Background paper

23 October 2025

Background paper on tracking and data processing in the digital economy

Executive Summary

This document serves to provide factual information about tracking and data processing in the digital economy and is intended to place the political debate surrounding the planned Digital Fairness Act on a fact-based foundation.

The aim is to correct technical misconceptions, explain the actual technical processes and clarify the role of tracking as a central infrastructure for user-oriented digital offerings, media diversity and economic competitiveness. Tracking is not an end in itself, but an essential tool for the security, financing, optimisation and personalisation of digital services and offerings.

By tracking, we mean the data-driven collection and analysis of usage information to make digital offerings more relevant, secure and efficient for consumers. Among other things, it enables the measurement of reach and advertising impact, fraud prevention, improvement of the user experience and the delivery of context- or interest-based content. Personalisation is now the norm for users – not the exception.

The digital economy is a highly networked ecosystem of digital services, publishers, advertisers, technology providers and intermediaries. The open, interoperable internet in particular relies on efficient, data-driven advertising and measurement mechanisms to ensure diversity, innovation and European competitiveness. Technical standards such as the Transparency & Consent Framework already ensure data protection and user control.

The political debate is currently often dominated by concerns about manipulative or unethical practices. This document makes it clear that there are no technological processes for continuous emotion analysis in everyday advertising, nor are individual vulnerabilities specifically exploited. Profiling in particularly sensitive areas is already prohibited by existing law (in particular the GDPR and DSA) and is not practised by the industry.

Against this background, we advocate a focus on clear definitions of terms, consistent enforcement of existing rules and the preservation of innovation-friendly framework conditions. A Digital Fairness Act can only be effective and proportionate if it avoids double regulation, takes technical realities into account and ensures a competitive, open internet in Europe.

Contact

Daphne van Doorn | Head of EU Affairs | vanDoorn@bvdw.org

Philipp Hagen | Director Legal Affairs & Data Privacy | Hagen@bvdw.org

Background paper

1. Table of contents

Background paper

Background paper

1. What is the purpose of this document?

This document serves to provide technical information about the methods and purposes of tracking and data processing in the digital economy. It is intended to contribute to an objective assessment of the political debate surrounding the planned Digital Fairness Act, particularly with regard to the function and necessity of data-based business models in the field of online advertising and content personalisation.

The aim is to create a sound factual basis on which opportunities, risks and possible regulatory approaches can be objectively assessed. Especially in an environment where discussions are often conducted in a simplified manner, we want to create transparency about technical processes, economic contexts and existing protection mechanisms.

The document is aimed at decision-makers in policy and public authorities, experts, political stakeholders and other interested stakeholders who want a deeper understanding of the technical fundamentals in order to be able to conduct a differentiated and fact-based debate.

2. About the digital economy

The digital economy is a key driver of innovation, value creation and competitiveness in Germany and Europe. It encompasses not only platforms and technology providers, but also a broadly networked ecosystem of media companies, digital services, advertisers, agencies, start-ups, and data and infrastructure providers. Digital offerings and data-based business models are no longer just part of individual industries, but are shaping the structure of almost all sectors of the economy, from retail and mobility to education, culture and health.

Digital advertising is a crucial part of this ecosystem. It enables companies to reach users in a targeted manner and finance business models (especially on the open internet). Tracking and data-based analysis methods are primarily used to improve digital offerings, better understand user interests, make advertising performance measurable and prevent fraud. They form the basis for personalised offerings and thus for users' current expectations of receiving relevant and inspiring content.

A distinction must be made between the open and closed web. In the open web, advertising is traded using standards, with a high degree of transparency and competition from a large number of independent publishers and technology providers. In the closed web ("walled gardens"), large platforms bundle data, advertising inventory and playback entirely within a proprietary system. While closed ecosystems offer high reach and can coordinate within their system, the open web is also essential for economic diversity, innovation and the independence of European companies.

Today's digital economy is highly organised around the division of labour. Intermediaries such as SSPs (supply-side platforms), DSPs (demand-side platforms), ad exchanges and consent management platforms take on specialised roles to efficiently market advertising space, implement legal requirements and strengthen competition. This technological infrastructure enables European companies to access regional or global markets, regardless of whether they themselves have significant platform power.

