivacy Directive to device fingerprinting.

[341] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 2.

[342] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 3.

[343] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, para. 40 et seq.

3.2.2.2 Legal basis: Basically consent

While Art. 6 sect. 1 GDPR provides for six possible conditions under which personal data processing may take place, Art. 5 sect. 3 ePD focusses on one legal basis for the protection of terminal equipment, namely consent. Only one practically relevant exception applies in case “technical storage or access [is] strictly necessary in order for the provider of an information society service explicitly requested by the user to provide the service”.[344]

First of all, it is highly questionable as to whether user consent is an appropriate instrument in the context of privacy of communication. As mentioned, access to the terminal device is the most critical point at which de facto the loss of control begins. Certainly one could argue that adding more legal bases just leads to more opportunities for controllers to (falsely) rely on one of them. However, conceptual wise it seems not favourable to build such a pivotal point on a legal basis that depends on transparency and subjective insightfulness and is easy to manipulate and exploit - at least if no combination with other control mechanisms is in place. The reason for this is best explained using a historical example: in times when communication still took place via horse-drawn stagecoaches (and even earlier), the need for objective protective measures arose from the fact that the sender of the letter could not control whether the stagecoach driver secretly opened the letter after the next corner. It is obvious that this need for protection could hardly be addressed by the sender's consent. The same doubts actually arise in the age of digital communication.

Beyond that, the ePrivacy Directive does not contain any specific requirements for consent, but refers to data protection law with regard to the formal and substantive requirements. Accordingly, the same standards apply as laid down in the GDPR but 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.

At the same time, the addresses of the regulation certainly try to expand the scope of the exception to consent. The industry criticises that there are uncertainties about when the requirements for an exemption are actually met. They argue with various approaches that the term “strictly necessary” should be interpreted broadly. Even though the term “strictly necessary” is not defined in more detail in either the German Telecommunications-Digital Services-Data Protection Act (TDDDG)[345] or the ePrivacy Directive, however, the explanatory memorandum to the TDDDG assumes a technical necessity, which suggests a narrow understanding.[346] This means that even for services explicitly requested by users, only those accesses to the terminal equipment that are technically necessary to provide the requested service are covered by the exception.[347] This includes, for example, processes that serve to provide a digital service securely, quick and stable, including fraud prevention and IT security. But also

[344] Art. 5 sect. 3 ePD contains another exception which, however, is aimed at providers of telecommunications services and is therefore not relevant for this report: “for the sole purpose of carrying out the transmission of a communication over an electronic communications network”.

[345] Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten of 23.6.2021, BGBl. I 1982; 2022 I 1045.

[346] BT-Drs. 19/27441 p. 38; see also Austrian DPA, FAQ regarding Cookies and Data Protection, 20.12.2023, https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html.

[347] See recital 66 of the ePrivacy Directive 2009.

the shopping basket and payment function in an online shop count towards this.[348] The narrow interpretation is also supported by the fact that the criterion of necessity relates to the functionality of the service as such. Therefore the storage of or access to information in the terminal equipment cannot be justified by the fact that it is economically necessary for the business model in which the requested service is integrated.[349]

During legislative procedure regarding § 25 TDDDG as well during the discussion on the draft for an ePrivacy Regulation, it once again became clear that there are even more efforts to allow significantly more exceptions to the consent requirement than is currently provided for in Art. 5 sect. 3 ePD. Nevertheless, the German legislator stayed closely to the wording of the European provision and did not allow any exceptions beyond Art. 5 sect. 3 ePR.

3.2.2.3 Responsibility and accountability

Art. 5 sect. 3 ePR does not explicitly designate an addressee, since it is not directly linked to a telecommunications or digital service, but to the use of a terminal equipment. Therefore the obligation to store or access information in a user's terminal equipment only after consent was given or the requirements for an exception are met applies to anyone.[350]

This includes any natural or legal person who provides their own digital service, participates in the provision of such service or provides access to the use of a digital service. It is irrelevant whether the entity that stores or accesses information on a terminal device is the operator of a website, app platform or another third party, e.g. the provider of a software.[351]

The obligation does not only apply to website or app operators with regard to processes that take place via their own server. Operators must also comply with the requirements set out in Art. 5 sect. 3 ePD with regard to processes that have been carried out by third parties in case the design of their website allows these processes. This means in case the JavaScript code of a third party or a link to this code is embedded into the HTML code of a website, so that the user's browser is prompted to establish a connection to the server of a third party and information from the server is then stored on the users' devices, the website operator is in charge to ensure that the requirements pursuant to Art. 5 sect. 3 ePR are met. In consequence the target group is very broad in scope, whereby it should also be noted that the concept of joint controllership or controller-processor-relationships are alien to the ePrivacy Directive.

3.2.3 Complementarity with the GDPR: narrow conditions of admissibility at the gateway to GDPR

Art. 5 sect. 3 ePD complements the GDPR insofar as its obligations affect controllers even for purely technical processes independent of the processing of personal data. Regarding tracking techniques used for the personalisation of advertising this might make a significant difference regarding the enforcement (see chapter 3.2.4.). Art. 5 sect. 3 ePD is more or less immune to any of the industry's attempts to evade the

[348] For more details, see DSK, Orientierungshilfe Telemedien, 2022, para. 68 et seq.

[349] Regarding the further interpretation of the exception and its requirements, see DSK, Orientierungshilfe Telemedien, 2022, in particular para. 62 et seq.

[350] Higher Regional Court Frankfurt a.M., 27.6.2024, 6 U 192/23 - Microsoft Advertising.

[351] Higher Regional Court Frankfurt a.M., 27.6.2024, 6 U 192/23 - Microsoft Advertising.

GDPR by arguing that IP-addresses[352], UIDs, further identifiers or data stored in a cookie is no personal data. In the past the advertising industry even claimed that some core components of the personalisation of advertising don´t fall within the scope of the GDPR, namely the TC String, which is used within the TCF framework (see chapter 2.2.4.1.). This led to years of legal disputes just about the question of which processed information is personal data and which actor of the ecosystem is in charge of it. The European Court of Justice has rejected the industry's argument and confirmed the nature of the TC string as personal data.[353] When it comes to Art. 5 sect. 3 ePD, there is no basis for such defence tactics at all.

In addition, Art. 5 sect. 3 ePD acts as a gatekeeper to the GDPR by protecting whether the data to be processed can be obtained at all. The storage of or access to information in the terminal equipment in principle requires user consent in accordance with Art. 5 sect. 3 ePD and Art. 4, 6 and 7 GDPR. If no such consent has been given at all or it's not valid, this will likewise affect the subsequent processing. Data processing that is based on the storage of or access to information in the terminal equipment can only be lawful if the upstream processing is lawful under the ePrivacy Directive. Otherwise the gateway to gather this data in the first place was not “opened” by the user. In consequence the lawfulness of data processing under the GDPR must be examined incidentally to determine whether the upstream processes of storing or accessing information have taken place lawfully.

3.2.4 Reasons for ineffective implementation in practice

At the same time, the ePrivacy Directive has its weak points. Far and foremost the biggest problem is the European Commission's failure to ensure consistency with the GDPR by neither making appropriate amendments nor harmonising the sector-specific rules by agreeing on a text for a new regulation.[354] Recital 173 of the GDPR contains a mandate to the European legislator to review the ePrivacy Directive and ensure consistency with the GDPR by making appropriate amendments. In 2017 the European Commission published the proposal for a new “Regulation on Privacy and Electronic Communications” that was supposed to come into force at the same time as the GDPR.[355] However, all efforts have so far been fruitless, and even eight years after the GDPR came into force the future of a potential ePrivacy Regulation is unclear.[356]

Therefore, the specifications of Art. 5 sect. 3 ePD had to be transposed into national law by the member states. In most ones the implementation took place in 2011 and 2012 with correspondingly long application practice.[357] In Germany, Art. 5 sect. 3 ePD has only been implemented into national law with effect from 1 December 2021. In this

[352] ECJ, 19.10.2016, C-582/14, para. 49 - Breyer.

[353] ECJ, 7.3.2024, C-604/22, para. 33-51 - IAB Europe.

[354] Selzer, Die Zukunft der ePrivacy-Verordnung, DuD 2024, p. 463.

[355] Proposal for a Regulation of the European Parliament and of the Council of 10 January 2017 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), COM(2017) 10 final.

[356] Selzer, Die Zukunft der ePrivacy-Verordnung, DuD 2024, p. 463.

[357] Art. 5 para. 3 ePrivacy Directive was implemented in 2011, for example, in Ireland (provision 5 of the ePrivacy Regulations 2011), France (Art. 82 of the Loi Informatique et Libertés, adapted by Ordonnance no 2011-1012), the UK (Art. 6 of the Privacy and Electronic Communications Regulations, adapted by Statutory Instrument No. 1208/2011), Denmark (Sect. 9 of the Bekendtgørelse af lov om elektroniske kommunikationsnet og -tjenester in conjunction with the Implementing Regulation No. 1148/2011) and Austria (§ 96 Abs. 3 of the Austrian Telecommunications Act 2003, adapted by Federal Law Gazette I No. 102/2011, now Section 165 öTKG 2021) and in 2012 in Italy (Sect. 122 of the Codice in materia di protezione dei dati personali, adapted by Legislative Decree No. 69/2012), the Netherlands (Sect. 11.7a of the Dutch Telecommunications Act of 5 June 2012) and Spain (Art. 22 para. 2 of Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico, adapted by Legislative Decree 13/2012).

report, the German transposition in § 25 TDDDG is used as a representative example, since it is very closely based on the wording of the European regulation.

The different national regulations lead to a conceivably inefficient supervision structure. As described above, when displaying personalised advertising processes take place that are inextricably linked but trigger both the application of the ePrivacy Directive and the GDPR. While Art. 56 et seq. GDPR provides for a OSS mechanism to designate one lead supervisory authority within the EU, there is no such cooperation mechanism for the supervision of processes falling within the scope of the ePrivacy Directive.[358] Beyond that, in several member states it's not the data protection authorities that are competent to investigate ePrivacy matters, but others like the telecommunication authorities.[359] Such lack of a central supervisory structure in context of personalised advertising therefore means that depending on the territorial extent of the respective violation up to 27 national ePrivacy-authorities plus data protection authorities - represented by one lead authority - are in charge.

Indeed it is possible for the national “ePrivacy-authorities” to deal with an infringement without taking subsequent data processing operations into account and to limit their investigation to national facts. This way no coordination is required for the investigation, but at the same time a decision only has domestic impact. However, some authorities chose this path in the past in order to achieve quick results or to take action against companies for which they aren't lead DPA. Inter alia this was done by the French data protection authority, the Commission Nationale de l’Informatique et des Libertés (CNIL), which is likewise the national ePrivacy authority in France. The investigations by the CNIL under ePrivacy have caused a great stir, although they were actually nationally limited. Several times the CNIL has taken action with regard to the french-language websites of Amazon, Google and Facebook, among others, whose EU headquarters are located in Luxembourg or Ireland. The controllers doubted the CNIL competency, but it was confirmed by the french administrative court that no OSS was applicable.[360] Accordingly, the CNIL was not obliged to cooperate or hand over the cases to the lead data protection authorities in Luxembourg and Ireland and was therefore able to impose fines of up to 90 million Euros in very expeditious procedures (see table below) .

Conversely, “GDPR-authorities” may limit their investigations to processes within the scope of the GDPR. However, the authority incidentally has to deal with the question of whether the data was collected lawfully when accessing the terminal device. As a rule GDPR-investigations therefore cannot take place in complete isolation. However, there are reasons why some authorities investigate the use of cookies and the subsequent data processing separately although both processes are so strongly connected. On the one hand, cooperation with (several) other ePrivacy-authorities is complex (in countries

[358] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, para. 80.

[359] Art. 5 para 3 ePrivacy Directive was implemented in Poland by Section 173 of the Polish Telecommunications Act, which is supervised by the Office of Electronic Communication; in Denmark, the implementation took place by Sect. 9 of the Act on Electronic Communications Network and Services in conjunction with Regulation No. 1148 of 9.12.2011 which is supervised by the Danish Business Authority; in Finland, the ePrivacy requirements were implemented in Sect. 105 of the Act on Electronic Communication Services, which is supervised by the Finnish Transport and Communications Agency (Traficom); in Austria, the Telecommunication Authorities is competent to supervise Section 195 öTKG. In Belgium, the Belgian Institute for Postal Services and Telecommunications was originally competent to supervise Art. 129 of the Electronic Communications Act - however, the provisions were transferred on 10.1.2022 to Art. 10/2 WVP (Act of 30.7.2018 on the protection of natural persons with regard to the processing of personal data), which lies in the competence of the Belgian DPA now.

[360] Contrary to the claimants' demand, the court also saw no reason to refer the question to the ECJ for a preliminary ruling, Conseil d’État, 18.1.2022, no. 449209, para. 12 et seq. – Google, www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-01-28/449209; Conseil d’État, 27.6.2022, no. 451423, para. 4 et seq. – Amazon, www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-06-27/451423.

with split competency). Furthermore, in some Member States the competent authorities have not been given enforcement powers with regard to the processes covered by the ePrivacy Directive.[361] Accordingly, the data protection authorities in these member states focus on investigations under the GDPR.

Furthermore, it is remarkable that the implementation of Art. 5 sect. 3 ePD in the member states is comparable, but not the same. With regard to the legal consequence, for example, in Germany the fines range for violations of § 25 TDDDG is 300.000 Euros while in France, on the other hand, for violations of Art. 20 sect. 4 no 7, Art. 82 Loi Informatique et Libertés the GDPR fine range applies, meaning up to 20 million Euros. Again in Spain, in contrast, violations of Art. 39 sect. 1 lit. c, Art. 38 sect 4 lit. g, Art. 22 sect. 2 of Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico may only result in fines up to 30.000 Euro (with further reduction options).

Due to some procedural advantages of the ePrivacy Directive, the national implementation laws have been used to challenge deficits in the digital advertising market in a number of cases, particularly in relation to the use of cookies and cookie banners. See **Annex 2** for a table of particularly noteworthy cases.

Finally, within the last decade disputes regarding the application of Art. 5 sect. 3 ePR did arise. Unlike the GDPR, this does not concern the question of whether personal data is involved at all. Rather, the transition from less stateless to more stateful tracking methods led to the question, whether some of the new techniques involve end device access or storage at all (for more details see 3.2.2.)

3.2.5 Technical settings and control mechanisms: PIMS

The European Commission's proposal for an ePrivacy Regulation included a provision for consent to be expressed using the technical settings of a software application that enables access to the internet (e.g. a browser).[362] As the regulation has never been finalised, the idea has not been implemented at European level. In Germany, however, attempts have been made to at least create a national legal framework for the use of PIMS. § 26 TDDDG stipulates that the German federal government can determine requirements for PIMS by a delegated act. The resulting Verordnung über Dienste zur Einwilligungsverwaltung nach dem TDDDG (Einwilligungsverwaltungsverordnung – EinwV) was adopted in December 2024,[363] despite heavy criticism at all stages of the legislative process.[364]

A key criticism was that it would not be possible to achieve the aim of the EinwV because consent banners on websites would still not be completely redundant.[365] Further points of criticism were that the EinwV is limited to national law since it can only refer to consent in accordance with § 25 para. 1 TDDDG not to data protection consent

[361] For example, Luxembourg law does not provide any powers to impose fines or remedies for violations of the national ePrivacy implementation in Art. 4.3 e of the amended law of 30 May 2005.

[362] See Art. 9 para. 2 of the proposal for an ePrivacy Regulation.

[363] BT-Drs. 20/12718, 4.9.2024, approved by the German Bundesrat in its meeting on 20.12.2024, plenay protocol 1050, p. 502.

[364] VZBV, Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten, Stellungnahme, 28.08.2024, https://www.vzbv.de/sites/default/files/2024-09/24-09-04_Stellungnahme_vzbv_RegE_EinwV.pdf; VZBV, Anreize für Einwilligungsverwaltungssysteme fehlen, Stellungnahme, 14.7.2023, https://www.vzbv.de/sites/default/files/2023-07/Anreize%20f%C3%BCr%20Einwilligungsverwaltungsdienste%20fehlen%2014.%20Juli%202023_0.pdf; VZBV, Anforderungen des vzbv an die Rechtsverordnung des Bundes nach § 26 Absatz 2 TTDSG, 2021, 3.11.2021, https://www.vzbv.de/sites/default/files/2021-11/21-11-03_vzbv-Anforderungen_%C2%A726_Abs2_TTDSG.pdf.

[365] DSK, Stellungnahme zum Referentenentwurf des BMDV, 11.7.2023, p. 1, https://www.datenschutzkonferenz-online.de/media/st/23-07-11_DSK-Stellungnahme_Einwilligungsverwaltung_TTDSG.pdf;

though,[366] and that neither the specific functioning of the consent management service nor the technical and organisational design have been sufficiently described.[367] Further criticism concerned the fact that, according to § 18 sect. 1 EinwV, the integration of so-called "Anerkannte Dienste" (meaning certified PIMS) by providers of digital services is voluntary.[368] As a consequence, publishers who use such certified PIMS, but do not receive consent, can continue to display separate banners in order to ask users for their consent again. It is therefore not clear how the regulation is intended to provide a real remedy in practice.

3.3 ARTIFICIAL INTELLIGENCE ACT

3.3.1 Scope of application and regulatory objective: Protection of fundamental rights against the risks of AI systems

The regulatory objective of the Artificial Intelligence Act (AI Act)[369] is to promote the uptake of human-centric and trustworthy artificial intelligence (AI) and supporting innovation, Art. 1 sect. 1 AI Act. In particular, the AI Act aims at ensuring a high level of protection of health, safety, fundamental rights enshrined in the European Charter of Fundamental rights, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems.

To this aim, Art. 3 sect.1 AI Act defines its scope, comparable to the GDPR fairly widely, referring to an AI system as a "machine-based system that is designed to operate,

- with varying levels of autonomy and
- that may exhibit adaptiveness after deployment, and
- that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions
- that can influence physical or virtual environments."

This definition has a fairly broad scope of application, which ultimately comes close to a general algorithm liability. At least, the structure of the law is based on product liability law and therefore consists of objective obligations and no subjective rights of individuals.[370]

3.3.2 Complementarity with the GDPR: Ban on certain AI practices and transparency obligations

Focusing on the provider of the AI system, the AI Act introduces provider liability and thus contributes to the above-mentioned gap between legal responsibility and technological capacity that the GDPR has left (see chapter 3.1.2). Insofar as the deployment of AI systems requires the processing of personal data, the two laws hence are complementary: Both the AI Act and the GDPR pursue the same goal, i.e. to avert the risks to the fundamental rights of individuals and to society as a whole that arise

[366] DSK, Stellungnahme zum Referentenentwurf des BMDV, 11.7.2023, p. 2.

[367] DSK, Stellungnahme zum Referentenentwurf des BMDV, 11.7.2023, pp. 3, 5.

[368] VZBV, Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten, Stellungnahme, 28.08.2024, pp. 9 et seq.

[369] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 12.7.2024, 1-144.

[370] See the interview with Paul Nemitz, Principal Adviser on the Digital Transition in DG Justice and Consumers, EU Commission, „Es muss ein Primat der Demokratie über Technologie und Geschäftsmodell geben" at https://te.ma/art/yu5hji/nemitz-ki-verordnung-demokratie/.

from the use of AI systems or data processing, respectively; however, while the AI Act focuses on the design of AI-based algorithms, the GDPR focuses on the processing of personal data with such an AI system, i.e. the deployment of the system.

Thus, as long as both laws apply, the AI Act may well remedy certain deficits of the GDPR. What is most striking in this context is the clear ban on certain AI practices. 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),[371] the AI Act contains a real ban on certain AI practices. For some of these practices, it is possible that they are used for the purpose of personalised advertising. According to Chapter 2 of the AI Act, these prohibited practices are:

- the use of an AI system that deploys **subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques**, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably **impairing their ability to make an informed decision, thereby causing** them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons **significant harm** (Art. 5 sect. 1 lit. a);

- the use of an AI system that **exploits any of the vulnerabilities of a natural person or a specific group of persons** due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially **distorting the behaviour** of that person or a person belonging to that group in a manner **that causes** or is reasonably likely to cause that person or another person **significant harm** (Art. 5 sect. 1 lit. a);

- the use of AI systems for the **evaluation or classification of natural persons or groups of persons** over a certain period of time **based on their social behaviour** or known, inferred or predicted personal or personality characteristics, **with the social score leading to detrimental or unfavourable treatment** of certain natural persons or groups of persons **in social contexts that are unrelated to the contexts in which the data was originally generated** or collected (Art. 5 sect. 1 lit. c, i).

In all three cases, the question is, of course, what "significant harm" or "detrimental or unfavourable treatment" means. However, the examples show that the EU legislator is not squeamish about banning certain practices if it perceives these practices as definitively incompatible with "European values".[372]

A general ban on data processing practices for personalised advertising is therefore likely if it turns out that the chaotic processing conditions in the online advertising sector and the risks posed by these practices cannot be satisfactorily resolved, despite 'softer' legal initiatives such as the GDPR, and not even over a longer period of time (see

[371] The so-called "ban subject to permission" ("Verbot mit Erlaubnisvorbehalt") which many criticise with regard to the legal basis needed under Art. 6 GDPR, is actually a technical legal mechanism for consent and, at least theoretically, does not contain any rule of interpretation according to which exceptions (i.e. the legal bases in Art. 6 GDPR) to the rule must be interpreted narrowly, see v. Grafenstein, Refining the concept of the right to data protection in Article 8 ECFR – Part III, EDPL 2021, pp. 380 et seq.

[372] See, in general, the European data strategy as part of the European digital strategy at https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

chapter 5.2.). In this context, we would like to clarify that the authors of this study are well aware of the high administrative burden that the GDPR is placing on many actors, especially SMEs (which is why we put the term 'softer' in quotation marks). However, it is also obvious that the legal requirements imposed by the GDPR are not having the desired effect on the online advertising sector. Compared to a complete ban of personalised advertising or certain forms of it, the GDPR is definitely the 'softer' approach.

Apart from the ban of certain AI practices, there is also a transparency requirement, which likely applies to personalised advertising. Art. 50 sect.1 AI Act stipulates that AI systems intended to interact directly with natural persons must be designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of the persons. Since the aim of the advertising is for people to click on it and thus interact with it, the persons have to be shown the fact that they are interacting with an AI system. Whether this information is particularly important for consumers to protect themselves against the risks of personalised advertising is, of course, open to debate. In contrast to this, two other regulatory complexes are therefore much more important.

3.3.3 Limited complementarity: Technical design of AI systems and up/downstream coordination between providers, distributors and deployers

More important than the transparency requirements are, firstly, the extensive provisions on the technical and organisational design of so-called high risk AI systems. In their level of detail, these provisions go far beyond the general data protection by design requirement under Art. 25 sect. 1 GDPR. Therefore, these specifications reduce the uncertainty as to how a related data processing operation must be technically and organisationally designed so that this effectively protects individuals from the risks to their fundamental rights, considerably.

The AI Act achieves this by providing several requirements with respect to the development and maintenance of such an AI system while taking into account, also in this context, its intended purpose as well as the state of the art on AI and AI-related technologies. According to Art. 8 et seq. AI Act, high risk AI systems must comply with the following technical-organisational measures:

- Establishment, implementation, documentation and maintenance of a risk management system, in essence, to identify and mitigate the risks to the individuals' fundamental rights (**risk management**, Art. 9);
- development of high risk AI systems on the basis of training, validation and testing data sets that meet certain quality criteria (**data governance**, Art. 10);
- technical documentation, record keeping and provision of information to deployers to enable deployers to interpret a system's output and use it appropriately (**documentation and transparency**, Art. 11-13);
- design and development of AI systems in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use (**human oversight**, Art. 14);
- design and development of AI systems in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle (**accuracy, robustness, and cybersecurity**, Art. 15);

- and a quality management system that ensures compliance with the AI Act and which is documented in a systematic and orderly manner in the form of written policies, procedures and instructions (**quality management**, Art. 17).

The scope and level of detail of these requirements is the first regulatory complex that goes far beyond the general data protection by design approach in Art. 25 GDPR. A second important complex concerns the way in which the AI Act regulates, upstream and downstream, the coordination of the various actors involved, from the developers of high risk AI systems, to the importers, to the distributors, up to the deployers – and all the way back. According to this regulatory approach, providers of high-risk AI systems must, in essence, ensure that they comply with all the above requirements, undergo a corresponding conformity assessment (Art. 43 et seq. AI Act), affix the CE marking issued upon successful completion of the assessment (Art. 47 and 48 AI Act) as well as their name to the system, and register their system and themselves in the corresponding EU database (Art. 71). Importers and distributors of high risk AI systems must, in turn, ensure that the system they place on the EU market has the necessary CE marking and that the technical documentation and instructions for use for the system deployer are included. Importers and distributors too must indicate their name etc. Furthermore, they bear independent responsibility not to place the system on the market if they have sufficient reason to consider that the system is non-compliant. If the system also poses a risk to the fundamental rights of the data subject, they must report this back, i.e. to the importer and the provider, but also partly to the market surveillance authorities. Finally, the system deployers are under an obligation to use the system in accordance with the instructions for use, to set up the technical and organisational human oversight and to monitor the system (in particular with regard to the input data and by keeping logs). The deployers must also stop using the system if they discover a non-conformity and, in the event of a risk to the fundamental rights of the data subjects, inform the distributor, developer, and here again, the market surveillance agencies.

In contrast to the rather generally defined legal roles and (cooperation) obligations of the GDPR, the AI Act thus defines quite precisely which actor has which obligations. Of course, these obligations will unfortunately not apply in most cases of personalised advertising. It is true that AI systems have long been used in the field of advertising. However, in most cases these are not high-risk AI systems. The reason for this is that Annex III of the AI Act lists specific areas that classify AI systems as high-risk systems if they are used in these areas for the purposes intended there. However, personalised advertising is not listed in this Annex III. Actually, annex III does not even list recommender systems, on which personalised advertising is usually based.[373] Therefore, the aforementioned regulations are not applicable to most cases of personalised advertising.

An exception exists for certain contexts of advertising, in particular political advertising (Annex III no. 8 lit. b) and advertising for the recruitment of employees (Annex III no. 4 lit. a). If political advertising is based on “AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda”, this classifies such an AI system as a high risk system. Similarly, if advertising is based on “AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements”, this also classifies an AI system as a high risk system. In these cases, the aforementioned regulations on the technical and organisational design of AI

[373] Viktoratos/ Tsadiras, Personalized Advertising Computational Techniques: A Systematic Literature Review, Findings, and a Design Framework, Information 2021.

systems and on the coordination of the various actors involved thus supplement the GDPR, because the application of these systems in these contexts usually requires the processing of personal data.

However, the presentation of the aforementioned provisions of the AI Act is also important for the purposes of this study for another reason. This is because the provisions point to ways in which the GDPR could be concretised or supplemented in the area of personalised advertising, even outside of these specific contexts. By concretisation, we mean that the rules could be used in the interpretation of Art. 25 sect. 1 GDPR as generally accepted rules of practice or even as state of the art for the context of consumer goods purchases. By supplementation, we mean the case in which a new independent law would establish these rules for the case of personalised advertising. The provisions of the AI Act may thus serve as an important source of inspiration for the interpretation of existing laws or even the design of new laws (see chapter 5).

3.3.4 Consideration of the needs of SMEs, implementation in practice

The AI Act also goes beyond the provisions of the GDPR in terms of taking the needs of SMEs into account. SMEs are often faced with the challenge of complying with the (often complex) legal requirements despite limited resources in terms of capital, personnel and knowledge. Larger companies face this challenge less, as their size enables them to set up appropriate legal departments.[374] In this respect, the GDPR only stipulates that the needs of SMEs should be taken into account in the certification procedures, for example. However, as it is not specified how this is to be done, this is usually only reflected, if at all, in the data protection authorities' fee tables in the form of reduced fees (see chapter 2.5.8.3.).

In contrast, the AI Act provides for significantly expanded mechanisms for SMEs to develop or use legally compliant AI systems. These include, in particular, the so-called AI regulatory sandboxes (see the objectives of these sandboxes in Art. 57 sect. 9 AI Act). The provisions of the AI Act stipulate that access for SMEs to these regulatory sandboxes must not only be free of charge (Art. 58 sect. 2 lit. d AI Act). Rather, Art. 62 AI Act also contains numerous additional specific provisions according to which SMEs must be supported.

In more general, a key factor for effective enforcement in practice will also be which authority is responsible for enforcement. In light of the coordination challenges with respect to the GDPR and the ePrivacy Directive, it is to be hoped that procedures will be harmonised as far as possible if the areas of application of the various laws overlap.

3.3.5 Parallels and experience from REACH Regulation

In order to illustrate that the provisions of the AI Act are general principles of risk regulation that can be conceptually applied to the regulation of the risks of processing personal data, we would like to take a brief look at the REACH regulation.

[374] Levie, J., Autio, E., Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, in: Journal of Management Studies 48 (6) (2011), pp. 1392–1419, quoted as: Levie and Autio, Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, p. 1411.

The Regulation concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH regulation)[375] was enacted in 2007 to improve the protection of human health and the environment from the risks that can arise from chemicals and at the same time to increase the competitiveness of the EU chemical industry. In a nutshell, the starting point for the restrictions and registration mechanisms of the REACH regulation is the fact that even harmless chemicals can develop a high risk potential during certain further processing. Various players are involved in a network-like distribution structure, from manufacturers and importers to distributors and other downstream users. In order to fulfil the obligations of the regulation, the addressees must first identify and control the risks associated with the substances they manufacture and place on the market and demonstrate to the competent authority how the substance can be used safely, among other things. The basic idea of the REACH regulation and the AI Act are astonishingly similar to the linking of processing operations in data protection, so that we assume that interesting possible conclusions can also be drawn here for regulatory alternatives in the advertising market.

According to its Art. 1, the REACH Regulation follows the regulatory principle that manufacturers, importers and other actors in the supply chain, like downstream users, must ensure that they manufacture, place on the market or use such substances that do not adversely affect human health or the environment. The Regulation is based on the precautionary principle, which results from the fact that (harming) consequences of the use of substances cannot or can hardly be contained.[376] The regulation explicitly defines the key players involved in the supply chain. For all of them a standard of responsibility applies, which demands that substance-related risks need to be “appropriately controlled”. The behavioural contributions to risk identification, risk-related communication and cooperation that are envisaged for this purpose are to be provided to a considerable extent on one's own responsibility. This is also referred to as the assignment of substance responsibility (“Zuweisung der Stoffverantwortung”).[377]

As the most stringent measure, the REACH Regulation stipulates that risk-reducing measures can be prescribed on the basis of Art. 67 et seq. REACH Regulation. These include not only restrictions on the use or placing on the market of a substance, but also, under certain circumstances, the production itself (the current substance prohibitions and restrictions are listed on 450 pages in Annex XVII of the regulation, including 52 substances or substance groups)

Differentiated according to the various addressees of the regulation, there are registration requirements with prior risk assessment procedures (Art. 6 et seq. REACH Regulation), information requirements based on the value chain (Art. 31 et seq. REACH Regulation) and finally cooperation requirements, according to which the actors not only exchange information but also develop joint strategies for risk management.

In contrast to its predecessors, the focus of the REACH regulation is no longer limited to classifying substances and labelling them. Rather, the entire lifecycle of a substance must be taken into account and it must be demonstrated that the risks are controlled

[375] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC.

[376] See on the implementation of the precautionary principle in data protection law, for example, v. Grafenstein, Refining the concept of the right to data protection in article 8 ECFR – Part II, EDPL 2021, pp. 190 et seq.

[377] Führ/ Bizer, Zuordnung der Innovations-Verantwortlichkeiten im Risikoverwaltungsrecht – Das Beispiel der REACh-Verordnung, 2009, p. 309.

from production to disposal. For substances classified as substances of “very high concern”, all manufacturers, importers and downstream users need to apply for a multi-stage authorization procedure according to Art. 55 et seq. REACH Regulation. Because the Regulation stipulates that marketing is prohibited without registration, there is a considerable incentive for the players who want to market the substance legally to register.[378]

The excursus on the REACH Regulation shows that these co-ordination duties are an essential element of risk regulation and can be consistently incorporated into the regulation of the risks of personalised advertising.

3.4. REGULATION ON THE TRANSPARENCY AND TARGETING OF POLITICAL ADVERTISING

On 9 April 2024 the Political Targeting Regulation (PTR)[379] entered into force. So far, political advertising was regulated heterogeneously in EU Member States, which led to the fragmentation of the internal market and decreased legal certainty for providers of political advertising services. The PTR concretises and supplements the GDPR with several specific objective requirements for data processing for political advertising and even with some subjective data subject rights.

3.4.1 Scope of application and regulatory objective

This PTR applies to political advertising, which covers in particular “*the preparation, placement, promotion, publication, delivery or dissemination of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign by, for or on behalf of a political actor or which is liable and designed to influence the outcome of an election*”.

The regulation applies both to sponsors and providers of political advertising services (purely ancillary services, being those that merely complement and depend on political advertising services, such as transportation, financing and investment, are excepted). Political advertising services are a broad category. The category includes a broad range of providers of services connected to political advertising such as political consultancies, advertising agencies, platforms within the advertising ecosystem, public relations firms, influencers, various data analytics and brokerage operators, as well as publishers.

In doing so, the regulation aims to establish a common regulatory framework enhancing the transparency of sponsored political advertising (both online and offline), reinforcing the integrity of election campaigns and fighting disinformation and foreign interference. Member States must lay down rules on sanctions or other measures, applicable to sponsors or providers of political advertising services for infringements of the above mentioned rules. The maximum amount of the financial penalties that may be imposed must be: 6% of the annual income or budget of the sponsor or of the provider of political advertising services as applicable and whichever is the highest; or 6% of the annual worldwide turnover of the sponsor or the provider of political advertising services in the preceding financial year.

[378] Führ/ Bizer, Zuordnung der Innovations-Verantwortlichkeiten im Risikoverwaltungsrecht – Das Beispiel der REACh-Verordnung, 2009, p. 324.

[379] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L, pp. 1-44.

3.4.2 Complementarity with the GDPR: Ban on the use of certain types of personal data, enhanced transparency obligations and data subject rights, as well as clarification of cooperation duties

The PTR concretises and supplements the GDPR with several specific objective requirements for data processing and even with some subjective data subject rights. For example, Art. 18 sect. 1 PTR allows the processing of personal data for political targeting and corresponding targeting techniques only when:

- the controller collected the personal data from the data subject; and
- those techniques do not involve profiling using special categories of personal data (for example, data revealing political opinions).

At first glance, these **bans** seem clear, but at second glance they raise a number of questions. For example, the PTR appears to prohibit the processing of data that the controller has not collected itself, but has collected from other sources (see also the distinction in Art. 13 and 14 GDPR). The regulation thus appears to significantly restrict the pool of legally available data in comparison to the practices described above in the normal advertising ecosystem. At second glance, however, it is unclear whether this also applies to data provided by a joint controller. If several actors who have collected data directly from data subjects cooperate with each other, the legally available data pool appears to grow accordingly. The fact that the provision only refers to the general legal role of the ‘controller’ and not to the specific actors specified in Art. 3 PTR may indicate that the legislator did not want to limit the data pool to certain actors. Further, the legal form of joint controllership forces the joint controllers to coordinate their protective measures (see chapter 3.1.2.7.). These coordination obligations of the GDPR therefore add to the protection duties of the PTR. Thus, there is no need to assume a protection gap here if data that joint controllers have collected may also be used for political advertising. However, the legal situation is not unambiguous.

A similar question arises with the second ban. According to this, no sensitive data pursuant to Art. 9 GDPR may be included in the profiles for political advertising; this includes political opinions. This ban is perplexing for two reasons: Firstly, the term profiling is defined so broadly in Art. 4 no. 4 GDPR that any political targeting is actually based on profiling. After all, political targeting is intended to use automated means to evaluate the personal aspects of a voter, namely which specific advertising message may best convince this voter. At the same time, it may be hard to imagine how this evaluation can take place without taking the voter's political opinion into account. Even if the personal ‘raw data’ used does not in itself represent a political opinion, profiling at least amounts to inferring such political opinions of the voter. So either this is exactly what is meant, that at least the raw data used for profiling must not yet prescribe any political opinions. Or it is meant that political targeting may only take place on the basis of factual issues, but not on the basis of political convictions. Both questions therefore require further clarification.

In addition to these bans, the PTR is characterised above all by significantly **expanded transparency obligations**. In particular, Art. 11 and 12 PTR require the political advertising publishers to ensure that each political advertisement is made available together with information about, amongst other aspects, their sponsor, the election or referendum to which they are linked, and the amounts paid. Furthermore, in the case of political online advertising, Art. 19 sect. 1 PTR requires data controllers to provide, again together with the indication that it is a political advertisement, additional information necessary to enable the data subjects to understand how the advertisement that they are seeing is personalised to them. This includes, amongst other aspects, information about:

- the specific groups of recipients targeted, including the parameters used to determine the recipients to whom the advertising is disseminated;
- the categories of personal data used for the targeting techniques or ad-delivery techniques; and
- the period of dissemination of the political advertisement and the number of individuals to whom the political advertisement is disseminated.

It would have been helpful to have a clarification in the law that the controller must provide this information via a visual interface in direct connection with the advertisement shown. However, this requirement follows from the purpose of the requirement that this information must be provided with the indication that it is a political advertisement' anyway. So far, the PTR is hence concerned with ensuring that consumers receive this information in direct connection with the advertising, enabling them to better understand why they are seeing this advertising and no other. If implemented correctly, this can indeed be a very effective measure against the risk of manipulation as described above.

Art. 13 PTR requires, furthermore, that the information from Art. 12 sect. 1 PTR be made public in a **European online repository for each political advertisement**. The information shall be publicly accessible for the entire period during which the political advertisement is presented and for seven years after the political advertisement was last presented. An overview provided by such an online register has several functions: First, such a repository makes it possible to identify structural risks for society as a whole that only arise from the amount of all advertisements displayed on one or more platforms (see chapter 2.3.3.). Along the same lines are the duties in Art. 17 and 20 PTR, which require the disclosure of information to certain groups of people, such as vetted researchers, members of a civil society organisation, and journalists, are along the same lines. A public registry further encourages public debate by anyone.

Art. 12 sect. 2 PTR and Art. 19 sect. 3 to 4 also clarify **how the different actors must cooperate** to make sure that the publisher or controller is able to fulfil its transparency obligations and that the information is correct. For example, the actors must inform each other if they become aware that the information they have received from the other is incomplete or incorrect. For example, in the case of political online advertising, the actors must communicate the information to each other in a machine-readable format. They must also inform each other if they ‘become aware’ that the information received from the other is incomplete or incorrect.

Finally, the PTR even contains provisions forcing **publishers to accept the signals of consent agents** (Art. 18 sect. 4 lit. a PTR) and to provide a link for more direct exercise of data subject rights (Art. 19 sect. 1 lit, e PTR). Indeed, Art. 18 sect. 4 lit. a PTR only refers to cases where consumers have expressed their refusal to receive political advertising in advance. In particular, controllers must make sure that “the data subject is not requested to consent if he or she has already indicated by automated means that he or she does not consent to data processing for political advertising purposes, unless the request is justified by a substantial change of circumstances”. However, since a publisher naturally hopes to obtain consent, this provision means that publishers must read the signals from consent agents, and of course accept them in the event of a refusal.

In any case, here, too, more detailed provisions would have been desirable. Since consent agents and privacy dashboards for exercising data subjects' rights are still relatively unknown, the legislator could and should have provided a kind of guide for constructing these technical and organisational building blocks, which are so central for more effective data subject rights, by clarifying which actor has to provide which technical interfaces and with whom they have to exchange which signals.

3.4.3 Reasons for an eventually ineffective implementation in practice

As shown, the PTR contains some objective-structural provisions and even data subject rights that significantly concretise or supplement the GDPR. However, the PTR is also accompanied by questions, not only about how certain terms are to be interpreted, but also how they are to be implemented technically and organisationally. Probably the legislator itself did not have the detailed knowledge to provide such instructions. However, at least, the European Commission should provide such instructive details by way of the delegated acts and guidelines for which it is expressly authorised, at least in part (see Art. 12 sect. 6, Art. 19 sect. 5 as well as Art. 15 sect. 11 PTR). Since this authorisation does not apply to all the obligations mentioned here and the European Commission, even if it is authorised, does not always issue such delegated acts (see, for example, with respect to the much-vaunted privacy icons according to Art. 12 sect. 8 GDPR), it remains to be seen how effectively these provisions will be implemented in practice. Apart from this, a key factor for effective enforcement in practice will be, here again, which authority is responsible for enforcement. Since the areas of application of the various laws widely overlap, it is to hope that procedures will be harmonised as far as possible.

3.5 DIGITAL SERVICES ACT

The Digital Services Act (DSA)[380] contains similar provisions, but this time focussing on online platforms. With respect to personalised advertising, Art. 26 and 27 DSA contain mostly structural-objective regulations, but also some very interesting subjective rights.

3.5.1 Scope of application and regulatory goal

According to Art. 3 lit. i DSA, "'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public". With the regulations for online platforms, the legislator is responding to the risks posed by these platforms due to their ability to disseminate content, which alone or in its mass violates the rights of individuals or the common interests of society as a whole, and by the power of the platform operator to influence this dissemination.[381] The goal of the DSA therefore is, according to Art. 1 sect. 1 DSA, "to set out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected."

[380] 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), OJ L 277, 1-102.

[381] Hofmann/ Raue/*F. Hofmann*, Art. 1 DSA, para. 4, 16; Recital 9 DSA.

3.5.2 Complementarity with the GDPR

With regard to the personalisation of advertising, both the regulations for **online advertising** (Art. 26 and 39 DSA) and for recommender systems (Art. 27 and 38 DSA) are relevant. We begin with the more obvious rules for personalised advertising:

First of all, for online platforms, too, Art. 26 sect. 3 DSA **prohibits the use of sensitive data according to Art. 9 GDPR for profiling to personalise advertising**. Since the personalisation of advertising in general, unlike political advertising, does not necessarily imply the processing of political opinions or other sensitive data, the ban raises fewer questions here. However, it should be noted that protection limited to children and sensitive data is insufficient, since vulnerabilities arise not only from this social role or data, but also from other circumstances, depending on situations and contexts (see chapter 2.3.2.).

In addition, there are very similar transparency requirements to the PTR. Providers of online platforms must also "ensure that, for each specific advertisement presented to each individual" user, the user is "able to identify, in a clear, concise and unambiguous manner and in real time" that:

- the information is an advertisement, including through prominent markings;
- the natural or legal person on whose behalf the advertisement is presented, as well as the natural or legal person who paid for the advertisement if that person is different from the aforementioned person; and, most interestingly,
- meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

Here, too, the legislator is concerned with ensuring that **the consumer is able to understand**, in the immediate context of the advertisement, **why she or he is seeing this particular advertisement** and not another one. If implemented correctly, this can indeed be an effective measure against the manipulation risk and further risks as described.

Furthermore, according to Art. 26 sect. 2 DSA, online platforms must offer users the option of **indicating** whether the content they publish is or contains **commercial communications**; online platforms must also ensure that other users "can identify in a clear and unambiguous manner and in real time", such commercial communications. In doing so, Art. 26 sect. 2 DSA especially addresses influencer marketing, which is particularly widespread on online platforms.[382]

For very large online platforms (VLOPs)[383] and search engines, Art. 39 DSA also contains extended transparency obligations to "**make publicly available in a specific section of their online interface**, through a searchable and reliable tool that allows multi-criteria queries and through application programming interfaces, a repository containing" information, in particular, about

- the content of the advertisement, including the name of the product, service or brand and the subject matter of the advertisement;

[382] Hofmann/ Raue/ *Grisse*, Art. 26 DSA, para. 50.

[383] The European Commission designated 20 VLOPs and very large online search engines so far. For the current list see https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

- the natural or legal person on whose behalf the advertisement is presented, as well as the natural or legal person who paid for the advertisement, if that person is different from the person referred to in point (b);
- the period during which the advertisement was presented;
- whether the advertisement was intended to be presented specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose including where applicable the main parameters used to exclude one or more of such particular groups;
- the total number of recipients of the service reached and, where applicable, aggregate numbers broken down by Member State for the group or groups of recipients that the advertisement specifically targeted.

This information shall be available for the entire period during which they present an advertisement and until one year after the advertisement was presented for the last time on their online interfaces. As with the PTR, an overview provided by such an online register makes it possible to identify structural risks for society as a whole that only arise from the amount of all advertisements displayed on one or more platforms (see chapter 2.3.3.). Here, too, VLOPs are also subject to **access requirements for corresponding information**, in this case in favour of the so-called Digital Services Coordinator and, through her, vetted researchers, Art. 40 DSA.

In contrast, unlike the PTR, Art. 26 and 39 DSA contain **no further provisions on cooperation obligations, the integration of consent agents or support in the exercise of data subject rights**. The legislator may have considered these superfluous in view of the horizontal and vertical integration of the various data processing phases; on platforms, all online advertising services come from a single source anyway. In this case, there is indeed no need to ensure the integration of such third-party services.

However, the provisions in Art. 27 DSA on **recommender systems** represent a clarification or complement to the rights of data subjects, at least in comparison to the GDPR. Unlike the GDPR, the provisions on recommender systems are not linked to the specific risks of processing personal data, but to the use of certain technologies. Since some online platforms are financed by displaying personalised advertising and such a personalisation is mostly based on recommender systems, Art. 27 DSA is highly relevant for this report.[384]

First of all, Art. 27 DSA contains objective transparency provisions which aim to explain the functioning of these recommender systems to the platform users. Unfortunately, this information gets, however, hidden in the general terms and conditions of an online platform. A bit more interesting are the provisions that force online platforms, in the case of various options for displaying recommended content, to enable the user to select and modify at any time their preferred option. This functionality must be directly and easily accessible from the specific section of the online platform’s online interface where the information is being prioritised. However, since platforms offering several recommender options will promote this as a special feature of their platform anyway, the added value of this provision will also be limited in practice. Much more interesting are the similar provisions for VLOPs:[385] Art. 38 DSA **forces these providers to offer at least one option for their recommender system which is not based on profiling**.

[384] Hofmann/ Raue/ *Grisse*, Art. 27 DSA, para. 1.

[385] These provisions equally apply to very large online search engines.

Due to the broad definition of profiling, any personalisation of advertising is likely based on profiling. This means that these very large providers must always display a non-personalised advertising option, as an alternative to personalised advertising. Since Art. 27 DSA, as a more general provision, also applies to VLOPs,[386] this option must also be "directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised". This is nothing else than the above-proposed on/off toggle, which enables consumers to experience the added value of personalised advertising for themselves by comparing it in personalised and non-personalised form (see chapter 4.2.2.).

Finally, the DSA – following the example of the GDPR – provides co-regulatory instruments, in particular codes of conduct according to Art. 46 DSA (see also chapter 2.5.8.3.).[387]

3.5.3 Implementation in practice

Similar to the PTR, the DSA is accompanied by considerably extended transparency regulations for personalised advertising. However, the DSA addresses the special features of online platforms. For example, there are no specific provisions on the co-operative transfer of information between online advertising services or on the integration of consent agents and privacy dashboards from third-party providers. These seemed unnecessary to the legislator, given that all services on platforms usually come from a single source anyway. On the other hand, there are specific requirements for recommender systems. According to Art. 38 and 27 DSA, VLOPs must provide the on/off toggle required above. Indeed, it will be interesting to see whether or how effectively online platforms implement the extended transparency requirements for online advertising and VLOPs implement the on/off toggle for recommender systems, which may finally enable users to weigh up whether the added value of personalised advertising is worth the corresponding risks.

It will also be interesting to see how the DSA is enforced. Pursuant to § 12 sect. 1 of the German Digital Services Act (DDG), the Federal Network Agency (Bundesnetzagentur) is the competent authority in Germany in accordance with Art. 49 sect. 1 DSA. In addition, there are some special competences of other authorities regulated in § 12 sect. 2 and 3 DDG, namely for the Federal Center for the Protection of Children and Young People from Harmful Media (Bundeszentrale für Kinder- und Jugendmedienschutz) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

Pursuant to § 12 sect. 3 DDG the BfDI is competent to enforce Art. 26 sect. 3 and Art. 28 sect. 2 and 3 DSA. This allocation of competence to the BfDI has already been criticised, as the Federal Council (Bundesrat) favoured the data protection authorities of the federal states being competent and proposed a corresponding amendment in the legislative process.[388] The Federal Council justified its proposal by stating that the addressees of the obligations under Articles 26 and 28 DSA are exclusively non-public bodies which, according to § 40 of the Federal Data Protection Act, essentially fall within the competence of the federal states. The necessary expertise and enforcement experience can therefore be found there (not with the BfDI). The Federal Council

[386] Hofmann/ Raue/ *Grisse*, Art. 27 DSA, para. 11.

[387] Jaursch, What DSA codes of conduct for online advertising can achieve Opportunities and limitations of voluntary action and the need to move beyond it, Interface Policy Brief, 16.12.2024.

[388] BT-Drucks. 676/23, 2.2.2024, p. 1 et seq.

criticised the fact that the regulation in § 12 sect. 3 DDG leads to a splitting of data protection complaint procedures, which in turn results in an additional need for coordination between the BfDI and the state data protection authorities. The Federal Council's proposed amendment was rejected by the Federal Government on the grounds that the supervision should be as uniform as possible.[389] The DDG came into force on May 14, 2024, it remains to be seen whether this decision proves to be correct.

3.6 DIGITAL MARKETS ACT

The Digital Markets Act (DMA)[390] - like the DSA - originates from the 2022 EU initiative that aims to create a safer digital space when using online services.

3.6.1 Scope of application and regulatory objective: ensure fairness by limiting power concentration

With the DMA the legislator is seeking to take on a direct influence on too excessive concentration of market power by certain digital platforms. While the DSA specifies rules that primarily concern online intermediaries and platforms in general, the DMA focuses on specific gatekeepers. These are digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services, leading to the dependency of these users on the platform.

The DMA supplements competition law by trying to put a stop on unfair behaviour vis-a-vis business and end users that is caused by the size and entrenched position of the gatekeepers. By limiting the power of dominant digital platforms inter alia by preventing them to commercially exploit the data that they are easily able to collect from users the DMA aims at the heart of data economy. No surprise Art. 5 sect. 2 DMA was one of the most heavily discussed rules in the legislative process.[391]

The DMA focusses on gatekeepers that are an undertaking providing core platform services and have been designated pursuant to Art. 3 DMA. According to Art. 2 no. 2 lit. j DMA “core platform service” inter alia means “online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i)”. Some of these services are also addressed in the DSA, but for different reasons and with different types of provisions (see chapter 4.6.).

Until May 2024 the European Commission designated seven gatekeepers under the DMA, Alphabet, Amazon, Apple, Booking, ByteDance, Meta and Microsoft.[392] In total, 24 core platform services provided by those gatekeepers have been designated, three of which are online advertising services (Alphabet's online advertising service[393], Amazon Advertising[394] and Meta Ads[395]).

[389] BT-Drucks. 20/10281, 7.2.2024, p. 12.

[390] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 1-66.

[391] Podszun/ *Podszun*, Art. 5 DMA, para. 12.

[392] https://digital-markets-act.ec.europa.eu/gatekeepers_en.

[393] European Commission, Designation decision of 5.9.2023, EU OJ C/2023/549 of 27.10.2023.

[394] European Commission, Designation decision of 5.9.2023, EU OJ C/2023/905 of 15.11.2023.

[395] European Commission, Designation decision of 5.9.2023, EU OJ C/2023/1092 of 23.11.2023.

3.6.2 Objective obligations, subjective rights and responsibilities

The architecture of the DMA differs significantly from traditional competition law as it is a “self-executing” regulation which establishes 18 obligations that apply ex ante and per-se for gatekeepers as providers of core platform services.[396]

Art. 5 to 7 DMA contain the core of specific requirements for gatekeepers, of which Art. 5 sect. 2 DMA is most significant for the subject of this report. Art. 5 sect. 2 DMA states a prohibition for gatekeepers relating to the use, combination or cross-use of personal data without specific consent of the user. Without such consent, the gatekeeper has to keep separate data silos for each of its services, which includes the prohibition of transferring personal data from the core platform service to generative AI. Thus a gatekeeper shall

- **not process, for the purpose of providing online advertising services**, personal data of end users **using services of third parties** that make use of core platform services of the gatekeeper,
- **not combine** personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services,
- **not cross-use** personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa, and
- **not sign in** end users to other services of the gatekeeper **in order to combine** personal data,
- unless the end user has been **presented with the specific choice and has given consent** within the meaning of Art. 4 no. 11 and Art. 7 GDPR. Where the consent given for the aforementioned purposes has been refused or withdrawn by the user, the gatekeeper **shall not repeat** its request for consent for the same purpose more than once **within a period of one year**.

Art. 5 sect. 2 DMA does not actually create further substantive legal requirements, but clarifies that Art. 6 sect. 1 lit. b and f GDPR are no proper legal bases for the mentioned use, combination or cross-use of personal data.[397] The regulation, however, is without prejudice to the possibility for the gatekeeper to rely on Art. 6 sect. 1 lit. c, d or e GDPR, where applicable. Gatekeepers can therefore only merge data if they either receive consent following a specific choice or if specific circumstances for the existence of one of the grounds of Art. 6 sect. 1 lit. c-e GDPR are met.

On the one hand, this means the regulation does not preclude the possibility that a gatekeeper uses personal data without explicit consent as required according to Art. 5 sect. 2 DMA within its own respective core platform service.[398]

On the other hand, the prohibition to use, combine or cross-use personal data for the performance of a contract or on the basis of legitimate interests can be overridden by means of consent. Whether the DMA can achieve its objectives therefore stands and falls with the requirements for effective consent. In other words: consent remains the achilles’ heel of data protection.[399]

The DMA does not contain any specific requirements for consent, but refers directly to Art. 4 no. 11 and Art. 7 GDPR. Accordingly, the same standards apply as laid down in

[396] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, pp. 63, 64.

[397] Gersdorf/ Paal/ *Louven*, Art. 5 DMA, para. 38, 39.

[398] Podszun/ *Podszun*, Art. 5 DMA, para. 10; Gersdorf/ Paal/ *Louven*, Art. 5 DMA, para. 23.

[399] Podszun/ *Podszun*, Art. 5 DMA, para 13.

the GDPR but likewise the same interpretation questions may 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 may influence how the law is applied. Other than the GDPR, however, in its recitals the DMA comments on inadmissible user manipulation. According to recital 37 “Not giving consent should not be more difficult than giving consent. When the gatekeeper requests consent, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner. [...] Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent.” The DMA hereby leaves no doubt that the option to refuse consent must be possible with the same amount of clicks as giving consent in order to be freely given. This clarification is of great significance, since this design issue has been addressed by data protection authorities for years,[400] while the industry tried to argue that reject-options only at a second banner level fulfil the requirements according to Art. 4 no. 11 GDPR. Beyond that, Art. 5 sect. 2 DMA comments on the design of consent in one specific aspect, namely that a repeated request is only permissible after one year due to the harassment effect.