BVDW's goal is to promote innovation-friendly and responsible regulation that builds trust while ensuring the competitiveness of European companies. This includes better enforcement of existing legal frameworks instead of creating new hurdles, and enabling the opportunities for data-driven value creation, such as through personalisation or new technological developments, in the interests of the economy, consumers, politics and society.

3. What do we mean by "tracking"?

In the digital economy, tracking refers to the systematic collection, aggregation and processing of data about user behaviour on the internet. In addition to advertising, tracking is also used in the personalisation of content and services (recommender systems such as those found on e-commerce sites, streaming sites, news sites, etc.).

We understand tracking to be the data-supported collection and processing of usage information across digital offerings in order to better understand the behaviour, interests and interactions of users. This includes information about page views, interaction histories, devices used or repeat visits. Tracking does not automatically mean the creation of personal profiles, but encompasses various technical processes ranging from reach and performance measurement to session analyses and pseudonymised or aggregated usage data.

Tracking is primarily used to make digital offerings more user-friendly, secure and relevant. It enables the optimisation of the user experience and the measurement of campaign effectiveness in advertising. It also helps with fraud prevention and the delivery of context- or interest-based content and advertising. The aim is to provide users with information that is as accurate and helpful as possible, while enabling companies to operate digital business models in an economical and competitive manner.

4. Players in the digital economy

a. Players in the context of advertising

- *Advertisers*

Advertisers include all companies and organisations that want to promote their products, brands or services digitally. This includes both international corporations and small and medium-sized enterprises, as well as innovative start-ups. Their goal is to efficiently address the right target groups, increase brand awareness and build long-term customer relationships. The focus is on making the best possible use of marketing budgets, minimising wastage and targeting advertising measures so that they reach the right target group at the right time.

- *Publishers*

Publishers are providers of digital content and services, including news sites, social networks, video platforms, mobile apps, and smaller specialised sites and blogs. Their primary role in the advertising ecosystem is to provide content that attracts users. Publishers thus provide the necessary reach and attractive environments that advertisers need for their advertising campaigns.

- *Intermediaries*

Intermediaries include a variety of service providers, platforms and technology providers that act as intermediaries between advertisers and publishers in the digital advertising market. These include advertising agencies, demand-side platforms (DSPs), supply-side platforms (SSPs), ad exchanges, and specialised providers of data management platforms (DMPs), consumer data platforms (CDPs), and consent management solutions. Further and supplementary material on this topic is available on request.

- DSPs (demand-side platforms) enable advertisers to purchase advertising space automatically and run campaigns based on defined target group and campaign criteria.
- SSPs (supply-side platforms) bundle publishers' inventory, optimise delivery and make it available for automated trading.
- Ad exchanges connect supply and demand in real time and enable programmatic trading.
- Ad networks bundle advertising space from smaller publishers and sell it in bundles to advertisers or DSPs.
- Ad servers deliver ads technically, count impressions, clicks and other metrics, and support campaign management and reporting.
- Measurement & analytics providers create campaign analyses and attribution models to make advertising performance measurable and enable optimisation.

- DMPs/CDPs process and segment data so that targeting, personalisation and campaign management can be carried out in compliance with data protection regulations. Centralised and decentralised data clean rooms are environments that can be used as tools for this purpose to match data in compliance with data protection regulations.
- CMPs (consent management platforms) ensure compliance with user consent and data protection requirements.
- Ad verification/brand safety providers monitor the correct display of advertising in brand-safe environments and prevent fraud or problematic placements.
- Content recommendation/personalisation engines ensure that content and advertising are personalised based on user interests in order to increase relevance and user satisfaction.

The central function of intermediaries is efficient, data-based mediation between supply (publishers) and demand (advertisers). They ensure that digital advertising can be handled automatically and scalably. One of the key advantages is that advertisers can identify and book the right advertising spaces within a few milliseconds, while publishers can monetise their inventory optimally.

Data plays an essential role in this: intermediaries need data sets to ensure that ads are played at the right time, in the right context and to the right target groups. They also enable precise measurement of success and thus contribute significantly to the transparency and optimisation of digital advertising processes.