Art. 5 sect. 2 DMA furthermore provides for the gatekeeper to present users with “specific choice”. The practical implications of this reference is not entirely clear. At first glance, the term “specific choice” may be understood like “for the specific case” in Art. 4 no. 11 GDPR. Such interpretation, however, is contradicted by the wording, saying that the criterion of specific choice is additional to consent (“and”). Against this background, separate consent is required for each of the individual four use cases defined in Art. 5 sect. 2 DMA. A blanket general consent does not meet the requirements.[401]

Furthermore, according to recital 36 and 37 “gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user’s consent. [...] The less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent [...]” On the one hand, this means that the refusal of consent must have no consequences for the provision of the service by the gatekeeper. On the other hand, there is an obligation to proactively offer the end user different versions, between which she or he may choose. Such an *obligation to offer* alternatives is not yet provided for by the GDPR.[402]

According to recital 37, consent may exceptionally also be given via third-party services (e.g. an app that is used), but must nevertheless clearly refer to the gatekeeper service. In consequence it is possible to involve data trustees, PIMS, a central consent management tool or other intermediaries.[403]

Finally Art. 8 sect. 1 DMA safeguards the DMA strategy by requiring gatekeepers to provide proof of compliance. This is a real power shift – in comparison to competition

[400] See inter alia EDPB, Report of the work undertaken by the Cookie Banner Taskforce, 2023, para. 6 et seq.; DSK, Orientierungshilfe Telemedien, 2022, para. 48 and 54 et seq.; for further publications regarding cookie banner design, see footnote 140.

[401] Podszun/ *Podszun*, Art. 5 DMA, para 13.

[402] Gersdorf/ Paal/ *Louven*, Art. 5 DMA, para. 33.

[403] Podszun/ *Podszun*, Art. 5 DMA, para 23.

law – and places a burden of accountability on gatekeepers, not a burden of proof on the authorities.

While the DMA's provisions are intended to curb the power of gatekeepers, they can also be used in practice as leverage to implement more effective consent designs. Gatekeepers, as in the case of Google, usually pass on the collection of consent to their customers, e.g. the website operators. For doing so, Google recommends using certain Google-certified CMPs, which in turn obtain the corresponding consent for the website operator.[404] We have not further examined the conditions under which CMPs can become partners of Google. However, we doubt that Google checks whether and to what extent website operators and CMPs comply with the conditions for effective consent under Art. 6 sect. 1 lit. a and Art. 25 sect. 1 GDPR. In enforcing the law, authorities could therefore make use of the leverage effect of Art. 5 sect. 2 DMA by providing more specific guidelines for designing the required consents. Google would then pass these conditions on to website operators and CMPs, thus leading to an abrupt improvement in the effectiveness of the consent.

3.6.3 Complementarity with the GDPR

While the GDPR and DMA pursue different goals and purposes of protection, the DMA specifies the GDPR in some areas of personalising advertising. Generally, the GDPR opens up six legal bases for data processing, from which Art. 5 sect. 2 DMA excludes two when it comes to some legally defined scenarios of processing. Likewise the GDPR requirements regarding effective consent are clarified within the DMA to some extent.

Art. 5 sect. 2 DMA only applies from May 2023. However, a lot is already happening in terms of compliance inspections. In March 2024, the European Commission opened four investigations for non-compliance according to Art. 20 DMA, two of them against Alphabet, one against Apple and one regarding Meta's “pay-or-consent model”.[405]

Regarding the latter, the Commission informed Meta in July 2024 of its preliminary findings that its “pay or consent” advertising model fails to comply with Art. 5 sect. 2 DMA. In the Commission's preliminary view, the binary choice forces users to consent to the combination of their personal data and fails to provide them a less personalised but equivalent version of Meta's social networks.[406] If the Commission's preliminary views were to be ultimately confirmed, the Commission would adopt a “non-compliance decision” according to Art. 29 DMA and can impose fines up to 10% of the gatekeeper's total worldwide turnover in accordance with Art. 30 DMA. Such fines can go up to 20% in case of repeated infringement. Moreover, in case of systematic non-compliance, the Commission is also empowered to adopt additional remedies such as obliging a gatekeeper to sell a business or parts of it or banning the gatekeeper from acquisitions of additional services related to the systemic non-compliance.

In its decision regarding the Bundeskartellamt and Meta, the ECJ held that national competition authorities must seek “sincere cooperation” with the competent data protection authorities when relying on GDPR issues for competition law enforcement, hence they cannot depart from decisions by the competent GDPR authorities.[407]

[404] See the so-called consent mode described at https://developers.google.com/tag-platform/security/guides/consent?hl=de&consentmode=advanced.

[405] EU Commission, press release, 25.3.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689.

[406] EU Commission, press release, 1.7.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582; Meta has the possibility to exercise its rights of defence now; the Commission will conclude its investigation within 12 months from the opening of proceedings.

[407] ECJ, 4.7.2023, C-252/21, para. 63 – Meta Platforms (Facebook Ireland).

Regarding DMA enforcement actions by the European Commission it may be expected that this duty to cooperate also applies.[408]

3.6.4 Implementation in practice

The alternative approach of the DMA was chosen by politicians and regulators due to the perceived lack of meaningful enforcement of the GDPR.[409] In fact not only the creation of comprehensive user profiles and the personalisation of advertising is made more difficult this way, but rather solves procedural difficulties that arose in a case regarding the Bundeskartellamt.[410] Art. 5 sect. 2 DMA is thus an obligation that adds to the requirements under the GDPR, potentially making data protection more successful than it had been so far.[411] Whether these plans will work out in the long term remains to be seen, since no supervisory procedures have been completed since the regulation came into force in May 2023.

However, it is already becoming apparent that the DMA is not suitable to generally solve the fundamental problem and risks that arise from the current online advertising ecosystem. In fact it only applies to a handful of gatekeepers and a selection of processes. Even though they are the most important players in the industry that hold by far the largest share of the system, the approach of the DMA does not shed the necessary light into the complex system - it won't get more transparent, more comprehensible or less data-driven.

Beyond that, the user-centricity of Art. 5 sect. 2 DMA is remarkable: The prohibition to use, combine or cross-use personal data for the performance of a contract or on the basis of legitimate interests can be overridden by means of consent. Whether the DMA can achieve its objectives therefore stands and falls with the requirements for effective consent. The obligations of Art. 5 DMA do not refer in any clear way to informational or behavioural manipulative strategies (except in its recitals).[412] Therefore immense disputes are to be expected in practice about the conditions of consent and the impact of dark patterns, since the requirements for this are based on the GDPR. If the gatekeepers succeed to obtain (valid) consent, which may happen given their skills in seducing consumers and in building a profitable 'choice architecture', they can continue to use their data power.[413]

During the legislative process it was therefore already questioned whether to replace Art. 5 sect. 2 DMA through a direct prohibition of the combination of personal data from different services and sources without allowing gatekeepers to get consent is a more effective approach with respect to competition and data protection.[414]

3.7 CONCLUSION: REGULATORY GAPS AND POSSIBLE SOLUTIONS

In this chapter, we have analysed several laws relevant to personalised advertising in terms of whether and how they protect against the risks for consumers and society as a

[408] Podszun/ *Podszun*, Art. 5 DMA, para. 22.

[409] Podszun/ *Podszun*, Art. 5 DMA, para 12.

[410] Bundeskartellamt, 5.10.2023, B7-70/21, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf?__blob=publicationFile&v=4.

[411] Podszun/ *Podszun*, Art. 5 DMA, para. 10.

[412] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 88.

[413] Podszun/ *Podszun*, Art. 5 DMA, para. 11.

[414] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, pp. 71, 74.

whole, as shown in chapter 2.3. These laws can be read as a learning curve in the course of which the legislator addressed the problems that arise, particularly in the application of the GDPR, in ever more concrete terms:

The analysis showed that the **GDPR**, due to its broad scope of application and comprehensive approach to protection, is actually well-suited to capture the multifaceted risks for both individual consumers and society as a whole. In particular, the GDPR provides not only subjective data subject rights but above all numerous objective requirements for the processing of personal data, which form the actual basis for transparent and controlled processing that can be intervened in by consumers. Controllers must specify the purposes of data processing, document these together with the types of data processed, of data subjects and data recipients, make the processing transparent to the data subjects and provide them with numerous rights of intervention. If controllers pass the data on to recipients, there are numerous regulations to clarify who has to fulfil which rights and obligations. None of them may process the data in a way that is incompatible with the original purposes, and all of them must protect the data against unauthorised access, loss and alteration. Furthermore, all of this must be implemented in the technical and organisational design of the data processing so that this provides proven effective (!) protection against the risks. As mentioned above, the GDPR even provides co-regulation instruments (though voluntary), in particular certification mechanisms and codes of conduct, which data controllers and processors can use to reduce legal uncertainty and demonstrate compliance with all these regulations. Last but not least, by accessing the processing records and so on, data protection authorities would even have the possibility of identifying structural risks that only arise from an overall view of all processing operations that take place. The only problem is that all these provisions, with their numerous legal principles and undefined legal terms, leave so much room for interpretation that the addressee of the regulation can basically circumvent or call into question every single provision in each individual case. Together with the limited resources of the data protection authorities, as well as complex cooperation procedures, this leads to an extremely large compliance and enforcement deficit in practice.

Against this background, it was important to work out in what way other laws applicable to the personalisation of advertising do or, at least, may compensate for these deficits of the GDPR. Starting with the **ePrivacy Directive** which sets specifications to protect one's privacy when using a terminal equipment, regardless of whether or not personal data is processed. This means Art. 5 sect. 3 ePD applies beyond the scope of the GDPR by setting high hurdles directly at the gateway of a process chain, which usually develops like a domino effect on subsequent data processing. Even though Art. 5 sect. 3 ePD has the longest history and probably the biggest target group among all laws that regulate risks associated with personalised advertising, conceptual and technology wise it isn't at the cutting edge (anymore). On the one hand, the law focuses on legitimising the justifiable processes via consent – only very limited alternatives apply. On the other hand the application of Art. 5 sect. 3 ePD is well established and implemented for some tracking technologies such as cookies, but lacks guidance for the technical landscape that has been evolving during the last decade. This creates uncertainties and disputes about the scope of application, causing the law to lose its effectiveness. But the neuralgic point as to why the Directive is barely able to counter the risks of the advertising market is its low level of harmonisation leading inter alia to a chaotic supervisory structure. In its current version, therefore, the ePrivacy Directive ultimately falls short of its necessary impact.

In view of these deficits of the ePrivacy Directive, it was interesting to take a look at other laws that focus on further regulatory approaches for transparent, controlled and intervenable data processing. The first thing that stands out is the **AI Act**, which, based on or at least inspired by product safety law, focuses on structural-objective requirements. These requirements are not primarily aimed at enabling transparent, controlled and intervenable processing of personal data. However, due to the broad definition of AI systems (one might almost speak of an algorithm liability law), there is a significant overlap between its own and the GDPR's material scopes of application. Since the AI Act, unlike the GDPR, primarily holds IT providers liable rather than its deployers, both laws are complementary in their personal scope of application. Against this backdrop, it is interesting that the AI Act outright prohibits some AI practices that appear to be also relevant for the area of personalised advertising. The extensive provisions on the technical and organisational design of high risk AI systems and the cooperation between actors along the value chain could also compensate for the shortcomings of the GDPR described above. With respect to the latter, the AI Act, comparable to the regulatory tools used in the REACH Regulation, is primarily concerned with ensuring that all actors involved in the value chain exchange all the necessary information that is needed for effective protection against the risks of AI systems, from the provider, to the importer and distributor, up to the deployer. Such regulations might significantly help to clean up the messy and chaotic state of data processing in the online advertising ecosystem, as described. However, since these regulations only apply to the high-risk AI systems listed in Annex III and do not cover the personalisation of advertising (except probably in the area of political election advertising), they are not directly applicable to the personalisation of advertising. However, alongside the provisions of the REACH Regulation they provide a very good example for how coordination between players in the online advertising sector should be regulated.

The **Political Targeting Regulation** and the **Digital Services Act** also provide interesting insights for a more effective regulation of personalised advertising. The PTR sets out some requirements for when personalised political advertising may and may not be used. Above all, however, both the PTR and the DSA provide numerous specifications and supplementary requirements for how the controller must fulfil its transparency obligations and, building on these, the possibilities for consumer intervention. Both laws also regulate the protection of vulnerable groups and/or special categories of data. The protective mechanisms of both laws also address not only individual risks for consumers (in particular through individual information requirements and rights of intervention) but also structural risks for society as a whole (in particular in the form of data access rights for external audits and public registers, as well as risk management obligations). The PTR even defines rules for the integration of PIMS and how the various actors must work together so that the publisher can meet the transparency requirements.

In particular, Art. 18 PTR contains provisions forcing publishers to accept the signals of consent agents and to provide a link for more direct exercise of data subject rights. Here, too, more detailed provisions would have been desirable. **Since consent agents and privacy dashboards** for exercising data subjects' rights **are still relatively unknown, the legislator** could and **should** have **provided a kind of guide for constructing these technical and organisational building blocks**, which are so central for more effective data subject rights, by clarifying which actor has to provide which technical interfaces and with whom they have to exchange which signals. Probably the legislator itself did not have the detailed knowledge to provide such instructions. However, at least, the EU Commission should provide such instructive details by way of the delegated acts and guidelines for which the Commission is authorised.

In conclusion, the analysis of the further law shows that the legislator has increasingly addressed the deficits of the GDPR in a more and more specific way. These include, in particular, 1) the clarification of legal requirements for specific sectors and actors; and 2) a clear assignment of technical and organisational cooperation obligations to overcome governance problems (and knowledge deficits) in complex processing networks. Of course, these regulations are only applicable to specific technologies, areas or actors. If some of these regulations were to apply to the personalisation of advertising in general, which we definitely recommend, this would need its own law. Of course, this law should tie into already existing self-regulatory structures of the online advertising ecosystem (see especially the TCF described in chapter 2.2.4.) and streamline the diversity of already existing laws. This ensures that the regulatory burden for companies remains far below the economic and social benefits that result from the effective solution to the governance problem of the self-regulation approach as previously described.

Last but not least, the analysis of regulations that have a direct impact on competition also provided interesting insights into possible additional regulation of the online advertising market. For example, data protection authorities may use Art. 5 sect. 2 **DMA** as a leverage to improve the effectiveness of consent on a large scale. Actually, Art. 5 sect. 2 DMA only says that gatekeepers are allowed to process the data of end users generated by the use of third-party services that in turn use core platform services of the gatekeeper, only if they have obtained consent of these end users. In practice, however, gatekeepers like Google pass this obligation on to the website operators. Authorities could take advantage of this practice by specifying concrete conditions for gatekeepers under which they consider consent to be effective within the meaning of Art. 6 sect. 1 lit. s and Art. 25 sect. 1 GDPR.

Another example of where the legislator is seeking to take on a direct influence on market structures is the **Data Governance Act (DGA)**. In Chapter III, the legislator seeks to create a regulatory framework for so-called data intermediation services. According to Art. 10 lit. b DGA, providers of consent agents and privacy dashboards also fall within the scope. This is important because Art. 12 DGA sets out a number of conditions for providing data intermediation services. So if, for example, Apple or Google offer consent services that allow its users to manage their consents given on websites (see chapter 2.5.1.2.), these companies would have to comply with these additional requirements. In short, browser providers would only have to establish a separate legal entity to provide the consent management service within the meaning of Art. 10 lit. b DGA, and this entity would not be allowed to use the data collected for its own purposes (Art. 12 lit. a DGA). This service would then support the actual data-collecting service of Google or Apple in collecting the data from the consumers. However, in conclusion, these requirements do not impose any major restrictions on companies with market power such as Apple and Google. In contrast, it would have been possible to introduce stricter regulation, at least, for gatekeepers, up to their exclusion from providing such services, given their tendency to accumulate even more information power by providing such services.

The fact that the regulator dares to regulate companies with a great deal of information power more strictly is demonstrated not only by the DSA and DMA, but also by the recently enacted Data Act. The **Data Act** legally recognises the users of data-driven services as the actual owners of the data generated through their use and thus gives them comprehensive access and portability rights vis-à-vis the service providers. Users of the services may therefore request from the provider not only the transmission of the data to themselves, but also to third-party providers. The legislator thereby seeks to promote the dissemination and reuse of this data and thus the innovative capacity of the European data economy (see, for example, recitals 1, 15, 19, 32). This applies in particular to the innovative capacity of smaller companies vis-à-vis large providers. For this reason, according to Art. 5 sect. 3 DA gatekeepers are excluded from the potential group of data recipients. Service users may therefore request that data be transferred to third parties other than gatekeepers. At the same time, the gatekeepers are, of course, subject to the data sharing obligations. Thus, if they themselves are providers of data-driven services, they must share the data at the request of the service user. Of course, it remains to be seen to what extent these regulations are suitable for countering the threat of a further increase in the power of information in the hands of already large companies. But the regulation does show that European legislators are not squeamish about excluding gatekeepers from certain rights. A ban on gatekeepers providing certain services, such as consent agents or privacy dashboards, while they are under an obligation to accept the technical signals from such services, is therefore an obvious step.

In conclusion, this chapter turned to the regulatory aspects by raising the following questions: To what extent does existing law provide suitable building blocks to adequately protect consumers from the risks described above? What gaps and problems still exist? Which regulatory approaches or elements might be transferred from other laws to close these gaps or solve these problems? When analysing the laws, they could be read as a learning curve for the legislator, in the course of which the legislator addresses the shortcomings of the GDPR more and more clearly, albeit only in relation to specific players, technologies and sectors. Only when it comes to the question of the competent authorities and the coordination procedures between them, it appears that the coordination difficulties increase with every law that overlaps in its scope. Against this background, we will now clarify certain basic assumptions (see chapter 4) on which our regulatory proposals for regulating personalised advertising will be based (see chapter 5).

4 PRECONDITIONS FOR (RE-) ESTABLISHING A MARKET BETWEEN CONSUMERS AND ADVERTISERS

The regulatory options we propose in chapter 5 are based on the assumption that the conceptual and practical constraints of informed consent described above can be overcome. To this aim, this chapter clarifies the legal, technical and organisational requirements that are necessary to ensure effective consent and thus a direct feedback loop between consumers and advertisers, i.e. a market. In doing so, this chapter focuses on the consumer side of such a market and only discusses some important implications for the advertiser side. Thus, this chapter does not fully take all interests of the advertiser side into account, in particular not their need to measure the success of their chosen type of advertising more reliably and the requirements this would place on advertising service providers.[415]

4.1 CONCEPTUAL STARTING POINT: HOW TO CLOSE THE FEEDBACK LOOP BETWEEN CONSUMERS AND ADVERTISERS

So far and in theory, consent could be a suitable protection instrument by means of reflecting the different privacy expectations and risk considerations of consumers.[416] Privacy expectations and risk assessments are subjective per se, even if they can be objectified by referring to common interests and risk assessment methods.[417] In other words, it is possible to establish an objective, i.e. shared understanding of the risks that personalised advertising poses for individual consumers and society as a whole (see chapter 2.3.) and how these risks can be determined and assessed.[418] However, it depends on the subjective attitudes of every individual consumer as to whether they consider the probability of a certain risk materialising, the extent of possible harm and the ratio of this risk to the expected added value to be significant. Effectively informed consent would therefore lead to all consumers choosing the optimal form of advertising for themselves, depending on which risk-benefit ratio they prefer. Such an effectively informed consent would have far-reaching consequences for the online advertising market.

The reason for these far-reaching effects are that these individual risk-benefit considerations lead to purpose-specific consent rates across all consumers, i.e. user pools of different sizes: the higher the consent rate for a particular processing purpose, the larger the potential end user base that an advertiser can reach with the respective advertising type. Advertisers can then weigh up which advertising type to choose, taking into account 1) the number of potential end users that can be reached, 2) the expected conversion rate of this type of advertising and 3) the price they have to pay for this advertising type (as well as further aspects such as brand safety)[419]. Informed consent would thus create a direct feedback loop between consumers and advertisers with regard to the respective advertising type chosen. Perhaps one could even call this a market in which supply and demand for certain types of advertising get into an equilibrium according to the aforementioned criteria that consumers and advertisers consider relevant; for this market, not only the advertisers, but also the publishers would then just be brokers (though we are, of course, no economists).

With this objective in mind, our regulatory proposals are conceptually based on the approach of regulating innovation. According to this approach, laws should be designed in such a way that they provide effective protection against the risks of (data-driven) innovation and do not only unnecessarily hinder but even promote innovation.[420] This

[415] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 113 et seq.

[416] Masing, Herausforderungen des Datenschutzes, 2012.

[417]Jaeckel, Gefahrenabwehrrecht und Risikodogmatik, 2010, pp. 51 and 52, by referring to Evers/ Novotny, Umgang mit Unsicherheit, 1987, and to Luhmann, Soziologie des Risikos, 2003, pp. 30 ff, as well as, ibid., Die Moral des Risikos und das Risiko der Moral, 1993, pp. 327 and 331.

[418] Art. 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248), 2017.

[419] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 245 et seq. (chapter Areas for further analysis).

[420] Hoffmann-Riem/ Fritzsche, Innovationsverantwortung – Zur Einleitung, 2009, p. 16.

approach thus focuses on the innovative capacity of markets,[421] and fits in well with the EU's understanding of enabling and maintaining innovative (data-driven), but also value-orientated markets.[422] Thus, our regulatory approach is primarily aimed at creating a (more direct) market between consumers and advertisers by creating a (much more direct) feedback loop between the parties. We are doing this with the aim of enabling advertisers and service providers to compete for consumers' approval (rating) by developing ever more user-friendly advertising technologies. However, to create such a market via more immediate feedback loops, the following conditions for informed consent had to be met.

4.2 REQUIREMENTS FROM THE CONSUMER PERSPECTIVE

In chapter 2.4.2., we painted a disastrous picture of the current implementation of informed consent, drawing on numerous empirical studies. The abundance of opaque, deceptive and manipulative consent designs lead to consent fatigue and put consumers in a state of powerlessness and fatalism. Consumer confidence in the processing of online advertising is so shattered that it seems difficult to restore. Nevertheless, there are studies that show how consent processes may be designed more effectively and even how consumer trust may be regained.

4.2.1 Consent mechanisms design: clear information about benefits and risks

To answer these questions, over the last years research has developed many different design parameters and also specific designs for transparency and intervention measures, such as consent in various use contexts.[423] In several specific research projects, a research group has tested some of these designs both qualitatively and quantitatively to see how well they enable consumers in different contexts of use to understand the benefits and risks associated with the respective purposes of processing their data and to control them accordingly. The prototypes developed and tested focused on cookie banners, consent agents and privacy dashboards, which consumers may use to exercise their data subject rights, such as data access, data correction and data deletion. The development of these prototypes and numerous smaller, qualitative tests showed that information and consent processes can indeed be designed to be more effective than those designed according to current best practice rules (see above chapter 2.4.2.1.). The essential parameters here are which information is presented in which textual and visual form, as well as how much space,

[421] Wegner, Gerhard: Nachhaltige Innovationsoffenheit dynamischer Märkte, in: Martin

Eifert / Wolfgang Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation

und Recht II, Berlin: Duncker & Humblot, 2009, pp. 71–91; with respect to data protection law, v. Grafenstein, M. The Principle of Purpose Limitation in Data Protection Law, pp. 617 et seq.

[422] See the goals of the EU with respect to its innovative capacities and European values, for example, at https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

[423] Kitkowska et al., Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect, SOUPS 2020, pp. 437 et seq.; Schaub et al., Designing Effective Privacy Notices and Controls, IEEE 2017, pp. 70-77; Gluck et al., How short is too short? Implications of length and framing on the effectiveness of privacy notices, SOUPS 2016, pp. 321 et seq.; McDonald et al., A Comparative Study of Online Privacy Policies and Formats, PET 2009, pp. 37 et seq.; regarding control, for example, at Habib et al., Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts, CHI 2021; Feng et al., A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things, CHI 2021; Schaub et al., Designing Effective Privacy Notices and Controls, IEEE 2017, pp.70 et seq.; ConPolicy, Good Practice Initiative for Cookie Consent, 2023, as well as the final report of the preceding project both funded by the German Ministry of Education and Research “Innovatives Datenschutz-Einwilligungsmanagement”, available under https://www.conpolicy.de/referenz/innovatives-datenschutz-einwilligungsmanagement.

time, attention and opportunities the user has to process and even learn the information over time.[424]

On this basis, the research group also conducted a current quantitative study with 349 participants. In this A/B test using a fictitious plant webshop, the group sought to find out, on a broader user base, which cookie banner designs better inform consumers about the respective benefits and risks and how the use of a consent agent affects these results.[425] As mentioned previously, consent agents are an important building block for more effective transparency and user control. By giving the user the opportunity to familiarise themselves with the processing of their data within their consent agent in advance, there is more space, more time and more attention available for the user to process the information. Most importantly, the user is no longer forced to give their consent on every single website they visit, which avoids the resulting consent fatigue.[426]

In this quantitative test, the research group showed to each study group the same four processing purposes in the cookie banner designs. The research group then compared the current best practice cookie banner with an alternative cookie banner design, in which they showed the benefits and risks of each purpose on the first visual level. In a third study group, the research group additionally tested the effects of adding a consent agent to this alternative cookie banner. To do this, the participants in this study group had to download a browser extension and give their preference for the purposes mentioned. In doing so, the research group also presented the data typically processed for these purposes, the way the data is processed, and the advertising partner network behind it. These pre-settings were then passed on to the plant webshop as soon as the participants accessed the webshop. In this case, a handover notice informed the study participants that their pre-settings would be forwarded to the fictitious webshop in 12 seconds if they did not wish to make any adjustments to their pre-settings. If the participants did not react, i.e. did not adjust their presettings, their presettings were passed on to the webshop after 12 seconds and the handover notice disappeared by itself (“automatic time-out”). Finally, in a fourth and fifth study group, the research group tested in two further variants how a data protection seal and the information that the fictitious webshop uses particularly data protection-friendly tools and therefore poses fewer risks for consumers affect their informedness and consent behaviour.

The study results show that a clear formulation of the processing purposes, the supplementation of these purpose formulations by presenting their benefits and risks for consumers (already at the first visual level) and the use of privacy icons may contribute to a better understanding by consumers of the risks caused by the respective purpose. The additional use of a consent agent improves even further the consumers’ understanding.[427] In conclusion, the prototypes developed and the results of the studies show that it is possible to design more transparent and effective consent processes if the appropriate interdisciplinary methods as well as technical and organisational conditions are in place. In this regard, it is important to note that the scope for such

[424] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review, 2024.

[425] V. Grafenstein, Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, SSRN 2024, pp. 41 et seq.

[426] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 2024, pp. 20 et seq.

[427] V. Grafenstein/ Kiefaber/ Heumüller/ Rupp/ Graßl/ Kolless/ Puzst, Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR, Computer Law & Security Review, 2024, p. 23.

improvements seems far from exhausted, as a glance at the rough conceptual prototypes used for these studies suggests (see the conceptual designs in **Annex 3**).

4.2.2 Consent mechanisms advantages: Verification of personal relevance

Further empirical studies also provide insights into the extent to which a general ban on personalised advertising meets consumer expectations.[428] Interestingly, despite the low trust of consumers in online advertisement and the weakness of the current designs of cookie banners, a general ban on personalised advertising contradicts empirical findings that a research group gathered in a *qualitative* study about consumer privacy perceptions of personalised content in the internet. According to the findings within this study, consumers basically see added value in the personalisation of content, including of advertising, if this makes the content or advertisement more relevant for them.[429] This result appears to contradict the aforementioned quantitative studies at first glance, according to which the majority of consumers are against the current practice of personalised advertising.[430] At second glance, however, the difference lies in the different study designs. While *quantitative* studies usually allow closed questions (e.g. whether, how much, how strongly), *qualitative* studies answer questions such as "Why?" and "How else?". In such a qualitative study the research group conducted 20 interviews (each of 60-90 minutes) with laypersons and observed that most of these participants opposed the current practice because of the aforementioned lack of transparency, deceptive designs and consent fatigue. However, if these problems could effectively be solved by consent processes that they find actually transparent and effective, the participants would feel put in a position to effectively decide on whether they really agree with personalised advertising or not. In theory, the participants saw the added value promised by the advertising industry that personalised advertising would be more relevant to them. However, based on the current design of consent (and withdrawal) processes, they are just not in a position to verify whether this promise really applies to them and justifies the risks.

To find out whether such more effective information on the benefits and risks is possible, the research group created mockups for a website cookie banner with two functionalities: The first functionality involves allowing consumers to enable or disable profiling for personalised advertising on a simulated basis. With a toggle switch, users could see banner ads automatically switch between personalised and non-personalised versions in the background of the screen. Technically, a major search engine being asked in the research process stated that the main challenge here would be billing rather than technology itself. However, there were two other notable issues. First, if the aim is to show data subjects in real time how profiling affects advertising by comparing personalised and non-personalised ads, a legal challenge arises: such functionality requires a profile to exist before the data subjects actually give their consent. Second, even with consent, building an actual profile takes time, so immediate personalisation isn’t feasible. In the prototyping process, the research team addressed this issue by creating fictional personas that would appear in the cookie banner. Data subjects could

[428] See, for example, https://edaa.eu/your-online-voices-your-voice-your-choice/; and https://extranet.greens-efa.eu/public/media/file/1/7267.

[429] V. Grafenstein, Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, SSRN 2024.

[430] European Interactive Digital Advertising Alliance, Your Online Voices: What consumers told us about their perceptions, needs, hopes, and expectations of data-driven advertising, p. 9; McCann/ Stronge/ Jones, The future of Online Advertising, 2021, pp. 75 et seq.; Forbrukerrådet, Surveillance-based advertising survey, 2021, p. 3.

select one, allowing them to see a simulated version of personalised advertising. This approach provides data subjects a (simulated) glimpse of how personalised advertising might become more relevant for them.

The second functionality addressed the requirement from the Belgian data protection authority with respect to the TCF that a data subject's consent for personalised advertising is only informed if they have access to their profile where this data will flow in (see above chapter 2.2.6.). The challenge here is that the data subject must be able to view their profile in connection with the cookie banner. Legally, this requires linking informed consent with the data subject's right to access. To address this issue, the research team developed mockups for a privacy dashboard. Data subjects could expand this dashboard from the cookie banner as a second layer, allowing them to access detailed information as per Art. 12-14 GDPR and exercise their rights (including the right of access and the right to rectification) from Art. 15-21 GDPR. The dashboard then opened across the full screen of the device of the data subject.

In qualitative interviews, three testers of these mockups stated that, for the first time, they understood how personalised advertising works. Two participants mentioned that they would consider consenting to personalised content, at least temporarily, even though they typically reject it (especially when there's an option to decline immediately). This change in attitude was attributed to their newfound understanding of both the benefits and risks, as well as at least a basic understanding of the underlying processes. However, all three expressed doubts about whether the prototype could be implemented as designed. They cited concerns over technical feasibility and voiced a general, though unspecified, suspicion that the advertising industry might oppose such transparency and user control. Even though the number of testers of these mockups was small, the research team assumed, by drawing on the general state of research in the field of feedback design, that such immediate feedback processes may significantly increase consumers' understanding of the benefits and risks as well as their control.[431]

Future studies will probably focus on further differentiating the binary scheme of 'personalised advertising – non-personalised advertising' used in the studies presented. In our opinion, the studies should take up the purpose scheme that we propose below, which further differentiates the umbrella purpose of personalised advertising on the basis of its risks for data subjects, namely: retargeting, profile-based personalisation, cohort-based personalisation and contextualised advertising (see chapter 5.3). Another focus should be on conducting the study as part of a long-term field test. In this way, the subjects would not be dependent on fictitious personas, but could observe over a longer period of time how the advertising displayed to them actually changes depending on the chosen advertising purpose: The consumers could thus find out for themselves which form of advertising they feel is actually most relevant and is most appropriate in relation to the corresponding risks (see section 4 for more details).

4.2.3 Data use control

The last tile of the aforementioned privacy dashboard contained a description of additional objective protection measures implemented by the website shop operator. These measures included a certification mechanism to which the website operator adhered to demonstrate compliance with the GDPR, according to Art. 41 and 42 GDPR. Such a certificate thus demonstrates that data recipients process the personal data of the consumer solely as outlined in the cookie banner and privacy dashboard

[431] V. Grafenstein, Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, SSRN 2024.

(see mockup of the privacy dashboard tile in Annex 4). According to recital 100 GDPR, such data protection seals shall enable "data subjects to quickly assess the level of data protection of relevant products and services" (see the demonstration function of these mechanisms with respect to data controllers and processors in chapters 2.5.8.3. and 3.1.2.7.).

4.3 PRE-CONDITIONS TO ENSURE SUSTAINABLE EFFECTIVENESS

However, in order to make consent processes significantly more effective, also in the long term, specific legal, technical and organisational measures must be met. The two most important legal requirements result from existing regulation, namely the data protection by design approach in Art. 25 sect. 1 GDPR. However, there are also certain technical and organisational conditions that are essential for the successful implementation of effective consent processes in practice.

4.3.1 Optimisation goal, future and technological openness

In order to keep pace with technological developments in both a negative and positive sense, the data protection by design approach in Art. 25 sect. 1 GDPR contains three elements. In order to also effectively control risks that only arise from new technical developments, Art. 25 GDPR refers to the risks of the most current processing purposes. The provision also clarifies that the data controller must ensure the effective implementation of the legal provisions of the GDPR in the technical and organisational design not only at the time of data collection, but also later at the time of processing. The regulation thus ensures effective protection against the risks of future developments, regardless of the technology that causes them.[432]

However, Art. 25 sect. 1 GDPR ensures that data controllers also keep pace with technological developments in a positive sense. The so-called dynamic reference to the current state of the art fulfils this function. As illustrated previously (see chapter 3.1.2.6.), the state of the art means the scientifically proven *most effective* implementation of a legal provision that is available on the market.[433] Thus, the controller must additionally consider the most effective implementation available on the market, so to speak, as a benchmark. The controller is only not required to implement the most effective implementation available on the market if the implementation costs are disproportionate.[434] This dynamic reference to the market-development can turn out to be a powerful legal mechanism to constantly push the data protection level in practice because as soon as someone has advanced the state of the art, everybody else must take it into account. This mechanism can thus trigger the long-sought competitive advantage of the GDPR and the innovation developments that follow from it.[435] We will illustrate this mechanism again in detail for the present context in chapter 5.5. To do that, it must, of course, be applied more consistently in practice. However,

[432] Simitis/ Hornung/ Spiecker/ *Hansen*, Art. 25 GDPR, para. 33 et seq.

[433] Cf. Martini, Integrierte Regelungsansätze im Immissionsschutzrecht, 2000, pp. 210 et seq.

[434] Ehmann/ Selmayr/ *Baumgartner*, Art. 25 GDPR, para. 22.

[435] v. Grafenstein, Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design, 2019.

this is to be expected, given the methodological clarification that has taken place in recent years.[436]

4.3.2 Empirical proof of effectiveness

The second essential legal requirement for the effective implementation of consent processes is also set out in Art. 25 sect. 1 GDPR. As pointed out previously, Art. 25 sect. 1 GDPR requires the controller to implement the legal requirements in a way that *effectively* protects the data subjects from the risks of the specific processing in question. Thus, the controller must provide for an empirical proof of the effectiveness of its implementation. This provision is the actual innovative turning point that Art. 25 sect. 1 GDPR entails.[437] This requirement is so important in the current context because it ensures that the interests of the industrial providers of these processes are not unilaterally reflected in the design of the consent processes. Rather, the proof of effectiveness ensures that the consent processes always enable consumers to make effective decisions (even most effective decisions, see previous subchapter) with regard to the benefits and risks, regardless of whether this ultimately also benefits the interests of industry or not (see in particular chapter 2.5.1.).

Indeed, proving effectiveness is challenging. To do this, lawyers need to synchronise their objectives, concepts, methods and processes with those of other disciplines. As far as the implementation of legal provisions is concerned, whose effectiveness depends on their usability, such as consent processes and further data subject rights, these are primarily from the fields of user experience design and behavioural science research (see above chapter 2.4.2.).

4.3.3 Technical-organisational measures to make it work

In order to effectively implement these legal provisions, certain technical and organisational measures are required. It has already been shown in chapter 2.4.2. that this implementation requires the coordination of all the actors involved in the processing of consumer data. In particular, the actors must:

- pass on the necessary information about the insights into the consumers' private lives so that consumers get this information right in time and according to their usage context, upwards and downwards along the data value chain, especially since most players do not have a direct end-user interface with them (see in more detail chapter 5.5.3);
- pass on the necessary information so that consumers are able to control, right in time and according to their current usage context, the risks of manipulation, discrimination, material and health harm; here, the focus has to shift from the moment when the data is collected to the moment when the consumer is shown the advert and interacts with it (see in more detail chapter 5.5.3.);

[436] Datenschutz by Design in der (Vollzugs)Praxis – Workshop für Expert*innen, From 28.10.2021 to 28.10.2021, Humboldt Institut für Internet und Gesellschaft, Berlin, Germany. Co-Organised by: Alexander Dix (EAID), Frank Pallas (TU Berlin) (National).

[437] V. Grafenstein/ Jakobi/ Stevens, Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods, Computer Law & Security Review 2022, pp. 2 et seq.

- to have the necessary technical interfaces in place to exchange this information automatically, that is, in machine-readable form; in particular, actors like publishers and browser providers must accept signals from PIMS, which consumers will use to manage their risks more effectively (see in more detail chapter 2.5.1. and 5.5.3.2.);
- and finally make sure, not only through legal obligations, but also through technical-organisational measures, such as through certification mechanisms, that receivers of the data stick to the conditions set out by the consumers in their consent forms (see in more detail chapter 5.5.3.).

For this coordination to actually work in practice, the corresponding legal, technical and organisational specifications must be standardised and bindingly defined between the actors. This is a fundamental condition that the TCF of the IAB Europe has not been able to comply with, given its self-regulatory nature, that is, its one-sided representation of industrial interests and governance mechanisms (see above in chapter 2.2.4.3.).

In this context, an important fact should be emphasised: Since the TCF has already implemented these conditions in its very basic form, 'upscaling' these conditions in a mandatory law (or a delegated act) causes a relatively low regulatory burden for the stakeholders. The only thing that such an upscaling achieves is to slightly tighten the requirements with respect to specific aspects and to clarify their adherence for the respective actors more specifically.

4.4 ADVANTAGES FROM A BUSINESS PERSPECTIVE

In turn, this specification and clarification of the legal, technical and organisational aspects goes hand in hand with decisive benefits for almost the entire online advertising ecosystem. In particular, the small and medium-sized advertising services and advertisers will be able to gain a competitive advantage from these specified and clarified conditions. Only very large companies with market power could face difficulties. This does not apply to smaller companies, however, since their processes are far less complex. These effects are reasonable given the differences in the financial, technical, organisational and human resources of small and medium-sized companies on the one hand and very large companies on the other. Thus, our regulatory proposals help to create a somewhat fairer level playing field.

4.4.1 Increasing the consent rate by lowering the risks

Let's start with the competitive advantages of advertising services. The reason for the potential competitive advantages for advertising services lies in the fact that they may positively influence consent behaviour of consumers by establishing more data protection-friendly processes.

There are already a few empirical studies showing that consumers prefer technologies that protect their data more than those that protect their data less.[438] For example, one study has already shown that consumers are willing to pay a higher price for privacy-friendly technologies.[439] However, this fact is not the focus here. As shown, such pricing models are associated with numerous ethical issues (see chapter 2.5.7.). Rather, the

[438] Gupta et al., Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information, 2023.

[439] Skatoval/ McDonald/ Maple, Unpacking privacy: Valuation of personal data protection, PLos One 2023.

focus here should be drawn to the fact that consumers are enabled to choose between processing methods that cause lower and higher risks to them, and they actually do so.

The above-mentioned empirical quantitative study (which is currently still ongoing) not only showed that certain consent processes do better than other processes at informing consumers about the risks to them. Rather, this information also had an effect on their consent behaviour: With the currently widespread best practice cookie banner, 53% of participants decided to click on the accept-all button, while 27% clicked on the deny all button and 20% on the save button.[440] Interestingly, hardly any of the latter group gave specific consent for the individual purposes, although the save button is intended for this. This points, by the way, to a misunderstanding of the function of the save button.[441] Anyway, in contrast to the current cookie banner design, in the alternative cookie banner design, which pointed out the benefits and risks of the respective purposes on the first visual level, only 42% pressed ‘accept all’, while 32% now clicked the deny all button. However, what is more decisive for the question of whether consent is the appropriate legal instrument at all is that now 26% of participants suddenly made, via the save button, differentiated consent decisions with respect to the different purposes.

This effect was even stronger in the study group that used the alternative cookie banners together with a consent agent. First of all, in this group, 92 % of the participants made use of the automatic time-out, which means that the vast majority had made their choice already when installing the consent agent. These participants had therefore more time and space available to understand the benefits and risks of the four purposes and to make their choice (see the reason for this effect above chapter 4.2.1.). This appears to be the main reason why there are now clear differences in consent behaviour for each individual purpose: While 65% consented to the processing of their data to customise the website, 52.2% did so for statistics to improve the website, 29.2% did so for personalisation of the website and 27.5% did so for personalisation of advertising.

What is most important here is that these figures change again significantly as soon as a data protection seal is displayed or information on the use of particularly data protection-friendly technologies that cause lower risks. In the present case, for example, the visited website stated that it did not engage in price discrimination. In addition, the website stated that it only created limited profiles and shared them only to a limited extent with other partners in its advertising network (confer similar promises with respect to Google’s Topcis above in chapter 2.5.4). The starting point for the testers was the information in their consent agent, according to which they had to expect price discrimination and the creation of extensive profiles and the sharing of these profiles in a relatively large advertising network when consenting to personalised content and advertising. The information provided by the specific website visited by the testers therefore suggests that the risks were lower than originally stated in the consent agent on a typified basis. The data protection seal also had a strong effect on the personalisation of the website, where 36.5% now gave their consent. For the display of particularly privacy-friendly technologies, the consent rates increased significantly for all four purposes, namely up to 76.4% (website customisation), 61.8% (statistics to improve the website), 49.1% (website personalisation) and 40% (personalisation of advertising). With all due caution in view of the ongoing evaluation of the data collected

[440] V. Grafenstein, Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, SSRN 2024, p. 41 (the full paper is currently in preparation).

[441] See Grassl/ Gerber/ v. Grafenstein, How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights?, European Data Protection Law Review 2024, pp. 101 et seq.

in this study, these results allow the justified assumption – not least in view of similar results from the other studies mentioned above – that consumers are more likely to give their consent to the processing of their data the less risk this entails for them or, more precisely, the more favourable they rate the value-risk ratio for them.

Advertising services are therefore in a position to increase the likelihood that consumers will give their consent the less risky they organise their processing processes and the more convincingly they can present the benefits for the consumer. In the case of personalised advertising the latter means, the more relevant consumers perceive the advertising to be. In our estimation, it therefore also seems to be a question of the future development of more and more effective privacy-enhancing technologies to further reduce the risks of personalised advertising and thus potentially push the consent rate higher. Advertising services can thus gain a competitive advantage from this by increasing the pool of potential customers for advertisers, increasing the consent rate of the respective advertising form they provide. This leads us to the next point.

4.4.2 Selection of appropriate advertising form by advertisers

As already summarised in the introduction to this chapter, advertisers can now decide on this basis which online advertising method is most advantageous for their advertising strategy. The size of the pool of end customers that can be reached with the chosen advertising form, which results from the corresponding consent rate, will certainly be an important factor in this decision.

Of course, there are other factors as well.[442] The conversion rate, for example, will also be important. This is the probability that end customers who are addressed by a particular form of advertising will ultimately also buy the advertised product. Other factors include the price that advertising service providers charge advertisers for one or other form of advertising, as well as the options for measuring the success of the respective advertising method. Last but not least, brand safety will also play a role. It is reasonable that certain consumer groups will prefer certain forms of advertising to others and that this will have an impact on reputation, which advertisers can protect, enhance or even reduce by choosing the advertising method (perceived as appropriate or inappropriate by the targeted consumer group).

Of course, all this raises numerous interesting questions, all of which require further empirical (marketing) research. However, the prerequisite is that this level playing field is created in the first place. The aim of the regulatory option we will propose in the next chapter is to open up this level playing field, on which a corresponding competition can arise in the direction of increasingly data protection-friendly solutions and thus potentially higher consent rates – without jeopardising consumer trust and, this is crucial, thereby maintaining brand security.

4.4.3 More efforts for quasi-monopolies

We have already pointed out in various parts that the quasi-monopolistic Big Tech companies will probably be able to expand their positions of power even further in view of the already existing economic and informational power concentrations and the expected technical developments. Contrary to what one might expect, these companies

[442] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, pp. 113 et seq.

currently appear to be even the players most likely to achieve a higher level of data protection than their smaller competitors in the online advertising ecosystem.

There are various reasons for this: first of all, it is financially easy for these companies to provide the necessary resources. Secondly, due to the vertical and horizontal integration of the various phases of the value chain, it is far easier for them to adapt their technical and organisational system accordingly. On their own end-user interface, these companies can obtain consent themselves, collect the personal data themselves, process the data themselves without having to share it with anyone, and finally play the advertising back on their own interfaces. Actually, it is a raison d'être for their progressive power accumulation that they do not sell data but just sell advertising space. Thirdly, these companies are increasingly realising that they can also use data protection compliance to further marginalise their competitors. Again, the less data they share for reasons of data protection, the greater their power.

From a consumer protection perspective, this increasing economic and informational power accumulation is problematic for two reasons: firstly, the concentration of economic power leads to less and less competition and thus to a smaller and smaller range of digital products and services for consumers, which is opposed to the approach taken here of maximising the dynamics of competition and the associated innovation dynamics towards increasingly data protection-friendly processing. And secondly, this development leads to a concentration of information power, which data protection actually aims to prevent.

On the other hand, there are meanwhile numerous efforts, particularly from the EU legislator, to limit, if not push back, this increasing accumulation of power and the resulting risk of power abuse. In particular, the DSA should be mentioned here, which places special demands on very large online platforms and very large search engines. We also discussed the DMA, which, due to the gatekeeper role of most of these companies, places special demands on them with regard to obtaining informed consent. In contrast, with its requirements for PIMS, the DGA is likely to pose only minor obstacles, particularly for the initiatives recently observed by browser providers to now also take over the management of consent in favour of their end users and thereby to their own advantage, which likely means to the disadvantage of their competitors. In short, browser providers would only have to establish a separate legal entity to provide the consent management service within the meaning of Art. 10 lit. b DGA, and this entity would not be allowed to use the data collected for its own purposes (Art. 12 lit. a DGA). This service would then support the actual data-collecting service of Google or Apple in collecting the data from the consumers.

In turn, the DA takes a relatively clear stance by obliging gatekeepers to share their data, but at the same time excluding them from corresponding data access rights.

The approach we are proposing here is likely to have a further effect, even if it is not primarily intended and is certainly not very far-reaching, which will set further controls on the practices of these companies. The reason for this is that our proposed transition of the certification requirement for companies operating in the online advertising ecosystem, which is already provided for in the TCF, to the certification programmes established in Art. 42 et seq. GDPR for very large companies is a much more complex undertaking than for smaller companies. Their horizontal and vertical integration of the various processing phases along the data value chain for personalised advertising may give them a major advantage in the governance of these processes, for example in the internal implementation of data protection regulations. But an external audit of these processes, as required in the context of certification procedures under Art. 42 et seq GDPR, is likely to pose significant problems for these companies. This is because for such an external audit, the processes must now be broken down into their individual processing steps. The more comprehensive and integrated these processing phases are, the more complex their breakdown is likely to be.

This does not apply to smaller companies, since their processes are far less complex. Now it is the other way around: for smaller companies that operate on the basis of the division of labour, it is a relatively complex governance task to coordinate their respective processing steps between them, especially when it comes to complying with data protection regulations. However, since an audit only focuses on their own processing operations, the external audit is correspondingly more manageable. This applies all the more since our regulatory proposal is aimed at clarifying and thus considerably facilitating coordination between companies. An external audit can build on these governance structures, which have been clarified between the smaller companies, and therefore concentrate on the internal processes of the company to be audited in each single case.

Ultimately, the different audit efforts correspond to the differences in the financial, technical, organisational and human resources of small and medium-sized companies on the one hand and very large companies on the other. Our proposals therefore merely help to create a fairer level playing field for very large and smaller advertising companies.

4.5 SOCIETAL PERSPECTIVE: MONITORING OF NEGATIVE THIRD PARTY EFFECTS

There is one last aspect that should not be forgotten here. As shown above, personalised advertising can not only pose individual risks to consumers but also numerous risks to third parties and society as a whole (see chapter 2.3.3.). Some of these risks may indeed be contained by consumers finally being able to make really informed decisions. This may apply in particular to risks to collective goods such as a fair market, a functioning democratic polity, public discourse or even how solidarity is practised in a certain community.

However, these risks cannot be contained by effective consent processes alone. Rather, further objective-structural protective measures are required to be able to measure such structural risks at all. To do that, one has to be able to gather the necessary information, e.g. which advertisement was played to whom and how often, who paid how much and where did the money go. This can be done, for example, through access to information rights for representatives of the public interest (such as journalists, scientists, law enforcement authorities), and more comprehensively through public registers (see in more detail, for example, the chapters 3.3., 3.4. und 3.5.). We will also propose regulatory options for this in the following chapter.

5 STRATEGIES, PROPOSALS AND PERSPECTIVES FOR AN ALTERNATIVE REGULATION

On the basis of the above analysis, we would now like to make our regulatory proposals for how the risks of personalised advertising can be controlled much more effectively than before and how a market can be created for this, in which competition will lead to the development of ever more data protection-friendly technologies. To do this, we are relying in particular on an analysis of the current legal framework. We will start by looking at the shortcomings of the GDPR and then move on to its positive elements, as well as those of more recent legislative initiatives. As already said, the analysis of the current legal framework was highly instructive in order to understand the learning curve of the legislator, in the course of which the legislator addressed the problems described in an increasingly specific manner: These include, in particular, 1) the clarification of legal requirements for specific sectors and actors; and 2) a clear assignment of technical and organisational cooperation obligations to overcome governance problems (and knowledge deficits) in complex processing networks. Our regulatory proposals will focus on these building blocks, although the whole issue will be preceded by a discussion of a general ban on personalised advertising for dramaturgical reasons.

5.1 STARTING POINT: ADDRESSING THE DEFICITS OF THE GDPR IN ITS PRACTICAL IMPLEMENTATION

The above analysis has shown that the GDPR would actually provide a comprehensive law that would theoretically be able to address the above-described risks of personalised advertising: In essence,

1) the GDPR is applicable to all phases of the personalisation of advertising that involve the processing of personal data[443]*,*

2) the GDPR not only protects individual fundamental rights, but also, at least according to the conceptual understanding, societal assets and positions, and

3) the GDPR provides a combinable set of objective rules for data processing and individually enforceable rights.

4) In addition, the GDPR requires data controllers and, to some extent, processors to implement these requirements into the technical and organisational design of the data processing so that they protect the data subjects, effectively.

5) Finally, the GDPR even provides co-regulation instruments, such as certification procedures and codes of conduct, which may be used to significantly reduce the ambiguity of the numerous legal principles and indeterminate legal terms and the associated legal uncertainty, as well as the enforcement deficit on the part of the authorities.

[443] However, the crucial point of collecting data by accessing user's terminal equipment is governed by ePrivacy, see chapter 3.2.

However, it became apparent that existing legislative mechanisms are not capable of countering the individual and social risks inherent in the digital advertising market. The identified gaps are also not satisfactorily covered by the legislative approaches applicable besides the GDPR, since they only cover specific sections or actors of personalised advertising and therefore only partially address the risks posed by personalised advertising in its current form (see chapter 3.2. – 3.6.).

The most effective and long term solution ensuring the users fundamental rights, of course, is to ban certain purposes and methods in respect of specific data flows, categories of data or players within the ecosystem (see chapter 5.2.). Even though such an ultimate proposal has strong advantages, it's not sufficient to only envisage one strategy in order to be able to react to the dynamics of the market and permanent changes regarding players and processes. Ultimately, the complexity of the online advertising market can only be addressed if substantive, procedural, technical and organisational measures are introduced at the same time at several levels that are aligned with each other.

Several deficits in the current regulation stem from the fact that basically just a rough distinction is made between: does personal data processing take place, yes or no. Since it is beyond dispute, though, that personal data is processed in the course of a personalised ads lifecycle, it is of much more significance to further differentiate at another level, namely the specific purposes and methods. Because the pertinent risks requiring regulation and the severity of an infringement of fundamental rights mainly arise from these factors. However, this is not yet reflected (enough) within the law.

Since the current law lacks definition and specification of purposes and methods regarding personalised advertising, including chains of data flows and participants associated with such purposes, there are legal uncertainties on the one hand and room for exploitation on the other. To this end we have come to the conclusion that there is a need to close this gap by specifying purposes on a legal level and further conditions on a technical and organisational level (see chapter 5.3). Only when clarity has been established here the appropriate legal basis as well as accompanying measures can be determined, depending on the risk potential of each purpose (see chapter 5.4.). If consent proves to be the most suitable legal basis – at least for some purposes – it is essential to specify the requirements for this at a legal level. Beyond that it is necessary to underpin the process of obtaining consent with actor-specific obligations.

At the same time experiences from other areas of law show that privileges create incentives, for example to choose less risky options or to act compliant. In the present context this might be a strategy to help actors within the ecosystem to decide for less invasive, less data driven purposes and methods.

Finally, a crucial building block will be to bring transparency into the system and to become master of the chaos. Ultimately there is only one solution: introducing cross-actor obligations in form a registration mechanism (chapter 5.5.)

In view of this, we propose the following measures, taking into account regulatory approaches from existing laws that have the potential to serve as a template for new proposals.

5.2 BANS ON PERSONALISED ADVERTISING

In view of the risks and enforcement deficits discussed as well as the conceptual and practical limits of consent (see chapter 2.3.), it seems plausible to abandon the regulatory focus on consent and replace it with a ban on personalised advertising altogether. This is all the more justified if the risks for data subjects clearly outweighs the interests in data processing and the concept of consent won't remedy the imbalance due to several market failures.

The advantages of a ban are obvious, even if it is only applied to certain parts of the advertising ecosystem. Regarding the consumers, a per se ban creates the most effective level of protection against the risks arising from personalised advertising. In addition, such strong regulatory intervention promotes an economic level playing field for those at the outer edge of the network, namely publishers and advertisers. At present, they are completely dependent on the ecosystem with no viable alternative. As far as such a ban would go, it would eliminate the need for coordination. If the data is not allowed to be processed in the first place, there is no need to set up technical and organisational protection measures to contain the risks. Against this background, a ban is not only the most legally effective protection, but also the most economically effective.

Since traditional ex-post control of (il)legal behaviour includes lengthy proceedings, problems of providing evidence and ineffective remedies, it is slow and ineffective.[444] With an ex-ante prohibition approach in turn, authorities would be relieved of the procedural burden of assessing legal bases in individual cases. Depending on the specific scope of a ban, it hence leads to facilitating and accelerating law enforcement.

The advantage of a ban strategy also means that no more detailed regulations need to be created regarding the prohibited practices – meaning such regulations that further complicate the already existing landscape of laws and that needs to be evaluated with view to their efficiency and effectiveness for years.