- *Cross-platform ecosystems*

Large platforms offer advertising space, user data and targeting within closed systems. They enable greater reach and data-based campaign management, but are less interoperable than the open web.

- *Potential customers/consumers*

Today's consumers increasingly expect personalised offers that are tailored to their individual interests as much as possible, while at the same time seeking inspiration in their digital interactions. Personalised content, offers, services and advertising are now perceived as "normal". The BVDW, in collaboration with Kantar Media, has also published a recent study in which consumers were surveyed about personalisation in the digital world. This trend is further reinforced by generative AI. Meeting these changing expectations is therefore crucial for European companies to remain competitive and sustainable.

b. Actors in the context of content personalisation

These include, in particular, digital platforms, digital companies and services that personalise content or functions, such as streaming and video platforms, music and audio platforms, e-commerce platforms and companies, news, weather and information platforms, social networks and community platforms, navigation and mobility services, learning platforms and educational services, and mobile apps and digital services.

These players use tracking to evaluate user behaviour and, based on this, offer personalised recommendations, content, interface adjustments or notifications. The aim is to increase relevance and user loyalty through tailor-made service offerings, content or functions.

5. List of tracking and personalisation methods

Below, we provide an overview of the most important tracking and personalisation methods used in today's digital economy. These range from classic cookies to modern privacy APIs. Each technology has specific functions, strengths and weaknesses. This list is not exhaustive, as it is continuously being developed.

- *Cookie tracking*

HTTP cookies are small text files that are stored in the browser by the provider when required. However, they are not automatically set on every website. Cookies are only used when certain functions require them, such as user identification, targeting, storage of privacy settings (including consents), conversion tracking (assigning sales to advertising clicks), measuring campaign success or fraud prevention. Cookies can also enable cross-site tracking. They are therefore both an optional and a purpose-specific tool.

First-party cookies

- When you visit a website, it can store a unique ID in your browser (first-party cookie). Each time you visit the site again, the ID is sent along with you so that you are recognised. This is used to personalise content, measure usage behaviour, and target advertising. Technically, this is achieved by the browser automatically sending the cookie information with every request to that specific domain.
- First-party cookies are set directly by the domain visited and are therefore particularly important for functions such as login, shopping basket, language settings or analysis of your own traffic.
- They primarily enable the tracking of user interactions within the same website and serve to optimise the user experience and the design of the website.

Third-party cookies

- Third-party cookies work in a similar way, but originate from external domains (e.g. an advertising network, analytics or social media provider).
- They enable cross-site tracking, as the same external domain can be integrated into many different websites. This allows users' activities and interests to be observed across multiple sites and used for advertising, reach measurement or profiling.
- Technically, this is achieved by reloading third-party content (e.g. advertising banners or tracking pixels) when the website is loaded, which in turn place a cookie in the browser. The browser then sends this cookie with every subsequent contact with this third-party domain.

- *Server-side tracking*

In this case, tracking actions are not reported directly to third-party servers by the user's browser; instead, the website operator forwards the data from its own server. For example, a pixel on the page can no longer make a call to an external ad server, but sends a request to its own server, which then informs the third-party provider on the server side. A white paper on this topic is available upon request.

- *IP addresses and geolocation*

Every internet connection has an IP address that allows conclusions to be drawn about the approximate location (country, city, provider). IP addresses are often recorded automatically and are used, for example, to adapt advertising content to specific regions (keyword: geotargeting) or to detect cases of fraud (suspicious foreign access). An IP address alone is not a perfect identifier, as it can change and may be assigned to multiple users, but it does provide important contextual data.

- *Tracking pixels and tags*

These are 1×1 pixel images or scripts that are embedded in web pages. When the page is loaded, this pixel is also loaded from the provider's server, allowing the provider to register a page view. Tracking pixels provide, for example, statistics on how often articles have been read (a well-known example is VG-Wort pixels for author remuneration) or whether an email has been opened. In

advertising, pixels and so-called tags are mainly used for measurement (view tracking of ads, counting ad impressions) and retargeting (a pixel on the order confirmation page can report to an advertising network that the user has become a customer).