Nevertheless, a general ban on personalised advertising might be offset by obvious disadvantages. On the one hand, the efficient nature of this approach is contrasted with possible economic losses incurred by market participants, due to less effective advertising methods and lower consumption. Of course, this factor is not the focus of a consumer protection perspective. Still, it would have to be taken into account when weighing up all the rights affected by a ban.

On the other hand, a general ban might also negate the heterogeneous privacy attitudes of consumers and the fact that they theoretically see added value in the personalisation of advertising, provided that this would really make the advertising more relevant to them (for studies on consumer perceptions see chapter 4.2. and 4.3.). That is why we are discussing a general ban more as a fallback regulation should it turn out that the risks cannot be effectively contained due to the excessive coordination efforts, despite our regulatory proposals to reduce these efforts.

When assessing at which level and to what extent prohibitions are to be imposed, the rights and entrepreneurial freedoms of the companies whose activities would be restricted must always be taken into account. Prohibitions must therefore be considered in a differentiated way, depending on how suitable they are for limiting which risks. A general ban on data processing practices for personalised advertising is therefore likely if it turns out that the chaotic processing conditions in the online advertising sector and the risks posed by these practices cannot be satisfactorily resolved, despite 'softer' legal initiatives such as the GDPR, and not even over a longer period of time.

[444] Kerber/ Specht-Riemenschneider, Synergies between data protection law and competition law, 2021, p. 56.

Therefore, we also consider more specific focal points for ban scenarios, from a user-related approach to process-related or actor-specific bans. Among them, a ban on the processing of personal data of vulnerable groups for personalised advertising stands out, as it is the ban scenario that probably receives the highest level of approval, even among business representatives.

5.2.1 User-related: Ban regarding specific types of data and data subjects (esp. vulnerable groups)

Initially, a user-related approach can be taken into account by prohibiting the processing of certain types of data or certain groups of data subjects. This can achieve protection specifically for vulnerable groups.

This strategy is partly already in use in Art. 18 sect. 1 PTR – limited to political advertising – and in Art. 26 sect. 3 DSA – limited to online platform providers. In both regulations the use of "targeting techniques or ad-delivery techniques" respectively the presentation of advertising is restricted in case it is based on profiling according to Art. 4 no. 4 GDPR using special categories of personal data according to Art. 9 sect. 1 GDPR. This means a group of conclusively enumerated data, that usually has a particularly high potential for causing harm, is excluded from a specific type of automated evaluation.

This approach has two weak-spots. On the one hand, as discussed in chapter 3.4.2., the term profiling is defined so broadly in the GDPR, that linking to it leaves the regulation blurry. The same vagueness also arises with regard to Art. 9 GDPR, after the ECJ has applied a very broad understanding of – at least – health data in its latest rulings.[445]. Such leeway for interpretation, leads to uncertainties regarding the scope of the prohibition. In order to implement a user-related approach in a meaningful way, it is therefore not enough to make a superficial reference to profiling and sensitive data within the meaning of the GDPR. Rather, it would be necessary, at the very least, to specify the definition of profiling in relation to the advertising market (see below 5.3.).

On the other hand, in the digital society all users experience vulnerability detached from age or processing of sensitive data. Even digital-savvy people face online contexts in which they are situationally vulnerable (see chapter 2.3.1.3.).[446] The fact that the restriction to sensitive data in the meaning of Art. 9 GDPR is unlikely to achieve the desired result is evident not least from the document that a team of journalists had come across in 2023 (see chapter 2.2.3.).[447] The file contains more than 650,000 different categories into which users are categorised in order to target them more effectively with advertising. Instead of focussing on the few and relatively rough categories of data according to Art. 9 GDPR, we propose to regulate the processing of demographic data that is used on a larger scale during the lifecycle of a personalised ad, including age, income, gender and family status. This may sound trivial, but is necessary with regard to corresponding risks. A look beyond the data protection sector has shown that substances that carry risks may need to be regulated in great detail. For example, the REACH Regulation contains Annexes in which substance prohibitions

[445] The ECJ considers purely hypothetical conclusions about illnesses as sufficient to classify order data at a pharmacy as sensitive, regardless of whether the controller wants to draw health-specific conclusions from it, ECJ, 4.10.2024, C-21/23, para. 74 et seq. - Lindenapotheke.

[446] Kroschwald, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 5; Strycharz/ Duivenvoorde, The exploitation of vulnerability through personalised marketing communication: are consumers protected?, IPR 4/2021, p. 6.

[447] Dachwitz, Microsofts Datenmarktplatz Xandr: Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert, Netzpolitik, 8.6.2023.

and restrictions are listed on hundreds of pages, including 52 substances or substance groups (see chapter 3.3.5.).

We see this as the most suitable approach to meet the need for protection of particularly vulnerable groups. Nevertheless, it is clear that the existing approaches in the PTR and DSA show weaknesses. For a ban that pursues a user-related approach, these weaknesses should be counteracted by not referring to general provisions of the GDPR, such as Art. 9 GDPR, but to the actual circumstances within the advertising system in detail.

5.2.2 Process-related: Ban regarding specific purposes and types of processing methods

Likewise, specific purposes or types of processing methods should be subject of a prohibition – depending on how severe the related data processing is and how likely and how extensive the realisation of personal or societal risks is.

This strategy is already used to some extent in Art. 5 sect. 2 DMA, but only applies to the use, combination or cross-use of personal data by a handful of gatekeepers without specific consent. This approach should be extended to apply not only to gatekeepers but also to other players in the system. Therefore, it is necessary to adapt the restriction, since it leaves loopholes in its current form, first for the gatekeepers own use of that data, and second because consent is not excluded as a legal basis (see chapter 3.6.2.).

Also the AI Act uses this approach in Art. 5 AI Act, which contains three real ban scenarios on certain (AI) practices. This includes, inter alia, the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm (Art. 5 sect. 1 lit. a AI Act). All three cases are dependent on the question of what “significant harm” or “detrimental or unfavourable treatment” means. However, the examples show that the EU legislator is not squeamish about banning certain practices if it perceives these practices as definitively incompatible with “European values” (see chapter 3.3.2.).

The exact connecting factor of a ban needs to be considered carefully. It may tie in at different levels and in different sections of the life cycle of personalised advertising (see chapter 2.2.2.), depending on how comprehensively it shall take effect. Starting with the collection of data at the very beginning of the process chain, **cross-site tracking** should in general be restricted. Such a ban is suitable to ensure that only as much data is collected as is of interest for first-party advertising and no exhaustive profiles of users can be created. This approach would need to be completed by prohibiting the subsequent **combination with additional data**, e.g. from offline sources, or **enriching** the data with those from DMPs databases, since the synchronisation methods within the advertising system have reached such a level of efficiency that the collection of data in separate silos does not rule out the possibility that it will not be combined later (see chapter 2.2.3.). If the goal is to not only eliminate third-party trackers, but to make it impossible for any single company or a group of companies to collect and combine insights about users, the definition of cross-site tracking needs to be defined in a way that leads to outlawing all forms of combining users’ activity from different websites, apps, services or devices for advertising purposes, regardless of what technology is used.[448] These two steps – no cross-site data collection and no subsequent combination – that are closely interlinked, would have an effect on everyone and every step within the advertising network and is therefore a strong intervention.

Such a proposal could be limited to specific steps within the lifecycle of a personalised ad. One option could be to regulate with a blacklist or whitelist, what data is (not) allowed to be included in a bid request (see chapter 2.2.2.).

Art. 18 PTR pursues a small part of this approach by determining that the controller is only allowed to process data collected directly from the data subject. The regulation thus appears to significantly restrict the pool of legally available data in context of online political targeting.

Instead, a focus should be placed on another aspect, namely to derive information from collected data. Such **inferred data** carries a particular risk in that, on the one hand, it is susceptible to incorrect conclusions and, on the other hand, the conclusion can lead to sensitive data that promotes vulnerability. As an example: the information that a specific webshop was visited eight times within a week is not in itself very risky. In case baby clothes were viewed in the webshop conclusions might be drawn such as the visitor is pregnant or the visitor addicted to shopping – or both. The processing of these inferred attributes significantly increases the potential for manipulation, discrimination or other risks. Against this background, the sub-process of deriving attributes from collected data should be subject to a restriction. This would have an effect at the audience segmentation level.

Beyond that, it is conceivable to ban processing for **specific purposes**. A ban might be linked to (some of) the purpose categories that we differentiate in the following chapter 5.3.

5.2.3 Actor-related: Ban regarding specific positions in the ecosystem

Furthermore, a ban could target specific actors within the ecosystem, like gatekeepers or intermediaries, or both. With Art. 5 DMA the European legislator already pursues the concept of a (partial) actor-related prohibition. However, the DMA only targets “core platform services”, meaning specific actors within the digital market as a whole, not the sub-sector of online advertising.[449] Also Art. 5 sect. 3 DA includes the approach to exclude gatekeepers from specific processes (in this regard: from the potential group of data recipients).

In comparison a legislative initiative in the USA pursued an approach in March 2023 according to which large companies shall be prohibited from controlling more than “one part of the digital ad ecosystem”.[450] As a result, they would not be able to act as both an SSP and a DSP provider at the same time. In addition, providers and buyers of advertising space (meaning publisher and advertiser) would only be allowed to offer one DSP or SSP for the sale of their own inventory.

[448] Iwańska, To track or not to track?, 2020, p. 41.

[449] Bundeskartellamt, Sektoruntersuchung Online-Werbung - Diskussionsbericht, August 2022, recital 394 et seq.

[450] Advertising Middlemen Endangering Rigorous Internet Competition Accountability (AMERICA) Act, proposed by Senator Mike Lee in the 118th Congress on 30.3.2023, https://www.lee.senate.gov/services/files/6D030FD4-D961-466B-A1F1-D00B279A24A1.

In addition to the size of the company or the specific business model, another point of reference is conceivable, namely the relevance of a player to the existence of the market itself. So far, the focus has been on publishers or players within the advertising network. Advertisers operating on the edge of the ecosystem are said to have apparently little influence on the market's behaviour, since they are neither directly in contact with users nor their data. At the same time, without them there would be no market – advertisers are the player keeping the system alive by being the ones who feed money into the system and get the money flowing in the first place. If you want to grab the system by the scruff of the neck, it is necessary to go where the money flows. Therefore, taking into account the role and influence of advertisers for the whole ecosystem should be given more attention to when considering which players may be prohibited from participating in the market (in terms of certain actions).

5.3 DEFINING SUB-PURPOSES OF PERSONALISED ADVERTISING ACCORDING TO THEIR RISKS

The above analysis has shown that the GDPR only provides a very basic level of regulation when it comes to purposes and methods. In the past this led to quite different approaches by the industry to categorise purposes in the area of personalised advertising (see chapter 3.1.2.1.). In principle, controllers must specify the purposes in such a way that the purposes serve as suitable starting point for the legal requirements and the data subjects are able to assess whether they find them appropriate or objectionable and therefore prepare themselves for the processing of their data accordingly. To this end, controllers must specify and differentiate the purposes in such a way that they identify the different risks that the corresponding processing operations cause for the data subjects and, eventually, the society as a whole.

Against this background, it becomes apparent that in a diverse and complex system such as the current advertising market, it is necessary to establish clearer purpose-categories by law (not only at the level of supervisory guidance). This was recognized, among other things, in conjunction with the PTR, DSA and DMA, where specific processing operations are clearly designated, to which prohibitions and obligations are linked. We do not consider it expedient or necessary to make such a strong differentiation as is provided for in the TCF, for example, where a total of 19 purposes are differentiated (see chapter 2.2.4.2.). In contrast, the specification of purposes that we propose ultimately follows the principle that, in view of the typically underlying technical and organisational procedures, these must make the various risks explicit and must, insofar, be capable of being distinguished from the other purposes.

For this goal, we propose to basically differentiate between the following sub-purposes in the area of personalised advertising. In the course of this report, we will limit ourselves to the definition of purposes that serve personalisation in the narrower sense. This means that "annex purposes", such as ensuring IT security or the dimensioning of advertising space, are not included here. The following proposed purposes may, of course, be combined with each other, which is what usually happens in practice. The combination of purposes must then be pointed out accordingly.

5.3.1 Re-targeting to complete online shopping processes

We consider re-targeting to be the most intrusive way of personalising advertising. Re-targeting is about re-identifying a consumer across browsers and devices based on a specific event. For example, if a consumer has clicked on an advertisement or even filled a shopping basket without clicking on the purchase button, retargeting aims to persuade this consumer to complete the purchase process over a certain period of time, regardless of where they are on the internet. Based on retargeting, the consumer is therefore shown adverts for products or services related to the triggering event over a long period of time and on various websites and digital services that may be connected with the retargeting system.[451]

With regard to the resulting risks for the fundamental rights of data subjects, retargeting is therefore characterised less by the depth of behaviour-based interest profiles than by the extent of the re-identification possibilities. The advertising industry makes this re-identification technically and organisationally possible by collecting as many identifiers of a consumer as possible and linking them together. A distinction can be made between deterministic or persistent identifiers and probabilistic identifiers. Deterministic identifiers are favoured over probabilistic identifiers for the purposes of re-identification, as they are associated with a higher degree of accuracy. Deterministic identifiers include, in particular, log-in data, email addresses, telephone numbers, postal addresses, payment data, device and network identification numbers (especially IMEI and MAC numbers), cookies that are stored in the browsers of individual end devices, and of course IP-addresses.

Probabilistic methods, on the other hand, rely on identifiers that are not considered deterministic due to their lower accuracy, but still have a sufficient re-identification probability from the advertising industry's point of view. This includes fingerprinting in particular, which uses a combination of various non-deterministic characteristics such as the language set, the time zone, the browser, the browser version, or the screen size of the device used by the consumer, and much more.

In view of the risks to their right to privacy, consumers often find re-targeting intrusive and even creepy because, although they may make a vague connection between the advertising displayed and their previous clicking or purchasing behaviour, they do not understand how this works technically. This sometimes gives consumers the feeling of being secretly tracked.

In terms of added value, consumers do not always disclose the advertising industry's view that re-targeting delivers what it promises. A well-known example is adverts for services or products that are displayed to consumers for weeks on end, even though they have long since bought them and are therefore no longer interested in the corresponding adverts. Of course, this is because the technical systems in these cases may not be able to distinguish whether the consumer has already bought the product or not. However, what counts here is not what is technically feasible, but whether consumers think that the added value of retargeting is worth the risks for them.

5.3.2 Profiling-based personalisation of online advertising

Similar but intrusive in a different way is the personalisation of advertising based on interest profiles, which are created by observing a consumer's behaviour over a longer period of time. The ad industry creates these profiles by observing which websites consumers visit, which content they click on, how long they use them, what they ultimately buy, which other people they interact with, etc. This information can then be used to draw conclusions about the consumer's interests, attitudes, characteristics and, of course, possible future behaviour. How much insight this information provides into a

[451] Wang/ Zhang/ Yuan, Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, FTIR 2017, p. 11.

consumer's private life depends, as mentioned above, on the following aspects in particular:

1) How long the observation takes place;

2) how comprehensive this observation is, i.e. on how many occasions the data subjects are observed,

3) how comprehensive and in-depth the analysis of this information is and

4) the extent to which the information collected and/or derived interferes with the social, private and intimate sphere of the data subjects.

Profile-based personalisation of advertising is therefore not primarily about persuading a consumer to complete the purchase process on the basis of a specific purchase interest shown. Instead, it is about finding out a consumer's wishes, needs and weaknesses and offering them appropriate services and products that satisfy these wishes or needs. As the consumer may not even be aware of their wants and needs, the suggestions may be surprising or inspiring, but also very manipulative.

In this context, it should be emphasised once again that the practices of re-targeting and profile-based personalisation of advertising may well be combined in practice. The same is the case with the cohort-based advertising described below. This type of advertising is also often combined with both re-targeting and profile-based advertising.

5.3.3 Cohort-based personalisation of online advertising

Although cohort-based advertising is similar to profile-based advertising, it is less intrusive. As described above (chapter 2.5.3.), cohort-based advertising separates the phases of data collection and analysis on the one hand and the attribution of the inferred buying interests to specific consumers on the other, affecting two basically different groups of data subjects. With respect to the first group, the risk of someone else gaining access to the observation data may actually be fairly low if the processing procedures are designed properly. However, it is clear that cohort-based advertising still poses a risk to the fundamental rights of the other consumer group, i.e. the consumers to whom the statistical interest profiles are attributed. Therefore, depending on how extensive this attribution is, there is a risk to privacy for this second group. In addition to the right to privacy, cohort-based advertising also poses a risk to the autonomous purchasing decisions of this second group. In this regard, cohort-based advertising is no different from the two other forms, re-targeting and profile-based advertising. The differences therefore lie more in the question of how and to what extent the three forms of advertising intrude into the private lives of the data subjects.

5.3.4 Performance measurement as a sub-purpose

In view of the purpose of measuring success of personalised advertising, this purpose might be considered not as a separate one, but as an ancillary purpose to one or more of the aforementioned purposes. The reason for this is not only that the aforementioned forms of advertising economically require a measurement of success, but that this requires basically the same processing of personal data. Indeed, depending on the key parameter for the measurement of success, the procedures differ in their intrusiveness.[452] For example, reach measurement, i.e. the number of websites on which the advertising appears, can be measured completely independently of the individual visitors to the websites. The same applies in principle to the measurement of impressions. Indeed, an impression does require the observation of how many users are on the website while the advertising is displayed; and this is usually done by processing the IP addresses of the website visitors. However, it does not matter whether the individual persons have seen the advertising or not. The number of IP addresses on all websites on which the advertising is displayed can therefore be aggregated without the need to observe the behaviour of individual users any further. The insights into the private lives of the individual users and other risks are therefore fairly low. Of course, the situation is different when it comes to measuring the conversion rate. To do this, you need to be able to observe the behaviour of individual users more closely, namely how many people click on an advertisement and then perform a relevant action on the target website (usually by pressing the buy button).

When measuring the conversion rate, the question hence arises as to whether, in view of the risks involved, it really is, as initially assumed, only an ancillary risk to the risks posed by the actual form of advertising. Or whether measuring the conversion rate gives rise to risks of its own, so that this additional risk must be identified through a separate purpose (see chapter 3.1.2.1.). On closer inspection, the insights into the private lives of users during conversion rate measurement are only the lesser of two evils. This undoubtedly applies to retargeting and profile-based personalised advertising (even compared to Google's Topics API, observing the user in two actions across two individual websites, namely the click on the advertising on the first website and the click on the buy button on the second website, represents significantly less interference than attributing interests when visiting numerous websites over an entire week). Even in cohort-based advertising, the attribution of at least one purchase interest to a person still appears to be equivalent to observing whether that person then clicks on the advertising and on the target website on the purchase button.

In view of this risk analysis, we therefore suggest that the measurement of success, even in the case of measuring the conversion rate, should only be treated as a secondary purpose of one or more of the aforementioned advertising purposes. In the absence of any risks for the data subject that need to be emphasised separately, this has the advantage that she or he is not further overwhelmed, in addition to the already numerous information needed from a consumer protection and data protection perspective.

However, even if the measurement of success is seen as a sub-category of the actual advertising purpose, the way in which this purpose is achieved in a privacy-preserving manner still plays a role. The Mozilla PPA technology for the Firefox browser, as described above, is a good example of how these risks can be significantly reduced even with such kind of processing (see chapter 2.5.5.). This leads us to the next point.

5.3.5 Contextual online advertising

The least intrusive method to personalise ads is (the traditional understanding of) contextual advertising. It's supposed to be a practice of placing ads on pages based on a match to their respective contents, achieved by a relatively straightforward keyword or URL analysis. Therefore it is often rated as a solution to escape several problems

[452] See the different key parameters at https://www.netzdenke.de/blog/online-marketing/erfolgsmessung-im-online-marketing-diese-kennzahlen-solltest-du-kennen/.

and risks posed by personalised advertising, not only for users but also advertisers and publishers.

Contextual targeting is indeed a promising alternative that is worth taking a closer look at from a regulatory perspective. Nevertheless, it is no sure-fire success since the understanding of “contextual” has been highly blurred by the industry. The term is inflationary used for methods that in fact include the processing of personal data, geo or session data (see chapter 2.5.6.).

To consider this method for regulatory approaches, it is vital though, to formulate a comprehensive and up-to-date definition of contextual advertising that takes into consideration the technical developments regarding the use of AI.[453] When we refer to contextual advertising below and suggest regulations and legal consequences for it, we are referring to an extremely narrow understanding of the term. We are therefore only evaluating methods that do not involve the processing of personal data (unless exceptions are explicitly stated).

Admittedly, specifying a narrow definition provides a practical disadvantage: Because no data about users is collected it can pose challenges in terms of frequency capping (i.e. avoiding showing the same user the same ad multiple times). Likewise some content may be difficult to contextualise.[454]

It is furthermore worth mentioning that even “zero data” methods are not automatically and absolutely risk-free for users. By using AI driven tools that enable very finely tuned context schemes, new methods like neuroprogrammatic advertising have evolved that is aimed at an emotional level (see chapter 2.5.6.). Nevertheless, if contextual data is used as a proxy for (sometimes sensitive) personal data, people are still profiled and monitored, not based on what they do, but the content they view.[455] Thus, the method also has the potential to manipulate or discriminate against users. However, such remaining risks cannot be regulated by data protection, if personal data in fact is left out.

5.3.6 Role of privacy-protecting technologies

The explanations on the various forms of personalised advertising have already shown that even within these defined categories, there may still be gradations as to how comprehensive and in-depth the insights into the private life of the consumers are. The same applies to the risk of manipulation, which is basically the same for all forms. Here, too, it comes down to how well consumers are informed about the respective type of advertising and how easily they may intervene to effectively protect themselves against the manipulation risk. Privacy-preserving technologies play a central role in this.

As outlined above, these privacy preserving technologies are not only important from the consumers’ point of view. They are also important from the perspective of the advertising industry, as their implementation may have a significant influence on how much consumers trust the respective form of advertising. This not only has an impact on consumer trust in the brands of publishers, advertisers and advertising services, but also has a very specific effect on the consent rate.

[453] Kopp, Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy Press 26.9.2023.

[454] Iwańska, To Track or not to track, p. 33.

[455] AWO Belgium, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, 2023, p. 141.

5.4 LEGAL BASIS AND SUPPORTIVE MEASURES FOR EACH SUB-PURPOSE

For the sub-purposes of personalised advertising described above, we propose to clarify the legal basis that is appropriate in each case. More specifically, we clarify the conditions under which the individual sub-purposes may or must be based on one legal basis or another. In doing so, we clarify the central function of Art. 25 sect. 1 GDPR and which elements, parameters and procedures are important to effectively (!) inform the data subjects about the risks of the data processing and, thus, enable them to effectively (!) control the corresponding risks. Since consent agents and privacy dashboards play a central role in this, we clarify the necessary conditions for effectively implementing these mechanisms, last but not least.

5.4.1 Prerequisite: Harmonisation of the ePrivacy Directive

All of the following proposals are based on the assumption that the ePrivacy Directive will initially be harmonised and adapted in order to ensure consistency with the GDPR (see chapter 3.2.4.). Otherwise, any new regulatory approach is likely to fail due to the fact that Art. 5 sect. 3 ePD sets high regulatory hurdles directly at the origin of data collection. Without the strict requirements of the ePrivacy Directive being met, it is currently not possible to access that data whose processing shall be regulated by new approaches. In consequence this means, if other legal bases than consent shall be taken into account regarding data processing within the advertising ecosystem, the ePrivacy Directive generally still demands consent for the upstream data collection.

When amending and harmonising the ePrivacy Directive in this regard, it is therefore necessary to link its requirements to those of the GDPR and further related laws. Ideally, this should be done by focussing less on technical methods and more on purposes (of subsequent data processing).

5.4.2 Specification of consent requirements

If and to the extent that the specific purposes and methods differentiated in chapter 5.3. are not prohibited per se, it should be clarified which ones are only permissible on the basis of consent. Accordingly, it should be clarified by the legislator, that no other legal basis is to be considered for these specific purposes or only under certain conditions.

Since the data processing operations of re-targeting and profile-based personalised advertising reveal (the most) extensive insights into the private lives of the data subjects, the appropriate legal basis at least for these two sub-purposes should be consent, meaning that data subjects must (be able to) consent to these procedures by clearly opting in. For the other purposes and methods, considering another legal basis should not be ruled out, in case that this could create incentives that promote risk minimization (see below chapter 5.4.3.).

However, it became clear from the entire report that such consent cannot mean consent as currently regulated in Art. 6 sect. 1 lit. a GDPR. Rather, more specific consent requirements must be adapted at various levels so that it really becomes an instrument that can counter the current conceptual and practical limitations. Therefore, additional objective requirements are necessary to ensure that the data recipient does not abuse the lack of control on the part of the consumer.

First of all, specifications are essential at the level of the requirements for valid consent. At various points in this report, it has not only been shown that the criterion of “informed consent” is interpreted far too flexible in practice. This likewise applies to the criterion of “freely given and unambiguous indication of the data subject's wishes”. Even though the data protection authorities have already given quite a lot guidance on this matter,[456] it is still the order of the day that cookie banners are designed in a way that manipulates users and makes it more difficult to refuse consent. The legislator has already recognized the problem with the definition of consent in Art. 4 no. 11 GDPR being so general that controllers use this circumstance for exploitation. The DMA correspondingly includes a clarification saying “Not giving consent should not be more difficult than giving consent. When the gatekeeper requests consent, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner. [...] Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent.” (see chapter 3.6.2.).

The problem of deceptive design has also been taken into account in other jurisdictions. Art. 14 lit. h of the California Privacy Rights Act stipulates, for example, that “Consent means any freely given, specific, informed and unambiguous indication of the consumer’s wishes by which he or she, [...] signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. [...]. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent. [...] ‘Dark pattern’ means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision□making, or choice, as further defined by regulation”.

Such clarification on consent requirements need to be made on a legal level, ideally by mandatory law or - for more flexibility - by means of delegated act. In contrast it is no promising option to leave it only to the authorities to give guidance, especially as this guidance is not binding for controllers.

Regarding the requirements for informed consent, Art. 25 GDPR already has the necessary tools ready, that just need to be implemented effectively (see chapter 5.5.3. for more details).

Irrespective of the level of material requirements for valid consent, another mechanism is crucial to finally get a grip on the opaqueness of the system. Therefore new requirements on a procedural level are inevitable. This may include, for example,

- a mandatory certification mechanism for all actors that want to participate in the chain of processing operations in general (see below chapter 5.5.2.)
- a notification obligation with a designated institution regarding specific information on the processing operations that shall be based on consent, including types of data and identifiers used for the processing purposes, the scope of profiling and the number of data subjects (see below chapter 5.5.2.).

5.4.3 Privileges for risk minimization to incentivize

For cohort-based personalised advertising, in contrast, one might consider a legal privilege over the aforementioned more intrusive types of personalised advertising. Such a privilege could have an incentive effect on the market in favour of less risky cohort-based advertising. The strongest incentive effect for the market would certainly come from a privilege in the form of an opt-out process. To reach this aim, cohort-based advertising could therefore be based on the legitimate interests of the data

[456] See footnote 140.

controller and third parties (especially advertisers), according to Art. 6 sect. 1 lit. f GDPR, but combined with a clearly visible and easily exercisable opt-out option. Such a privilege would, of course, require that the procedures do not exceed certain thresholds in terms of the type and scope of the observed characteristics and attributed interests.

In order to reduce the potential of exploiting such legal privilege and to ensure that it is used in a traceable and orderly fashion, the privilege should be subject to a certification procedure too (see in detail chapter 5.5.). The incentive effect for the data controller to submit to such an objective control mechanism is the fact of being able to base the certified data processing on an opt-out mechanism, instead of on an opt-in mechanism.

Last but not least, no legal basis would be required at all for pure contextual advertising in case the legislator determines a comprehensive and up-to-date definition (see chapter 5.3.5.) and the processes meet these determined criteria, inter alia no personal data is processed at all. Of course, to create a corresponding incentivising effect, the data controllers need legal certainty, which means specific criteria that clarify what contextual advertising is and is not. However, to keep pace with the speed of technological development, which is also to be expected in this area, a corresponding legislative proposal should limit itself to the main criteria and procedures. Further details should then be regularly updated by means of a delegated act. This recommendation is based on the assumption that such delegated acts may be issued more quickly than procedurally complex laws. Even faster could be the alternative or complementary option for data controllers to notify their data processing operations with the delegated institution, especially in the event that legislative or delegated clarifications do not yet exist, so that the competent institution may confirm the absence of personal data by means of a so-called negative demarcation. This brings us to a crucial point for the success of an alternative or complementary regulatory approach to the personalisation of advertising.

5.5 CLARIFYING ROLES AND RESPONSIBILITIES: COORDINATION AND ACCOUNTABILITY

In the previous chapters, we have suggested how the sub-purposes of personalised advertising should be specified so that they correctly reflect the different risks to the fundamental rights of data subjects. On this basis, we also made suggestions regarding the legal basis for these sub-purposes and explained why fulfilling the material elements of the legal bases alone is not sufficient. Rather a European Advertising Industry Registry accompanied by a certification and notification mechanism is inevitable to face the complexity of the advertising system and ensure the functionality of the material legal requirements.

In this chapter, we will now specify which actor must fulfil which concrete functions and how the various actors must cooperate in order to ensure effective protection against the risks of personalised advertising across all its processing phases. In doing so, we distinguish between obligations that are specific to individual actors and obligations that all actors must equally meet.

5.5.1 Definition and clarification of legal roles: Processors and (joint) controllers

As demonstrated in chapter 3.1, the GDPR rather generally defines legal roles and (cooperation) obligations of the actors processing personal data. Against this background, it gets clear that the same ambivalences arise with regard to the question of how the various actors in the advertising industry need to coordinate their activities in order to provide effective protection for consumers. This lack of specification has led to disputes in the past that had to be clarified by the ECJ (see chapter 2.2.6.).

In contrast to this, the AI Act defines quite precisely which actor has which obligations (see chapter 3.3.3.). Also the PTR, DSA and DMA set requirements for specifically designated players. As a prerequisite for implementing any new obligations on the actors within the advertising ecosystem (see chapter 2.2.2 und 2.2.4.), it is inevitable to demarcate and define their roles on a legal level in more precision. The aforementioned approaches in the existing laws that cover specific sections or actors of personalised advertising may partly serve as a model for details.

5.5.2 Cross-actor obligations: European registry and certification and notification mechanism

Derived from the instruments already practised in the PTR (see chapter 3.4.), but also in the AI Act (see chapter 3.3.) as well as the REACH Regulation (chapter 3.3.5.), we propose to establish a **European Advertising Industry Registry accompanied by a certification and notification mechanism**. In particular, the certification mechanism can ensure that the actors involved have actually taken all the necessary protective measures in an effective way to protect consumers from the individual risks (see, on the one hand, chapter Data misuse caused by non-specific purposes and insufficient data use controls, and on the other hand the specified requirements in the following sub-chapters). In addition, the notification mechanism combined with the registry ensures that the knowledge necessary to identify structural risks is available. As shown, these structural risks for the society as whole do not primarily result from the individual advertisement displayed to a particular user, but from the interaction of all advertisements, for example with regard to the manipulation of public opinion (see chapter Structural risks for the society (esp. Democracy, solidarity, fair competition). This requires a mechanism that provides knowledge about all advertisements displayed in the European Single Market over a certain period of time. This can be achieved through a register and a corresponding notification obligation.

Such a mechanism that contains certification and notification obligations for all players in the online advertising ecosystem is the only conceivable way to find out where and which data is processed by whom, to encourage players to do so only within the legal framework and to find out where all the money actually goes. In concrete terms this means that **all actors that participate in the advertising ecosystem**, meaning entities that exchange personal data for the personalisation of advertising, including the management of users consent, need to register in an **European Advertising Industry Registry**.

Various solutions are conceivable as to who establishes and operates such a register. We do not consider national solutions, i.e. by institutions of the member states, to be expedient. Rather, the European Commission itself should be engaged in such a register. We therefore propose that the European Commission shall establish and ensure, directly or by entrusting this responsibility to a management authority, the management of a European Advertising Industry Registry, which shall be publicly available.

Each actor that fulfils the registry process, shall receive a unique Ad Industry ID. Each actor shall enter not less than the following information in the European Advertising Industry Registry:

- Name, address, and, if seated outside the EU, name and address of the EU-based representative;
- Ad Industry ID;
- role in the advertising ecosystem;
- total number of EU-based data subjects concerned (in case the processing of data from vulnerable people is not prohibited anyway, then these should be categorically listed here);
- complete list of types of identifiers used and for which purposes;
- complete list of types of data used and for which purposes (if sensitive data is not prohibited anyway, then these should be listed separately);
- complete list of interest categories used and for which purposes;
- purposes certified, date of certification, and certification body.

An actor may **only be entered in the European Advertising Industry Registry if** he or she provides all aforementioned information and there is **no serious breach of her actor-specific obligations** as set out in chapter 5.5.2. A serious breach shall be deemed to have occurred, inter alia, if the actor persistently fails to fulfil essential parts of his or her duties as set out in chapter 5.5.2. If an actor is **not registered**, the actor **shall not be allowed to participate in the advertising ecosystem**, meaning to process data for personalised advertising.

Each actor shall maintain a **processing directory** with the following parameter for each data subject or identifier and, if several identifiers are bundled under a so-called Ad ID, for each Ad ID, whereby all parameters may be sorted or assigned under one specific parameter:

- all identifiers collected in the advertising profile to identify a data subject, including the data of collection or creation and for which purposes the are used;
- the total number and a complete list of all attributed interests collected in the advertising profile, including the date of their collection or creation, and for which purposes the are used;
- all raw data collected about the data subject in their advertising profile, including their date and source of collection, and for which purposes the are used;
- the legal basis on which the data were collected; and
- the total number and a complete list of all receivers of that data, including their roles and the date when they got access to the personal data.

If the processing directory does **not exist, is incomplete or obviously defective**, the actor **shall not be allowed to process** the data for personalised advertising.

An actor **may only pass on the personal data to a data recipient if** the recipient:

- is registered in the European Ad Industry Register;
- indicates the (sub)purposes for which they intend to process the data; and
- their sub-purposes are covered by the legal basis on which the data was collected and the legal basis continues to be valid; and
- the recipient has the necessary certification if legally required.

If an entity who has passed on data (data donor) to a recipient has reason to consider that the data recipient is not complying with its obligations, the **data donor shall immediately stop passing on the data** and report its reasons to the data recipient, to the competent data protection authority for the recipient and, if known, to the advertiser who commissioned the respective advertising and, if possible, to the data subject. If there is no direct connection to the advertiser or data subject, the data donor passes the information on to the actors in the data value chain, asking them to pass the information on to the advertiser or data subject. The other actors shall be obliged to pass on the information if they are able to do so.

Advertisers shall specify to the commissioned actor in the advertising ecosystem

- what type of advertising they want (the purposes defined in chapter 5.3. might also be combined),
- what interests they need,
- how many data subjects they want to reach and
- whether, and if so, what measures they want to take to reduce the risks for the data subjects (e.g. exclusion of certain vulnerable groups, exclusion of certain interests, exclusion of certain data, e.g. no sensitive data or no data older than six months).

It is imperative that all these obligations are **not a voluntary nice to have, but mandatory** (for details on the failure of voluntary commitments, see chapter 2.5.8.). For the implementation of any obligations of the respective actors, the existing tools might be used, namely codes of conduct according to Art. 40 GDPR and Art. 46 DSA and certification mechanisms according to Art. 42 GDPR. Beyond that the registration, certification and notification mechanisms implemented in the REACH Regulation, which have already been tested and approved, can also serve as a model for details of new cross-actor obligations.

5.5.3 Actor-specific obligations: effective implementation

In addition, it is crucial for the effective application of corresponding new regulations that they are designed in such a way that they are both more specific than the GDPR, but may also keep pace with technological developments. One possibility, as just mentioned, is that the law itself only lays down the general criteria, but then places an obligation on the administration to provide the details by means of binding delegated acts or, at least, specifying guidelines. Yet another way is established under Art. 25 sect. 1 GDPR.

5.5.3.1 Application of Art. 25 GDPR: Main visual elements, parameters and procedures

As described before (see chapter 3.1.2.6.), Art. 25 sect. 1 GDPR obliges data controllers to implement the legal requirements in a technical and organisational manner that effectively protects fundamental rights against the respective risks. The law thus requires data controllers to provide empirical evidence of the effectiveness of its measures. The approach is even more interesting with respect to the state of the art requiring the controller to implement the most effective implementation currently available on the market. At least, in environmental law in the 1980s, the introduction of such a dynamic reference actually generated the hoped-for momentum towards ever more effective environmental protection measures.[457] In fact, such a development is also possible in data protection, provided there are empirical methods available for proving effectiveness and the public authorities adopt the current state of the art when enforcing the law. Approaches in science and even in certain data protection authorities (which, in addition to lawyers and computer scientists, now also employ first UX and UI designers and even empirically working social scientists) are already clearly moving

[457] Gawel, Technologieförderung durch „Stand der Technik“: Bilanz und Perspektiven, 2009, p. 204.

into this direction. However, it is crucial that the legislator additionally provides support by clarifying which elements and parameters are particularly important in the effective implementation and their proof of effectiveness.

In our view, the following elements and parameters need to be clarified in order to ensure that consumers are able to understand the benefits and risks and thus make a genuine balancing decision for or against the respective form of personalised advertising: A consumer must be able to

- understand on the informational basis of which type of online advertising the advertising is personalised or displayed (cf. the corresponding requirements in the PTR and DSA in chapter 5.3.);
- switch personalisation, if present, on and off, so that they can experience / compare whether the advertising is really relevant to them;
- get the information about
    - the attributed interests on which the personalised advertising is based and for which purposes the are used,
    - the total number and type (including the date of collection) of the raw data used to personalise the specific advertisement and for which purposes the are used,
    - the total number and type (including the date of collection or creation) of the identifiers used to identify the data subject for the specific advertisement and for which purposes the are used, and
    - the total number and a complete list of all data holders[458]/ receivers involved in the specific advertisement including their roles;
- exercise their data subject rights via an interface or a link provided via this interface (see Art. 19 PTR), i.e. in particular to access, correct and/or delete the personal data about them held by the involved data holders/ receivers, be it the identifiers connected to the data subjects, the interests attributed to them or the underlying raw data;
- all four control and transparency mechanisms must be as easy as possible accessible on the same page on which the personalised advertising is displayed (see Art. 19 PTR and Art. 26 DSA), in the event of exercising the data subject rights,
    - a link to each single data holder/ receiver involved in the specific advertisement,
    - and a list to all, if existent, third party providers that support data subjects in exercising their data subject rights (esp. consent agent providers and privacy dashboard providers).

All these elements and parameters already follow from the application of Art. 25 sect. 1 GDPR, as soon as there is empirical evidence that these elements and parameters effectively (or even most effectively) protect data subjects from the risks of personalised advertising. However, to avoid legal uncertainty, these elements and parameters should additionally be clarified in a new regulation specifying the GDPR accordingly. On the basis of Art. 25 sect. 1 GDPR, the remaining aspects that need to be clarified are how the data controllers, in particular publishers, must implement these elements

[458] Data holders shall mean all parties that process the personal data of consumers, regardless of whether they are currently involved in displaying an advertisement on this website or not.

and parameters in their visual interface designs, concretely. This, too, must be explicitly clarified, in particular:

- the empirical methods that data controllers must use to prove effectiveness, in particular from human computer interaction and user experience design research,
- the meaning and functioning of the state of the art, as the most effective implementation of a legal provision available and demonstrably effective on a market,
- and that the controllers must disclose the methods that they have used and the state of the art to which they are referring.

Beyond that, the EDPB should update its Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Although (so far) no legal changes have been made to Art. 25 GDPR since the guideline was published, in terms of methodology in the assessment of effective implementation there has been great improvements, in particular, in research developing these empirical methods.[459] These external circumstances that influence the assessment of Art. 25, should be taken into account by adapting the guidelines accordingly.

On this clarified basis, it is much more reasonable that Art. 25 sect. 1 GDPR will actually be implemented in practice and contribute to the hoped-for development dynamic towards increasingly effective protection measures.

5.5.3.2 Consent agents and privacy dashboards: Ensuring the technical interlaces

A new regulation should also set out the conditions for the use of consent agents and privacy dashboards, which data subjects may use to manage their consent and exercise data subject rights. Consent agents and privacy dashboards, as shown above, are essential to counter consent fatigue and to enable data subjects to effectively exercise their data subject rights. To do this, however, publishers and all other parties, who usually obtain consent for personalised advertising on a case-by-case basis, must be obliged to accept the signals from consent agents. Without such an obligation, most websites and other service providers will continue to ask for their own consent, based on the fact that more users will give it due to fatigue.

Even more important is such an obligation for browser providers to forward such signals to the publishers and, eventually, other service providers. For browsers, such an interface is currently possible for stationary operating systems by means of a browser extension. However, this only applies to a limited extent to mobile browsers, which are now predominantly used.[460] Here, users must laboriously set up certain permissions in the settings of the mobile operating system before their consent management service may send, for example in the form of a mobile app or web app, technical signals to the websites visited. In practice, the click path needed for such a

[459] See,for example, the research groups around Cristiana Santos (law), Nataliia Bielova (computer science) and Colin Gray (Human Computer Interaction), or Arianna Rossi (legal design) and Gabriele Lenzini (computer security), or Alessandro Acquisti (information technology and public policy), Lori Cranor (security and privacy technologies), and Norman Sadeh (computer science).

[460] Statcounter, 1.11.2016, Mobile and tablet internet usage exceeds desktop for first time worldwide, https://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

setup will mean that consent agents will only be used to a very limited extent for mobile surfing.

A similar legal obligation is finally needed for publishers and the other parties to provide a technical interface through which consumers can access a privacy dashboard in order to exercise their data subject rights. As shown above in the analysis of the current regulatory framework, there is currently only such an explicit obligation for publishers in the PTR, and even there it is unclear where exactly this link should be made available for the data subjects (see chapter 3.4.2.). This uncertainty seems to be thoughtless, as it is likely that publishers will not provide this link in the immediate context of the displayed advertisement, as is actually required by the rules of good UX design, but somewhere more hidden.

So far, corresponding requirements can only be derived from Art. 25 sect. 1 GDPR, at the latest when it has been empirically proven that such integration of consent agents and privacy dashboards enable data subjects to more effectively protect themselves against the risks of personalised advertising than the design currently applied in practice. In order to avoid the associated legal uncertainties described above (see chapter 3.1.2.6.), publishers and browser providers should be explicitly required to provide for these interfaces, while clarifying the basic User Interface requirements.

In return for this obligation (and only for this), the providers of consent agents and privacy dashboards must fulfil two conditions: Firstly, the providers of browsers and publishers and similar providers have a legitimate security need to ensure that these interfaces are not exploited by malicious third parties, for example for malware attacks. For this reason, providers of consent agents and privacy dashboards must be accredited by a competent authority. This organisational mechanism ensures that these ‘third-party providers’ are trustworthy providers. The accreditation must be transferred to the providers of browsers, websites and the like via technical certification.

In addition, the providers of consent agents and privacy dashboards, for their part, must also prove that their information and control architectures are effective and take into account the state of the art. Particular attention must be paid to ensuring that these architectures also present the benefits and risks and thus enable consumers to make a real decision for or against the respective form of personalised advertising. Consent agents that aim to deny consent as easily as possible without evoking a real (namely informed) decision from the consumer are just as unlikely to meet the regulatory objective as a consent whose design is only aimed at getting the user to press accept as quickly as possible without having understood what they are actually consenting to.

However, with regard to the German regulation, it should be pointed out once again that such an obligation to accredit providers of consent agents and privacy dashboards is only justified in return for a corresponding obligation on the part of publishers and browser providers to make the corresponding links available and to accept the technical signals.

Last but not least, it should also be pointed out, already here, that gatekeepers, in particular providers of browsers with market dominance, must not themselves offer consent agents and privacy dashboards for the submission of consent to third parties or the exercise of data subject rights vis-à-vis third parties. The reason for this is that it would lead to a further increase in power on their side. Current developments are impressive proof of the corresponding interest of gatekeepers. Therefore, a new regulation must also regulate their exclusion from offering consent agent and privacy dashboard services.

5.5.3.3 Practical realisation

Publishers are best placed to obtain the end-user's consent due to their visual interface with the end-user; it should therefore be made clear that they are the ones that shall obtain consent. To increase effectiveness of consent, publishers **must implement the elements, parameters and procedures for effective consent as proposed above** (see chapter 3.1.2.6.).

To avoid consent fatigue, in particular, **publishers may not request consent again within a period of one year** after a user has given, refused or changed their consent for one or more purposes. A new request is only allowed within this period if significant circumstances have changed; this includes when a publisher

- makes a request for a new processing purpose for which the publisher has not yet made a request;
- has to request renewed consent or at least indicate the possibility to withdraw consent or object to the data processing due to a significant change in the processing operations for a purpose for which the user has already given consent; or
- wishes to make a renewed request, if the user has already refused consent for a purpose, but the processing procedures have become significantly more data protection-friendly, so that fewer or lower risks now arise.

In order to recognise the user when they visit the website or service again and to be able to retrieve their decisions, the publisher must and may place a cookie on the user's browser; the use of the cookie is limited to this purpose (in doing so, it is important to ensure that the data-minimisation principle is met, in particular that no IDs are used, which go beyond what is necessary).[461]

To increase informedness and avoid consent fatigue, **publishers must** also **accept and respect signals from content agent providers** and privacy dashboard providers. This means that when a user of a consent agent visits the publisher's website or starts using its service, the publisher may and must only display a prompt asking if the end user wants to change their consent preferences for the site or service as submitted through the consent agent; however, if the user does not respond to the prompt in a time, which is reasonable from the users' perspective, the publisher must withdraw the prompt so as not to coerce the user into actively clicking away the prompt. The publisher must empirically determine and prove, in accordance with Art. 25 sect. 1 GDPR, the appropriate time period, in which the user may react to the change request.

Last but not least, **publishers must inform data subjects via their cookie banner about the existence of consent agent providers** providing a complete and non-discriminatory list of all accredited consent agent providers with a direct link through which data subjects may download the consent agent of their choice.

Publishers shall only share the personal data they were allowed to collect based on consent or in the absence of objection by the data subject, **along with all identifiers**

[461] See, for example, DSK, Orientierungshilfe Telemedien, 2022, para. 79.

they have **used** to identify the data subject **for the purpose of personalised advertising**.

Consent agent providers must ensure that their end-users understand the consequences of their consent or objection pre-settings through an appropriate design of their visual interfaces in accordance with Art. 25 sect. 1 GDPR and **are** therefore **able to make informed balancing decisions** accordingly (see chapter 5.5.3.2.); the same applies to **privacy dashboard providers** with respect to the exercise of the data subject rights.

Advertising service providers, meaning alll actors within the advertising ecosystem, **must inform the publisher** along with the personalised advertisement **and, upon request of the data subject,** consent agent providers and **privacy dashboard providers**, via a technical interface, **of the following information** about the data subject on which the personalised advertisement is based (see chapter 3.1.2.6.):

- the attributed interests on which the personalised advertising is based,
- the total number and type (including the date of collection) of the raw data used to personalise the specific advertisement,
- the total number and type (including the date of collection or creation) of the identifiers used to identify the data subject for the specific advertisement, and
- the total number and a complete list of all data holders/ receivers involved in the specific advertisement including their roles.

Furthermore, advertising service providers **must provide the publisher and, upon request of the data subject,** consent agent providers and **privacy dashboard providers with a link through which data subjects may exercise their data subject rights** vis-à-vis the respective advertiser.

In all cases, the **identification of the data subject** in the data set of the advertising service provider **is done by means of the identifier(s) that the advertising service provider has received** from the publisher and, if applicable, from the consent agent provider or privacy dashboard provider.

Insofar as **advertising service providers** take on the role of gatekeepers, they are not allowed to process the data of end users generated by the use of third-party services that in turn use core platform services of the gatekeeper. The gatekeeper may only process the data on the basis of the end user's consent. For example, if a publisher uses an advertising service from Google, Google may only process this data for the purposes of personalised advertising if consent has been obtained to do so. In doing so, Art. 5 sect. 2 lit. a DMA clarifies that advertising service providers, if they are gatekeepers (such as Google), must obtain consent in any case, regardless of whether they are itself a controller or only a processor (see above chapter 3.6.). Gatekeepers must make sure that the consent retrieved complies with the requirement from Art. 25 sect. 1 GDPR that the consent is effective.

Data holders[462]/ receivers must inform, upon request of the data subject, consent agent providers and privacy dashboard providers, via a technical interface, **of the following information** about the data subject (see chapter 3.1.2.6.):

[462] Data holders shall mean all parties that process the personal data of consumers, regardless of whether they are currently involved in displaying an advertisement on this website or not.

- the total number and a complete list of all attributed interests collected in the advertising profile,
- all raw data collected about the data subject in their advertising profile,
- all identifiers collected in the advertising profile to identify the data subject, and
- the total number and a complete list of all data holders / receivers, including their roles, who got access to what exact personal data for which specific (sub)purpose.

In all cases, the **identification of the data subject** in the data set of the data receiver **is done by means of the identifier(s) that the advertising service provider has received** from the publisher and, if applicable, from the consent agent provider or privacy dashboard provider.

Upon request, **browser providers must accept and transmit the signals** received from consent agent providers and privacy dashboard providers to publishers, on the one hand, and accept and transmit the signals received from publishers to consent agent providers and privacy dashboard providers, on the other hand.

5.6 ECONOMIC ASPECTS: CONTROLLING GATEKEEPERS AND SUPPORTING SMES

In summary, the following three aspects must be taken into account in the proposed requirements for the parties involved in the personalisation of advertising. Firstly, the requirements and procedures for their verification should be designed in such a way that they correspond to the resource-related possibilities of SMEs. Since the above requirements are largely based on IABs TCF and only partially tighten them, but above all simply transfer them into an objectively binding legal regime, the requirements in principle go only slightly beyond the already existing ones.

Requirements for the effective implementation of the consent processes pursuant to Art. 25 para. 1 and Art. 6 para. 1 lit. a GDPR must be demonstrably effective and must consider the state of the art. Insofar as such a state of the art already exists, SMEs can adopt it in the implementation of their own consent processes. In doing so, they may take the implementation costs into account. However, in view of the high speed of development of the technical and organisational infrastructure and the associated high frequency of updates, the adaptations can usually be incorporated incrementally and thus cost-effectively into a company's own processing procedures. Where no state of the art yet exists, they must at least fall back on the recognised rules of technology. Actors who make the further development of the state of the art an integral part of their business model can gain a competitive advantage from the specifications. Furthermore, so-called innovation laboratories should be considered, along the lines of the AI Act (see Art. 57 et seq, in particular, Art. 62 AI Act), in which the relevant authorities, together with the scientific community, support SMEs in developing and implementing particularly data protection-friendly technologies (see chapter 5.3.6.).

The certification procedures should not only take into account the size of the applicant and the scope of the data processing to be certified in the fee schedules. According to the accountability principle, the higher the risks of data processing for consumers and society as a whole, the stricter the procedures should be designed. Given the previously proposed differentiation of sub-purposes for personalised advertising, SMEs are easily able to choose less risky data processing purposes and operations and thus leaner certification procedures. Certification procedures must reflect these differences.

In principle, the certification processes for an applicant company become more complex the larger and more extensive the data processing operations are. The certification procedures will therefore be more costly for quasi-monopolistic companies, which are relatively complex due to the horizontal and vertical integration of a very large number of different processing operations along the data value chain.

In order to counteract the increasing concentration of power in the information economy, gatekeepers should also be prevented from integrating additional services into their portfolio. These include, in particular, personal information management services such as consent agents. The requirements of Art. 12 DGA should be tightened in this respect. Similar to the DA, which also prohibits certain practices in connection with the gatekeeper role (see Art. 5 sect. 3 DA), gatekeepers should therefore be excluded from the possibility of offering their own PIMS (in contrast, see the current developments in chapter 2.5.1.2.).

5.7 RESPONSIVE REGULATION: SYNCHRONISING THE HIGH PACE OF TECHNOLOGICAL DEVELOPMENT WITH REGULATORY PROCESSES

A specific challenge that regulators face in the area of technology law is the question of how they can keep pace with the high speed of technological development in practice and help shape it in time. The question arises at all levels of regulation, with state procedures generally becoming more complex and time-intensive the higher up the governmental measure is zoned in the state structure (for example, from an enforcement authority to administrative legislation through to the parliamentary legislature). Ultimately, this is about the conflict between democratic legitimacy, direct or indirect legal effect on the actors and speed of action or reaction.

The proposals made above should be set out in a separate law, whether as part of a new ePrivacy Regulation, a stand-alone AdTech Act or as part of the updating of European consumer protection law. This is already required by the need for significantly greater legal certainty (see chapter 3.1.). This opportunity should also be taken to clarify the responsibilities of the enforcement authorities, which lead to ever greater coordination difficulties with each new law that overlaps in its scopes of application.

However, such a law must also take into account the need for openness to innovation and technological development. Not least as a result of the competition promoted here towards ever more data protection-friendly processing operations, it is quite conceivable that new sub-purposes might emerge that require independent purpose specification due to their specific risk contribution. In such cases, the law should define the conditions and the procedure under which a fast-track administration may issue corresponding delegated acts.

Last but not least, the enforcing entities, such as data protection authorities, should build up the competences not only in legal and technical terms, but also in terms of User Experience and User Interface design and empirical research methods. This is necessary to be in a position to check the effectiveness of the consent processes developed in the industry themselves and, if necessary, to develop their own positive examples.

6 CONCLUSION AND RECOMMENDATION: COMBINING COMPLEMENTARY REGULATORY MECHANISMS

The current ecosystem of personalised online advertising is very complex; on closer inspection, the underlying data processes and even payment flows appear messy and chaotic. The risks are correspondingly numerous and severe, both for individuals and for society as a whole. The individual risks include, in particular, uncontrolled insights into the private lives of consumers, manipulation, discrimination as well as material and health damage. Structural risks for society as a whole include, in particular, risks to free competition, democracy, public discourse and solidarity, but even security and environmental protection.

Empirical studies show that consumers have little trust in the current processing operations and rate the current implementation of data protection in the area of personalised advertising, particularly in the form of informed consent, as very poor. In view of non-transparent, deceptive and manipulative consent processes and the extremely high number of consents requested per day, which inevitably leads to consent fatigue, consumers alternate in their mood between powerlessness and fatalism. In view of this sentiment, some readers might find it astonishing that some consumers nevertheless see added value in personalised advertising, at least to the extent that it actually makes advertising more relevant to them. However, due to a lack of suitable mechanisms, consumers are currently unable to verify the allegedly increased relevance of personalised advertising.

Due to the general increase in attention for data protection, the loss of consumer trust in data processing, the numerous criticisms from scientific and civil society actors and the increased regulatory pressure, a number of data protection-friendly approaches have emerged in the area of personalised advertising in recent years. These include approaches to improve consent processes and other control options, be it government initiatives or so-called Personal Information Management Services (PIMS) from the industry or civil society. On the other hand, structural-objective approaches have also been developed to reduce risks independently of individual control by consumers, such as cohort-based personalisation, topics-based personalisation, contextual advertising, as well as encrypted and aggregated conversion measurement.

However, there are also developments that threaten to further worsen the current situation. Under certain circumstances, these include the so-called pay-or-okay model with questionable social consequences; and at any rate the use of data protection law and AI technologies by quasi-monopolistic providers to further accumulate economic and informational power. This further accumulation of power is problematic for consumers for two reasons: first, further power concentration leads to less services for consumers, which potentially provide for higher data protection levels; second, it leads to further informational power which data protection actually seeks to prevent.

With the GDPR, the EU legislator has provided a general regulatory framework that would in principle be flexible enough to control the aforementioned risks and promote emerging data protection initiatives. This includes, in particular, the data protection by design approach, which obliges data controllers to effectively control the risks through technical and organisational measures and to empirically prove their effectiveness by taking into account the current state of the art (i.e. the best measure available on the market). This approach has the potential to create a dynamic of innovation towards ever more data protection-friendly technologies, even in the current online advertising ecosystem.

However, the effective implementation of the GDPR suffers from a combination of four main factors: 1) the considerable legal uncertainties, 2) the complexity of the online advertising ecosystem, 3) the resulting lack of knowledge, ability and willingness of the economic players to implement the GDPR effectively (which, as in the case of the TCF of IAB Europe, results from the one-sided representation of interests and governance problems of its self-regulatory approach) and, last but not least, 4) the high legal enforcement deficit.

Against this background, it was highly instructive to analyse further legislative approaches that the legislator has adopted in response to these deficits (but also to specific new problems). These further laws can be read as a learning curve, in the course of which the legislator addressed the problems described in an increasingly specific manner: These include, in particular, 1) the clarification of legal requirements for specific sectors and actors; and 2) a clear assignment of technical and organisational cooperation obligations to overcome governance problems (and knowledge deficits) in complex processing networks.

Our regulatory proposal takes up the results of these analyses and builds, conceptually, on the approach of regulating innovation. According to this approach, laws should be designed in such a way that they not only provide effective protection against the risks (of data-driven innovation, for example), but also do not unnecessarily hinder or even promote innovation. It is therefore a regulatory approach that focuses on the innovative capacity of markets and thus fits in well with the EU's understanding of enabling and maintaining innovative (data-driven), but also value-orientated markets.

On this conceptual basis, our regulatory proposals are primarily aimed at creating a (more direct) market between consumers and advertisers by creating a (much more direct) feedback loop between both parties. Such feedback enables the parties to see which target groups they reach through which mechanisms and, vice versa, which advertisements they see based on these mechanisms. Both were relatively easy to understand in the offline advertising market. However, with the development of the online advertising market, online advertising services have emerged whose systems are so complex that no one – not even the advertising services themselves – can understand these mechanisms. This applies regardless of whether the complexity arises from the interaction of hundreds of companies (as in the case of the TCF) or from the horizontal and vertical integration of the various data processing operations within one quasi-monopolistic entity.

The most important mechanism for restoring this direct feedback – despite all the criticism – is informed consent, supposed to be truly effective. However, for consent to be truly effective, a number of key legal, technical and organisational conditions must be met. The main criticism of the consent model does therefore less concern, in our opinion, the consent model per se (however, see the conceptual limitations of the consent model in chapter 2.4.1.), but its poor implementation. In contrast, truly effective consent would create a market between consumers and advertisers regarding the method of personalised advertising in question. In our view, this would lead to competition between advertising services and spark a dynamic of innovation towards ever more data protection-friendly methods. Such an effective implementation of consent does not only solve numerous problems on the side of the consumers, but also for the society as whole, not only but above all for a fair market. In particular, advertisers would finally be in a position to make sure that they reach the consumer groups who appreciate the why and how the advertisers reach them and, therefore, safeguard their brand safety.

Interestingly, the regulatory approach we propose results in hardly any additional regulatory requirements, at least for small and medium-sized advertising services. In fact, our approach is largely based on the approach that the TCF is establishing anyway with its legal, technical and organisational specifications as well as certification requirements. Thus, structurally, the requirements are already implemented in the online advertising ecosystem anyway. To overcome the governance problem described above, we simply convert the requirements into an objectively legally binding system. Overall, our proposal creates a fairer level playing field, especially in relation to the quasi-monopolistic Big Tech companies.

In fact, there are significant economic advantages for the online advertising ecosystem. At a micro- and meso-economic level, innovative advertising services can gain a competitive advantage by restoring consumer trust with more privacy-friendly technologies, and thus eventually a higher consent rate. On a macroeconomic level, our regulatory proposal creates a functioning market in which consumers‘ expectations of online advertising, in terms of benefits and risks, and advertisers’ offers can finally be brought into an efficient equilibrium.

In this context, it should be emphasised that our approach, albeit not intended and not very far-reaching, may also contain the superiority of Big Tech with all its adverse effects on fair competition and information power. In particular, due to the sheer size of the integrated processing systems, the quasi-monopolies are likely to have more difficulty untangling them in the context of a risk management audit than smaller companies that only perform some of these operations. Of course, our proposal does not aim at breaking up the economic power of quasi-monopolies by means of data protection law. This is not the task of data protection laws. If one wants to break the economic superiority of these quasi-monopolies, one might have to consider a separation of certain processing structures, such as the separation of browsers and devices from the actual advertising services. However, this is a matter for competition law and not the subject of this report.

Last but not least: only if the coordination required for a socially sustainable advertising ecosystem proves to be prohibitively challenging, despite our proposed support, the legislator may have to ban personalised advertising, as a whole. The risks to consumers and society caused by current online advertising practices are just too high. In such a case, however, a complete ban of personalised advertising would not only be the most legally effective measure, but also the most economically effective.

REFERENCES

Alvim, M./ Fernandes, N./ McIver, A./ Nunes, G., The Privacy-Utility Trade-off in the Topics API, Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS), June 2024, 1-21, https://doi.org/10.48550/arXiv.2406.15309

Acquisti, A./ John, L. K./ Loewenstein, G., What Is Privacy Worth? The Journal of Legal Studies, 2013, 249-274, DOI: 10.1086/671754

Alizadeh, F./ Jakobi, T./ Boldt, J./Stevens, G., GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies, MuC '19: Proceedings of Mensch und Computer 2019, pp. 811 - 814, https://doi.org/10.1145/3340764.3344913

Armitage, C./ Botton, N./ Dejeu-Castang, L./ Laureline L. (AWO Belgium), Towards a more transparent, balanced and sustainable digital advertising ecosystem: Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers, Study prepared for the European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/

Art. 29 Data Protection Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, 2018, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/position-paper-derogations-obligation-maintain-records_en

Art. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251), 6.2.2018, https://ec.europa.eu/newsroom/article29/items/612053/en

Art. 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248), 4.4.2017, https://ec.europa.eu/newsroom/article29/items/611236/en

Art. 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203), 2.4.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Art. 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (WP 171), 22.6.2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

Bauer, J. M./ Bergstrøm, R./ Foss-Madsen, R., Are you sure, you want a cookie? - The effects of choice architecture on users’ decisions about sharing private online data, Computers in Human Behavior, 120/2021, 1-41, https://doi.org/10.1016/j.chb.2021.106729

Baumgartner, U./ Hansch, G., Onlinewerbung und Real-Time-Bidding: Datenschutzrechtliche Fragen im Lichte der BGH-Entscheidung Cookie-Einwilligung II, Zeitschrift für Datenschutz (ZD), 2020, 435-439

Becker, M., Consent Management Platforms und Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung - Real Time Bidding auf Basis von Nutzerprofilen als Ausprägung der Personendatenwirtschaft, Computer & Recht (CR) 2021, 87-98, https://doi.org/10.9785/cr-2021-370205

Benda, E., Privatsphäre und Persönlichkeitsprofil, in: Gerhard Leibholz et al. (eds.), Menschenwürde und freiheitliche Rechtsordnung, Festschrift für Willi Geiger zum 65. Geburtstag, 1974, 23-44

Beugin, Y./ McDaniel, P., Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving), Proceedings on Privacy Enhancing Technologies (PoPETs) 2024, 1–17, https://doi.org/10.48550/arXiv.2306.03825

Beugin, Y./ McDaniel, P., A Public and Reproducible Assessment of the Topics API on Real Data, IEEE Security and Privacy Workshops (SPW), 2024, 1-17, DOI: 10.1109/SPW63631.2024.00005

Bieker., F., The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law, 2022

Bleier, A., On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web, Social Science Research Network (SSRN), 2021, 1-40, https://dx.doi.org/10.2139/ssrn.3980001

Bouhoula, A./ Kubicek, K./ Zac, A./ Cotrini, C./ Basin, D., Automated Large-Scale Analysis of Cookie Notice Compliance, 33rd USENIX Security Symposium 2024, 1723-1739, https://www.usenix.org/conference/usenixsecurity24/presentation/bouhoula

Britz, G., Informationelle Selbstbestimmung - zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, W. (ed.), Offene Rechtswissenschaft, 2010, 561-596

Bundeskartellamt, Sektoruntersuchung Online-Werbung - Diskussionsbericht, August 2022, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Online_Werbung_Diskussionsbericht_lang.pdf?__blob=publicationFile&v=3

Bygrave, L. A., Core Principles of Data Privacy Law', Data Privacy Law: An International Perspective, 2014, https://doi.org/10.1093/acprof:oso/9780199675555.003.0005.

Cantu, C., Neuroprogrammatic Is the Future of Contextual Advertising, AdMonsters, 19.4.2023, https://www.admonsters.com/neuroprogrammatic-is-the-future-of-contextual-advertising/

Centre for Strategy & Evaluation Services (CSES), Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161, Study prepared for the European Commission, 4.10.2024, https://commission.europa.eu/publications/study-support-fitness-check-eu-consumer-law-digital-fairness-and-report-application-modernisation_en

Cisco, Consumer Privacy Survey - Privacy Awareness: Consumers Taking Charge to Protect Personal Information, 2024, https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html

Cisco, Consumer Privacy Survey - Building Consumer Confidence Through Transparency and Control, 2021, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf

Chavez, A., A new path for Privacy Sandbox on the web, 22.7.2024, https://privacysandbox.com/news/privacy-sandbox-update/

Chen, B., The Battle for Digital Privacy Is Reshaping the Internet, New York Times, 16.9.2021, https://www.nytimes.com/2021/09/16/technology/digital-privacy.html

Claburn, T., Shot down: Google's grand fancy plan for pro-privacy targeted ads, The Register, 18.1.2023, https://www.theregister.com/2023/01/18/google_topics_api/

ConPolicy, Good Practice Initiative for Cookie Banner Consent Management, Design Guidelines, 26.1.2023, https://www.bmuv.de/fileadmin/Daten_BMU/Download_PDF/Verbraucherschutz/cookie_guidelines_en_bf.pdf

D64 - Zentrum für Digitalen Fortschritt e.V., Utiq unter der Lupe: Zukunft des Trackings oder Bedrohung für die digitale Privatsphäre?, Mai 2024, https://d-64.org/wp-content/uploads/2024/05/D64_Recherche-Utiq.pdf

Dachwitz, I., Neue Tracking-Firma Utiq: Wie Telekom, o2 und Vodafone im Datengeschäft mitmischen, Netzpolitik, 15.5.2024, https://netzpolitik.org/2024/neue-tracking-firma-utiq-wie-telekom-o2-und-vodafone-im-datengeschaeft-mitmischen/

Dachwitz, I., Microsofts Datenmarktplatz Xandr: Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert, Netzpolitik, 8.6.2023, https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/

Dachwitz, I., Werbetracking: Wie deutsche Firmen am Geschäft mit unseren Daten verdienen, Netzpolitik, 8.6.2023, https://netzpolitik.org/2023/adsquare_theadex_emetriq_werbetracking-wie-deutsche-firmen-am-geschaeft-mit-unseren-daten-verdienen/

Dachwitz, I./ Meineck, S., Databroker Files: Firma verschleudert 3,6 Milliarden Standorte von Menschen in Deutschland, Netzpolitik, 16.7.2024, https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/

Dachwitz, I./ Meineck, S., Datenhändler verticken Handy-Standorte von EU-Bürger*innen, Netzpolitik, Netzpolitik, 17.1.2023, https://netzpolitik.org/2024/berliner-unternehmen-datenhaendler-verticken-handy-standorte-von-eu-buergerinnen/

D'Amico, A./ Pelekis, D./ Santos, C./ Duivenvoorde, B., Meta's Pay-or-Okay Model - An analysis under EU Data Protection, Consumer and Competition Law, Technology and Regulation (TechReg) 2024, 254-272, https://doi.org/10.26116/techreg.2024.019

Data Protection Commissioner of Ireland (DPC), Annual Report 2023, https://www.dataprotection.ie/sites/default/files/uploads/2024-08/DPC-EN-AR-2023-Final-AC.pdf

Data Protection Commissioner of Ireland (DPC), Annual Report 2016, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Annual%20Report%202016.pdf

Datenschutzkonferenz (DSK), Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) Version 1.1, Dezember 2022, https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

Datenschutzkonferenz (DSK), Bewertung von Pur-Abo-Modellen auf Websites - Beschluss, 22.3.2023, https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

Deutschlandfunk Nova, Auf Cookies verzichtet – trotzdem viel Geld mit Online-Werbung verdient, 6.8.2020, https://www.deutschlandfunknova.de/beitrag/personifizierte-werbung-ohne-cookies-geht-es-auch

Dunphy, S., Women are seeing fewer STEM job ads than men: are marketing algorithms promoting gender bias?, European Scientist, 28.7.2018, https://www.europeanscientist.com/en/public/women-are-seeing-less-stem-job-ads-than-men-are-marketing-algorithms-promoting-gender-bias/

Eberl, M., Tracking durch Identitätsprovider, Kuketz-Blog, 5.12.2021, https://www.kuketz-blog.de/tracking-durch-identitaetsprovider/

Engle, E., Third Party Effect of Fundamental Rights (Drittwirkung), Hanse Law Review (HanseLR), 2009, 165-173, http://hanselawreview.eu/wp-content/uploads/2016/08/Vol5No2Art02.pdf

European Commission, Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, Discussion Paper for Stakeholders´ Roundtable, 2023, https://commission.europa.eu/document/download/2594371b-b92b-4ef7-87f6-c0048ee684ed_en?filename=Discussion%20paper%20for%20stakeholders%27%20roundtable%20on%20cookies.pdf

European Commission Directorate-General for Justice and Consumers, Consumer Conditions Scoreboard, March 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1891

European Data Protection Board (EDPB), Guidelines 1/2024 on processing of personal data based on Article 6 (1) (f) GDPR, Version 1.0, 8.10.2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

EDPB, Opinion 8/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 17.4.2024, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

EDPB, Report on the use of SPE external experts, 16.4.2024, https://www.edpb.europa.eu/system/files/2024-06/edpb_1st_report-support-pool-experts-programme_en.pdf

EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, Version 2.0, 7.10.2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

EDPB, Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023, https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

EDPB, Guidelines 6/2022 on the practical implementation of amicable settlements, Version 2.0, 12.5.2022, https://www.edpb.europa.eu/system/files/2022-06/edpb_guidelines_202206_on_the_practical_implementation_of_amicable_settlements_en.pdf

EDPB, Guidelines 3/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, 14.2.2023, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

EDPB, Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13.4.2021, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7.7.2021, https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

EDPB, Guidelines 5/2020 on consent under Regulation 2016/679, Version 1.1, 4.5.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 12.3.2019, https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20.10.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

EDPS, Personal Information Management Systems, TechDispatch, 3/2020, https://data.europa.eu/doi/10.2804/11274

EDPS, Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data, OJ C225, 16.7.2014, p. 6-12, https://www.edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_ex_sum_en_0.pdf

Ehmann, E./ Selmayr, M., DS-GVO Kommentar, 3rd Edition 2024

European Interactive Digital Advertising Alliance, Your Online Voices: What consumers told us about their perceptions, needs, hopes, and expectations of data-driven advertising, https://edaa.eu/wp-content/uploads/YOV_external-report_27.06.pdf

Feng Y./ Yao, Y./ Sadeh, N., A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things, CHI Conference on Human Factors in Computing Systems (CHI) 2021, 1-16, https://doi.org/10.1145/3411764.3445148

Forbrukerrådet, Surveillance-based advertising - Consumer attitudes to surveillance-based advertising, Population survey conducted by YouGov on behalf of the Norwegian Consumer Council, June 2021, https://storage02.forbrukerradet.no/media/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf

Forbrukerrådet, Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy, June 2018, https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf

Forgó, N./ Krügel, T./ Rapp, S., Zwecksetzung und informationelle Gewaltenteilung, 2006

Förster, M., Für Werbung: Firefox sammelt ab sofort standardmäßig Nutzerdaten, Heise, 15.7.2024, https://www.heise.de/news/Fuer-Werbung-Firefox-sammelt-ab-sofort-standardmaessig-Nutzerdaten-9801279.html

Förster, M., Firefox verteidigt sich: Alles richtig gemacht, nur schlecht kommuniziert, Heise, 16.7.2024, https://www.heise.de/news/Firefox-verteidigt-sich-Alles-richtig-gemacht-nur-schlecht-kommuniziert-9802473.html

Fouad, I./ Santos C./ Laperdrix, P., The Devil is in the Details: Detection, Measurement and Lawfulness of Server-Side Tracking on the Web, Proceedings on Privacy Enhancing Technologies (PoPETs) 2024, 450–465, https://doi.org/10.56553/popets-2024-0125

FTC Staff Report, Self-Regulatory Principles for Online Behavioral Advertising, February 2009, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

Führ, M./ Bizer, K., Zuordnung der Innovations-Verantwortlichkeiten im Risikoverwaltungsrecht – Das Beispiel der REACh-Verordnung, in: Eifert/ Hoffmann-Riem (ed.), Innovationsverantwortung, 2009

Gawel, E., Technologieförderung durch „Stand der Technik": Bilanz und Perspektiven, in: Eifert/ Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 2009, 197–218

Gersdorf, H./ Paal, B. (ed.), BeckOK Informations- und Medienrecht, Article-by-Article Commentary, 45. Edition 2024

Gluck, J./ Schaub, F./ Friedman, A./ Habib, H./ Sadeh, N./ Faith Cranor, L./ Agarwal, Y., How short is too short? Implications of length and framing on the effectiveness of privacy notices, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 321-340, https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf

Golla, S. J., Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, Journal of intellectual property, information technology and electronic commerce law (JIPITEC), 2017, 70-78, https://www.jipitec.eu/archive/issues/jipitec-8-1-2017/4533/JIPITEC_8_1_2017_Golla.pdf

Google, The Basics of Micro-Moments, 2016, https://www.thinkwithgoogle.com/consumer-insights/consumer-journey/micro-moments-understand-new-consumer-behavior/

Grafenstein, M. v., Effective regulation through design: Cookie Pledge, Do Not Track... How Is All That Supposed To Work From A User's Point Of View?, Social Science Research Network (SSRN), 2024, 1-113, https://dx.doi.org/10.2139/ssrn.4934679

Grafenstein, M. v., Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design, in: González-Fuster, G., van Brakel, R., De Hert, P. (eds.), Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, 1st Edition 2022, pp. 402-432

Grafenstein, M. v., Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework, HIIG Discussion Paper Series, 2022 (2). DOI: 10.5281/zenodo.7390542

Grafenstein, M. v., Refining the concept of the right to data protection in Article 8 ECFR – Part III: Consequences for the interpretation of the GDPR (and the Lawmaker's Room for Manoeuvre), European Data Protection Law Review (EDPL) 2021, 373-387, https://doi.org/10.21552/edpl/2020/4/7

Grafenstein, M. v., Refining the concept of the right to data protection in Article 8 ECFR – Part II: Controlling Risks Through (not to) Article 8 ECFR Against Other Fundamental Rights, European Data Protection Law Review (EDPL) 2021, 190-205, https://doi.org/10.21552/edpl/2021/2/8

Grafenstein, M. v., Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I: Finding an Appropriate Object and Concept of Protection by Re-Connecting Data Protection Law with Concepts of Risk Regulation, European Data Protection Law Review (EDPL) 2020, 509-521, https://doi.org/10.21552/edpl/2020/4/7

Grafenstein, M. v., The Principle of Purpose Limitation in Data Protection Laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, 2018

Grafenstein, M. v./ Heumüller, J./ Belgacem, E./ Jakobi, T./ Smieskol, P., Effective regulation through design - Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach, June 2021, 1-31, DOI: 10.5281/zenodo.5008420

Grafenstein, M. v./ Hölzel, J./ Irgmaier, F./ Pohle, J., Nudging - Regulierung durch Big Data und Verhaltenswissenschaften, Gutachten, 30.7.2018, https://www.abida.de/sites/default/files/ABIDA-Gutachten_Nudging.pdf

Grafenstein, M. v./ Kiefaber, I./ Heumüller, J./ Rupp, V./ Graßl, P./ Kolless, O./ Puzst, Z.., Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Computer Law & Security Review, 52/2024, 1-26, DOI: 10.1016/j.clsr.2023.105924

Grassl P./ Gerber N./ Grafenstein M. v., How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights?, European Data Protection Law Review (EDPL), 2024, 96-104, https://doi.org/10.21552/edpl/2024/1/14; see also the extended version with charts and graphics available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012997

Gupta, R./ Iyengar, R./ Sharma, M./ Cannuscio, C. C./ Merchant, R. M./ Asch, D. A./ Mitra, N./ Grande, D., Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information, Jama Network Open, 2023, 1-13, DOI: 10.1001/jamanetworkopen.2023.1305

Habib, H./ Zou, Y./ Yao, Y./ Acquisti, A./ Faith Cranor, L./ Reidenberg, J. R./ Sadeh, N./ Schaub, F., Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts, CHI Conference on Human Factors in Computing Systems (CHI), 2021, 1-15, https://doi.org/10.1145/3411764.3445387

Harborth, D./ Cai, X./ Pape, S., Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym, in: Dhillon, G./ Karlsson, F./ Hedström, K./ Zuquete, A. (eds.), ICT Systems Security and Privacy Protection, 2019, 253-267, https://doi.org/10.1007/978-3-030-22312-0_18

Hartge, D./ Herbort, N., Der beste Weg im aufsichtsbehördlichen Verfahren?, Datenschutzberater 2020, 184-186

Helberger, N./ Lynskey, O./ Micklitz, H.-W./ Rott, P./Sax, M./ Strycharz, J., EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets - A joint report from research conducted under the EUCP 2.0 project, March 2021, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

Herbort, N./ Reinhardt, M., Vom Suchen und Finden der federführenden Aufsichtsbehörde (frei nach WP 244), Privacy in Germany (PinG), 2019, 28-29

Hercher, J., The Royal Rumble Is On For Who Wins Contextual Advertising, AdExchanger, 13.2.2023, https://www.adexchanger.com/online-advertising/the-royal-rumble-is-on-for-who-wins-contextual-advertising/

Hofmann, F./ Raue, B. (eds.), Digital Services Act, Article-by-Article Commentary, 1st Edition 2023

Hoffmann-Riem, W. / Fritzsche, S., Innovationsverantwortung – Zur Einleitung, in: Eifert/ Hoffmann-Riem (ed.), Innovationsverantwortung, 2009, 11-41

Hoofnagle, C. J./ van der Sloot, B./ Zuiderveen Borgesius, F., The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 2019, 65-98, DOI: 10.1080/13600834.2019.1573501

IAB Inc, Legal Issues and Business Considerations - When Using Generative AI in Digital Advertising, June 2024, https://www.iab.com/wp-content/uploads/2024/06/IAB_GenerativeAI_WhitePaper_June2024.pdf

Information Commissioner's Office (ICO), Update report into adtech and real time bidding, 20.6.2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

Incorporated Society of British Advertisers (ISBA), Programmatic Supply Chain Transparency - Study, May 2020, https://www.isba.org.uk/system/files?file=media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf

Irish Council for Civil Liberties (ICCL), The Biggest Data Breach - ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe, 16.5.2022, https://www.iccl.ie/news/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

Iversen, T./ Rehm, P., Big Data and the Welfare State: How the Information Revolution Threatens Social Solidarity, 2022, https://doi.org/10.1017/9781009151405

Iwańska, K., To track or not to track?, Towards privacy-friendly and sustainable online advertising, Panoptykon Foundation, November 2020, https://panoptykon.org/sites/default/files/publikacje/panoptykon_to_track_or_not_to_track_final.pdf

Jaeckel, L., Gefahrenabwehrrecht und Risikodogmatik – Moderne Technologien im Spiegel des Verwaltungsrechts, 2010

Jaursch, J., What DSA codes of conduct for online advertising can achieve Opportunities and limitations of voluntary action and the need to move beyond it, Interface Policy Brief, 16.12.2024, https://www.interface-eu.org/publications/dsa-advertising-codes

Jha, N./ Trevisan, M./ Leonardi, E./ Mellia, M., On the Robustness of Topics API to a Re-Identification Attack, Proceedings on Privacy Enhancing Technologies (PoPETs), 2023, 66-78, https://doi.org/10.56553/popets-2023-0098

Kaput, M., AI in Advertising: Everything You Need to Know, Marketing Artificial Intelligence Institute, 22.1.2024, https://www.marketingaiinstitute.com/blog/ai-in-advertising

Karaj, A./ Macbeth, S./ Berson, R./ Pujol, J. M., WhoTracks.Me: Shedding light on the opaque world of online tracking, Computers and Society, 25.4.2019, https://arxiv.org/pdf/1804.08959

Keegan, J./ Eastwood, J., From “Heavy Purchasers” of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You, The Markup, 8.6.2023, https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you

Kerber, W./ Specht-Riemenschneider, L., Synergies between data protection law and competition law, Study prepared for the Verbraucherzentrale Bundesverband e.V., 30.9.2021, https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf

Kitkowska, A./ Warner, M./ Shulman, Y./ Wästlund, E./ Martucci, L. A., Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect, Sixteenth Symposium on Usable Privacy and Security (SOUPS) 2020, 437-456, https://www.usenix.org/system/files/soups2020-kitkowska.pdf

Klosowski, T., How to turn off google’s privacy sandbox ad tracking – and why you should, Electronic Frontier Foundation, 28.9.2023, https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should

Kobie, N., Germany Says GDPR Could Collapse as Ireland Dallies on Big Fines, Wired UK, 27.4.2020, https://www.wired.com/story/gdpr-fines-google-facebook/

Kočišová, L./ Štarchoň, P., The role of marketing metrics in social media: A comprehensive analysis, Marketing Science & Inspirations, 2023, 40-49, DOI: 10.46286/msi.2023.18.2.4

Kopp, K., Is So-Called Contextual Advertising the Cure to Surveillance-Based “Behavioral” Advertising?, Tech Policy, 26.9.2023, https://www.techpolicy.press/is-so-called-contextual-advertising-the-cure-to-surveillance-based-behavioral-advertising/

Kozyreva A./ Lorenz-Spreen, P./ Hertwig, R./ Lewandowsky S./ Herzog S., Public Attitudes towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States, Humanities and Social Sciences Communications 8/2021, 1-12, https://doi.org/10.1057/s41599-021-00787-w

Kulyk, O./ Gerber, N./ Hilt, A./ Volkamer, M., Has the GDPR hype affected users' reaction to cookie disclaimers?, Journal of Cybersecurity, 1/2020, 1-15, https://doi.org/10.1093/cybsec/tyaa022

Kroschwald, S., Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften - Schutz, Selbstbestimmung und Teilhabe „by Design" vor dem Hintergrund des Art. 25 DSGVO und dem KI-Verordnungsentwurf, Zeitschrift für Digitalisierung und Recht (ZfDR), 2023, 1-22

Lancieri, F., Narrowing Data Protection's Enforcement Gap, Maine Law Review (MLR), 2022, 15-72, http://dx.doi.org/10.2139/ssrn.3806880

Levie, J./ Autio, E., Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, Journal of Management Studies, 2011, 1392–1419, DOI: 10.1111/j.1467-6486.2010.01006.x

Libonati, C./ Fernandez, M., The Digital Advertising Revolution: How Artificial Intelligence Is Changing the Game, Globant, 19.10.2023. https://stayrelevant.globant.com/en/technology/create/ai-is-changing-the-digital-advertising-landscape/

Lomas, N., Microsoft-owned adtech Xandr accused of EU privacy breaches, Tech Crunch, 8.7.2024, https://techcrunch.com/2024/07/08/microsoft-owned-adtech-xandr-accused-of-eu-privacy-breaches/

Lynskey, O., The foundations of EU data protection law, 2015

Margaritis, E., Online Behavioral Advertising as an Aggressive Commercial Practice - Targeting Consumers' Vulnerabilities as a Form of Undue Influence, Journal of European Consumer and Market Law (EuCML), 2023, 243-251

Martini, M., Integrierte Regelungsansätze im Immissionsschutzrecht: eine Untersuchung zu dem integrierten Ansatz der UVP-RL, der IVU-RL und der Öko-Audit-Verordnung sowie ihrer deutschen Umsetzungsgesetze, 2000

Masing, J., Herausforderungen des Datenschutzes, Neue Juristische Wochenschrift (NJW), 2012, 2305–2311

Mayer, T., Manipulierte Bilder, falsche Nachrichten: Wie es betrügerische Werbeanzeigen immer wieder in Online-Medien schaffen, Tagesspiegel, 21.3.2023, https://www.tagesspiegel.de/gesellschaft/medien/manipulierte-bilder-falsche-nachrichten-wie-es-betrugerische-werbeanzeigen-immer-wieder-in-online-medien-schaffen-9518303.html

McDonald, A. M./ Reeder, R. W./ Gage Kelley, P./ Cranor, L., A Comparative Study of Online Privacy Policies and Formats, Privacy Enhancing Technologies (PETs) 2009, 37-55, DOI: 10.1007/978-3-642-03168-7_3

Meyer, M., Warum seriöse Websites Werbung von Fake-Shops schalten, Deutschlandfunk, 11.4.2023, https://www.deutschlandfunk.de/online-werbung-fake-shop-100.html

McCann, D./ Stronge, W./ Jones, P., The future of Online Advertising, October 2021, https://extranet.greens-efa.eu/public/media/file/1/7267

McDonald A. M./ Cranor L., The Cost of Reading Privacy Policies, A Journal of Law and Policy for the Information Society, 2008, 543-568

McKay, C., Big Brands Experiment with Generative AI for Advertising, Maginative, 18.8.2023, https://www.maginative.com/article/big-brands-experiment-with-generative-ai-for-advertising/

Moerel, L./ Prins, C., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, Social Science Research Network (SSRN), 2016, 1-98, http://dx.doi.org/10.2139/ssrn.2784123

Müller-Tribbensee, T., Privacy Promise Vs. Tracking Reality in Pay-or-Tracking Walls, in: Jensen, M. et al. (eds.), Privacy Technologies and Policy, 12th Annual Privacy Forum (APF) 2024, 168-188, https://doi.org/10.1007/978-3-031-68024-3_9

Muttach, J.-P./ Köppel, M./Hornung, G., Google Topics als Ausweg aus dem Cookie-DIlemma?, Computer und Recht (CR), 2023, 644-655

Nissenbaum, H., Respect for Context as a Benchmark, in: Roessler, B. and Mokrosinska, D. (eds.), Social Dimensions of Privacy – Interdisciplinary Perspectives, 2015, 278-302

Ohly, A., »Volenti non fit iniuria« - Die Einwilligung im Privatrecht, 2002

Pfeiffer, L./ Muttach, J.-P., EU-Kommission: Initiative zur freiwilligen Cookie-Selbstverpflichtung, ZD-Aktuell 2024, 01520

Pins, D./ Jakobi, T./ Stevens, G./ Alizadeh, F./ Krüger, J., Finding, getting and understanding: the user journey for the GDPR'S right to access, Behaviour & Information Technology, 2022, 2174–2200, https://doi.org/10.1080/0144929X.2022.2074894

Podszun, R. (ed.), Digital Markets Act, Article-by-Article Commentary, 1st Edition 2024

Pohle, J., Datenschutz und Technikgestaltung - Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, 2016, https://edoc.hu-berlin.de/server/api/core/bitstreams/a6548e82-6668-48b5-b149-2133cdbe74c0/content

Rescorla, E./ Thomson, M., Technical Comments on FLoC Privacy, 10.6.2021, https://mozilla.github.io/ppa-docs/floc_report.pdf

Rupp, V./ Grafenstein v., M., Clarifying “personal data” and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection, Computer Law & Security Review, 2024, 1-25, DOI: 10.1016/j.clsr.2023.105932

Rützel F., Rechtsfragen algorithmischer Preisdiskriminierung: eine rechtsgebietsübergreifende Untersuchung, 2023

Ryan, J./ Toner, A., Europe’s governments are failing the GDPR - Brave’s 2020 report on the enforcement capacity of data protection authorities, April 2020, https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf

Ryan, J., Report - Behavioural advertising and personal data, September 2018, https://brave.com/static-assets/files/Behavioural-advertising-and-personal-data.pdf

Satariano, A., Europe’s Privacy Law Hasn’t Shown Its Teeth, Frustrating Advocates, New York Times, 27.4.2020, https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

Schaub F./ Balebako, R./ Cranor, L., Designing Effective Privacy Notices and Controls, IEEE Internet Computing, 2017, 70-77, DOI: 10.1109/MIC.2017.75

Scheppe, M., Wie KI das Marketing für Unternehmen revolutioniert, Handelsblatt, 2.1.2024, https://www.handelsblatt.com/tech-nik/gadgets/kuenstliche-intelligenz-wie-ki-die-werbung-fuer-unternehmen-revolutioniert/100002285.html

Schiff, A., When Does Contextual Targeting Cross The Line Into Something … Else?, AdExchanger, 28.8.2023, https://www.adexchanger.com/data-privacy-roundup/when-does-contextual-targeting-cross-the-line-into-something-else/

Schräer, F., Google und Aufsichtsbehörden ignorieren Kritik an Cookie-Ersatz Topics, Heise Online, 19.1.2023, https://www.heise.de/news/Google-und-Aufsichtsbehoerden-ignorieren-Kritik-an-Cookie-Ersatz-Topics-7463442.html

Scott, M., Cambridge Analytica did work for Brexit groups, says ex-staffer, Politico, 30.7.2019, https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/

Selzer, A., Die Zukunft der ePrivacy-Verordnung - Das große schwarze Loch im Datenschutzrecht, Datenschutz und Datensicherheit (DuD), 2024, 463-464

Simitis/ Hornung/ Spiecker gen. Döhmann (eds.), Datenschutzrecht, DSGVO and BDSG, Article-by-Article Commentary, 2nd Edition 2024

Skatova, A./ McDonald, R./ Ma, S./ Maple, C., Unpacking privacy: Valuation of personal data protection, PLoS ONE, 18(5) 2023, 1-21, https://doi.org/10.1371/journal.pone.0284581

Smieskol P./ Jakobi T./ v. Grafenstein, M. (submitted at CLSR), From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. Computer Law and Security Review, pre-print available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5021149

Strycharz, J./ Duivenvoorde, B., The exploitation of vulnerability through personalised marketing communication: are consumers protected?, Internet Policy Review (IPR) 4/2021, 1-27

Sydow, G./ Marsch, N., DS-GVO / BDSG, Article-by-Article Commentary, 3rd Edition 2022

Thiel, B., Zusammenarbeit der Datenschutzaufsicht auf europäischer Ebene - Eine erste Bilanz zu Kooperations- und Kohärenzverfahren, Zeitschrift für Datenschutz (ZD) 2021, 467-470

Tiwari, U., Privacy-Preserving Attribution: Testing for a New Era of Privacy in Digital Advertising, Mozilla Blog, 22.8.2024, https://blog.mozilla.org/netpolicy/2024/08/22/ppa-update/

Thode, W./ Griesbaum, J./ Mandl, T., “I Would Have Never Allowed It”: User Perception of Third-Party Tracking and Implications for Display Advertising, in: Pehar, F./ Schlögl, C./ Wolff, C. (eds.), Re:inventing Information Science in the Networked Society, 2015

Thomson, M., A Privacy Analysis of Google’s Topics Proposal, 6.1.2023, https://mozilla.github.io/ppa-docs/topics.pdf

Trevisan M./ Traverso, S./ Bassi, E./ Mellia, M., 4 Years of EU Cookie Law: Results and Lessons Learned, Proceedings on Privacy Enhancing Technologies (PoPETs), 2019, 126-145, DOI:10.2478/popets-2019-0023

Vanian, J., How the Generative A.I. Boom Could Forever Change Online Advertising, CNBC, 8.7.2023, https://www.cnbc.com/2023/07/08/how-the-generative-ai-boom-could-forever-change-online-advertising.html

Veale, M./ Zuiderveen Borgesius, F., Adtech and Real-Time Bidding under European Data Protection Law, German Law Journal, March 2022, 226-256, https://doi.org/10.1017/glj.2022.18

Viktoratos, I./ Tsadiras, A., Personalized Advertising Computational Techniques: A Systematic Literature Review, Findings, and a Design Framework, Information 2021 12(11) 480, 1-38, https://doi.org/10.3390/info12110480

Vigliarolo, B., Turns out AI chatbots are way more persuasive than humans, The Register, 3.4.2024, https://www.theregister.com/2024/04/03/ai_chatbots_persuasive

Vinocur, N., One Country Blocks the World on Data Privacy, Politico, 24.4.2019, https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/

Voßkuhle, A./ Eifert, M./ Möllers, C. (eds.), Grundlagen des Verwaltungsrechts, Companion, 3rd Edition 2022

Wagner, B./ Ruhmann, M., Irland: Das One-Stop-Shop-Verfahren, ZD-Aktuell 2019, 06546

Wang, J./ Zhang, W./ Yuan, S., Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting, Foundations and Trends in Information Retrieval (FTIR) 2017, 297-435, http://dx.doi.org/10.1561/1500000049

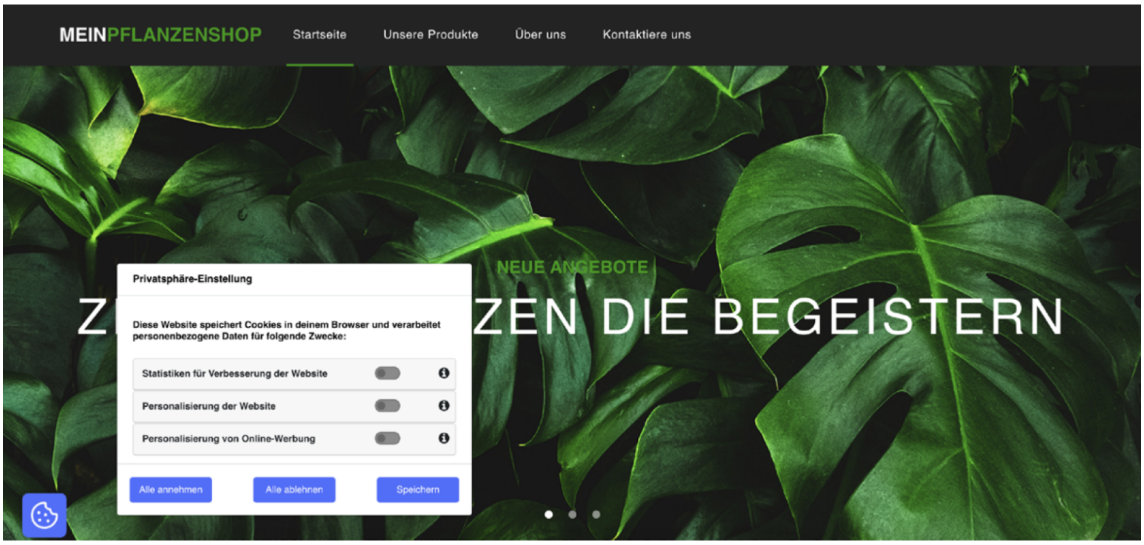
Wegner, G., Nachhaltige Innovationsoffenheit dynamischer Märkte, in: Eifert/ Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 2009, 71–91

Wolford, B., Google’s Privacy Sandbox is privacy quicksand, Proton Blog, 30.11.2023, https://proton.me/blog/google-privacy-sandbox

Yao, Y./ Re, D. L./ Wang, Y., Folk Models of Online Behavioral Advertising, Proceedings of the 2017 ACM Conference, 2017, 1-13, https://doi.org/10.1145/2998181.2998316

ANNEXES

Annex 1: Cookie banner used in a quantitative study to test the effectiveness (in the meaning of Art. 25 sect. 1 GDPR) of cookie banners that are designed according to current best practice rules



Privatsphäre-Einstellung

Diese Website speichert Cookies in deinem Browser und verarbeitet personenbezogene Daten für folgende Zwecke:

- Statistiken für Verbesserung der Website ○
- Personalisierung der Website ○
- Personalisierung von Online-Werbung ○

Annex 2

Table of particularly noteworthy cases that have been conducted by European data protection supervisory authorities under the **GDPR** (sorted by year):

Country / Supervisory Authority	**Subject Matter / Type of Violation**	**Measure taken / Amount of fine**	**Addressee**
Luxembourg/ CNPD/ 2021	Not known[463]	Fine / 746 Mio Euro[464] (GDPR - OSS)	Amazon Europe
Norway/ Datatilsynet/ 2021[465]	Transfer of personal data to third parties for advertising purposes without effective consent.	Fine / 65 Mio NOK (~ 6 Mio Euro) (GDPR - OSS)	Grindr
Italy / Garante / 2021[466]	Protection of minors, age verification	Limitation on processing (GDPR - no OSS)	TikTok
Ireland/ DPC/ 2022[467]	Processing of personal data of children on Instagram	Fine / 405 Mio. Euro (GDPR - OSS)	Meta
Belgium/ APD/ 2022[468]	Use of unnecessary cookies without prior consent, use of pre-ticked boxes for consent, insufficient information in the privacy policy, no option for withdrawal	Fine / 50.000 Euro (GDPR - no OSS)	Roularta Media Group
Spain/ AEPD/ 2022 and 2023	- Processing of personal data and profiling of data subjects below the age of 14[469]	Fine / 8.000 Euro / 15.000 Euro (reduced to	Div.

[463] Due to national legal requirements, the CNPD is not allowed to comment on the content, https://cnpd.public.lu/de/actualites/international/2021/08/decision-amazon-2.html.

[464] The amount was disclosed in Amazon's second quarterly report for 2021, Part I Item 1 Note 4, https://s2.q4cdn.com/299287126/files/doc_financials/2021/q2/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf.

[465] Datatilsynet, 13.12.2021, 20/02136–18, https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf.

[466] Garante per la protezione dei dati personali, 22.1.2021, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9524194, see also EDPB,press release, 26.1.2021, https://www.edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en.

[467] DPC, press release, 15.9.2022, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry.

[468] APD, 25.5.2022, DOS-2020–03432, www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-85-2022.pdf.

[469] AEPD, 13.4.2022, PS/00483/2021 - Ramona Films.

	- Data processing without a legal basis and missing cookie policy [470] - Violation of the duty to provide information and use of dark patterns[471]	9.000 Euro) / 12.000 Euro (GDPR - no OSS)	
France/ CNIL/ 2023[472]	Inter alia company had not checked whether the people whose data it processed had given their consent.	Fine / 40 Mio Euro (GDPR - OSS)	Criteo
Ireland/ DPC/ 2023[473]	Lack of transparency regarding personalised services, including personalised advertising on Facebook and Instagram; insufficient legal basis (contract).	Fine / 210 + 180 Mio. Euro (GDPR - OSS) (GDPR - OSS)	Meta
Ireland/ DPC/ 2023[474]	Platform settings and age verification.	Fine / 345 Mio. Euro (GDPR - OSS)	TikTok
Sweden/ IMY/ 2024[475]	Use of Meta Pixel to measure the effectiveness of the bank's Facebook advertising without consent; activation by mistake led to transfer of personal data of up to 1 million people to Meta.	Fine / 15 Mio SEK (~ 1,3 Mio Euro)	Avanza Bank AB
Netherlands/ AP/ 2024[476]	Setting of cookies before consent was given, "accept all" button selected by default, four clicks necessary to reject cookies	Fine / 600.000 Euro (GDPR - no OSS)	A.S. Watson (Kruidvat.nl)
Ireland/ DPC/ 2024[477]	Processing of personal data for the purposes of behavioural analysis and targeted advertising of LinkedIn-members	Fine / 310 Mio. Euro (GDPR - OSS)	LinkedIn

[470] AEPD, 18.4.2022, PS/00482/2021 - Jimbo Networks.

[471] AEDP, 23.9.2023, PS/00080/2023 - Chatwith.IO.

[472] CNIL, 15.6.2023, SAN-2023-009, www.cnil.fr/fr/publicite-personnalisee-criteo-sanctionne-dune-amende-de-40-millions-deuros.

[473] DPC, press release, 4.1.2023, https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

[474] DPC, press release, 15.9.2023, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.

[475] IMY, 24.6.2024, DI-2021-5544, https://www.imy.se/nyheter/sanktionsavgift-mot-avanza-for-overforing-av-personuppgifter-till-meta/.

[476] AP, 2.5.2024, z-2021-14274 - A.S. Watson, https://autoriteitpersoonsgegevens.nl/system/files?file=2024-07/Besluit%20boete%20A.S.%20Watson%20-%20Kruidvat.pdf.

[477] DPC, press release, 24.10.2024, https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million.

Table of particularly noteworthy cases that have been conducted by supervisory authorities under the – national implementation of the – **ePrivacy Directive** (sorted by year):

Country / DPA	**Subject Matter / Type of Violation**	**Measure taken / Amount of fine**	**Addressee**
France/ CNIL/ 2020 [478]	Cookie banner without the option to reject at the first level.	Fine / 40 Mio + 60 Mio Euro	Google
France/ CNIL/ 2020[479]	Setting of advertising cookies without prior consent; no satisfactory information.	Fine / 35 Mio Euro	Amazon
France/ CNIL/ 2020[480]	Setting of advertising cookies withour prior consent.	Fine / 2,25 Mio Euro	Carrefour
France/ CNIL/ 2020[481]	Setting of advertising cookies withour prior consent.	Fine / 800.000 Euro	Carrefour Banque
France/ CNIL/ 2021[482]	Refusing advertising cookies was more difficult than accepting them.	Fine / 90 Mio + 60 Mio Euro	Google (YouTube)
France / CNIL/ 2021[483]	Use of cookies without effective user consent; no equivalent opt-out button.	Fine / 60 Mio Euro	Facebook
Italy/ Garante/ 2022[484]	Proposed change to Tiktoks privacy policy regarding the legal basis for digital advertising.	Warning	TikTok Technology Limited

[478] CNIL, 7.12.2020, SAN-2020–012, www.cnil.fr/sites/default/files/atoms/files/deliberation_of_restricted_committee_san-2020-012_of_7_december_2020_concerning_google_llc_and_google_ireland_limited.pdf.

[479] CNIL, 7.12.2020, SAN-2020–013, www.cnil.fr/sites/default/files/atoms/files/deliberation_of_restricted_committee_san-2020-013_of_7_december_2020_concerning_amazon_europe_core.pdf; the decision was confirmed by the Administrative court, Conseil d'E' tat, 27.6.2022 – Nr. 451423, www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-06-27/451423.

[480] CNIL, 18.11.2020, SAN-2020–008, www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756.

[481] CNIL, 18.11.2020, SAN-2020–009, www.legifrance.gouv.fr/cnil/id/CNILTEXT000042564657.

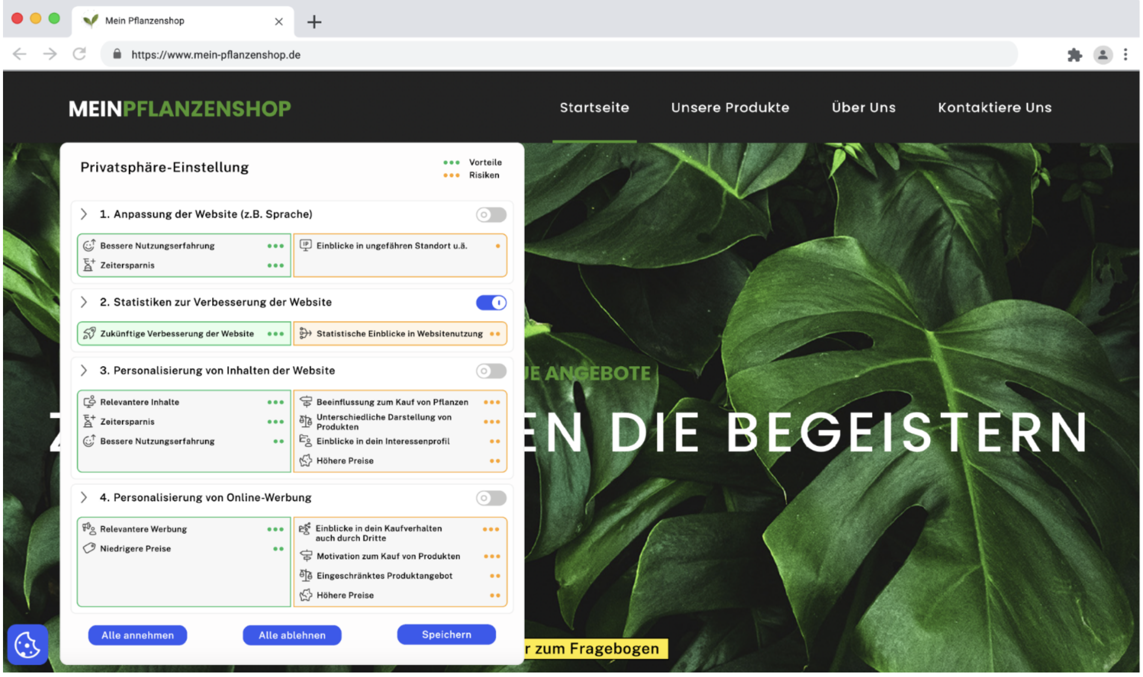
[482] CNIL, 31.12.2021, SAN-2021–023, www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf.

[483] CNIL, 31.12.2021, SAN-2021-024, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532.

[484] Garante, 7.11.2022, no. 9788429, www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9788429; Garante, press release, 11.7.2022, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9788342#english.

Spain/ AEPD/ 2019[485]	Pre-checked consent boxes that enabled non-essential cookies; use of non-essential cookies even after users clicked "reject all".	Fine / 18.000 Euro	Vueling

Annex 3:



Mein Pflanzenshop
https://www.mein-pflanzenshop.de

MEINPFLANZENSHOP
Startseite | Unsere Produkte | Über Uns | Kontaktiere Uns

Privatsphäre-Einstellung
●●● Vorteile
●●● Risiken

1. Anpassung der Website (z.B. Sprache) ○
- Bessere Nutzungserfahrung ●●●
- Zeitersparnis ●●●
- Einblicke in ungefähren Standort u.ä. ●

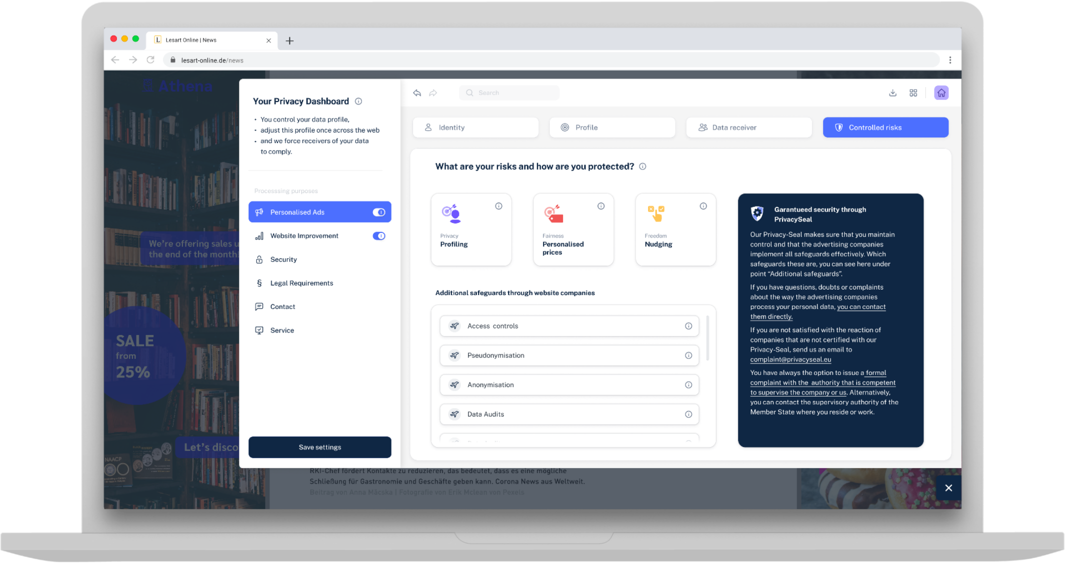
2. Statistiken zur Verbesserung der Website ●
- Zukünftige Verbesserung der Website ●●●
- Statistische Einblicke in Websitenutzung ●●

3. Personalisierung von Inhalten der Website ○
- Relevantere Inhalte ●●●
- Zeitersparnis ●●●
- Bessere Nutzungserfahrung ●●
- Beeinflussung zum Kauf von Pflanzen ●●●
- Unterschiedliche Darstellung von Produkten ●●●
- Einblicke in dein Interessenprofil ●●
- Höhere Preise ●●

4. Personalisierung von Online-Werbung ○
- Relevantere Werbung ●●●
- Niedrigere Preise ●●
- Einblicke in dein Kaufverhalten auch durch Dritte ●●●
- Motivation zum Kauf von Produkten ●●●
- Eingeschränktes Produktangebot ●●
- Höhere Preise ●●

Alle annehmen | Alle ablehnen | Speichern

Annex 4:



Lesart Online | News
lesart-online.de/news

Your Privacy Dashboard
- You control your data profile,
- adjust this profile once across the web
- and we force receivers of your data to comply.

Processsing purposes
- Personalised Ads ●
- Website Improvement ●
- Security
- Legal Requirements
- Contact
- Service

Save settings

Identity | Profile | Data receiver | Controlled risks

What are your risks and how are you protected?

Privacy: Profiling
Fairness: Personalised prices
Freedom: Nudging

Additional safeguards through website companies
- Access controls
- Pseudonymisation
- Anonymisation
- Data Audits

Garantueed security through PrivacySeal

Our Privacy-Seal makes sure that you maintain control and that the advertising companies implement all safeguards effectively. Which safeguards these are, you can see here under point "Additional safeguards".

If you have questions, doubts or complaints about the way the advertising companies process your personal data, you can contact them directly.

If you are not satisfied with the reaction of companies that are not certified with our Privacy-Seal, send us an email to complaint@privacyseal.eu

You have always the option to issue a formal complaint with the authority that is competent to supervise the company or us. Alternatively, you can contact the supervisory authority of the Member State where you reside or work.

Athena
We're offering sales u the end of the month!
SALE from 25%
Let's disco
RKI-Chef fordert Kontakte zu reduzieren, das bedeutet, dass es eine mögliche Schließung für Gastronomie und Geschäfte geben kann. Corona News aus Weltweit.
Beitrag von Anna Mäcska | Fotografie von Erik Mclean von Pexels
Search

[485] AEPD, 6.10.2019, EXP202103886 - Vueling, https://www.aepd.es/documento/ps-00032-2022.pdf