- *Mobile advertising IDs*

In mobile apps, tracking is not done via browser cookies, but via dedicated advertising identifiers of the operating system. On Android devices, for example, there is the Google Advertising ID (GAID), and on Apple devices, the Identifier for Advertisers (IDFA). These IDs are unique to each device and can be read by apps (with the appropriate authorisation). They enable user recognition across different apps for advertising purposes. However, users can reset these IDs or restrict tracking. Mobile ad IDs (MAIDs) are used for cross-app frequency capping, attribution of app installations or cross-app profiles.

- *Fingerprinting (device fingerprint)*

Fingerprinting refers to the collection of device data in order to recognise a user even without cookies. This involves running scripts in the browser that read out characteristics such as screen resolution, installed fonts, browser version, operating system, language, time zone, activated plugins or even the properties of HTML5 canvas elements. These numerous data points are used to calculate a virtually unique fingerprint for the device. Studies show that 80–90% of browser fingerprints are unique. This means that most users can be identified individually. Banks, shops and e-commerce sites, for example, use these device fingerprints to detect suspicious logins or transactions (fraud prevention). In the age of AI, fraudulent attacks are on the rise and are increasingly automated, making it ever more important to keep pace with the technical advances of attackers. The use of AI for pattern recognition and fraud prevention is therefore becoming increasingly necessary.

- *Local Storage / IndexedDB:*

These are browser-internal storage techniques that can be persistent across websites. Local storage is useful for storing consent decisions or user preferences, for example.

- *Click tracking and URL parameters*

A simple but effective method is to append identifiers to URLs when the user clicks on a link. Examples include UTM parameters (utm_source, utm_campaign, etc.), which are used for analysis purposes. Large platforms such as Meta or Google sometimes append their own IDs to external links (e.g. fbclid, gclid) so that they can later identify which click led to which action. Click tracking is helpful for attribution (assigning advertising expenditure to results) and also works without cookies. In practice, URL parameters are primarily used for analysis and campaign purposes.

- *Authenticated user IDs (login tracking)*

Many digital platforms rely on their own login systems. When a user logs in, their behaviour can be directly linked to their account. The big advantage is that this tracking is possible across devices (since the same account is used on smartphones and laptops) and is very precise. Providers use the account ID to obtain a comprehensive picture of interests. The corresponding data remains entirely within the platform and is not passed on directly to external third parties, but only in aggregated or anonymised form via the advertising or reporting interfaces controlled by the platform.
For context: in this context, these "walled gardens" refer to closed platform ecosystems in which central infrastructure elements such as login IDs, targeting or measurement mechanisms are exclusively under the control of the respective platform operator.

- *Privacy-enhancing browser APIs*

In response to stricter data protection rules and discussions about third-party cookies, the industry is working on new solutions that will enable targeted advertising without individual tracking. Here, the browser determines some rough categories of interest for the user locally (e.g. "sports", "travel") based on their surfing behaviour and shares this topic tag with advertising partners instead of individual IDs. Advertisers can then say, for example, show this ad to everyone who has the topic "cars" in their browser. The specific websites that the user has visited are not disclosed to the outside world. Such approaches aim to use group profiling instead of individual profiling.

- *Platform-internal personalisation*

Platforms such as YouTube, Instagram, TikTok, etc. use on-platform tracking. All activities (likes, views, scrolls) are recorded in order to personalise the feed or display relevant advertising within the platform, for example. Machine learning algorithms are used here to recommend similar content based on user behaviour (keyword: recommendation systems).

- *Hash matching , and CRM applications*

Companies have customer data (e.g. email addresses of newsletter subscribers or buyer lists). Many advertising platforms allow such data sets to be uploaded in hashed form, with consent, in order to find the corresponding users online. In this context, hashed means that the original data (e.g. email addresses) is converted into a code that is not directly readable before it is transmitted to the platform. For example, a retailer can deliver its customer emails to a platform; the platform hashes its user emails using the same hash method and creates a intersection (custom audience). This allows the retailer to specifically target its existing customers with advertising, exclude them or form similar target groups (lookalike audience).

- *Geo-location targeting*

Geo-location targeting uses the geographical position of users to deliver targeted content or advertising. This can be done on the basis of GPS data, IP address, Wi-Fi or mobile phone masts. Advertisers can, for example, display local offers, locations or regional services only to users who are in a specific area. Technologically, geodata services, mobile SDKs or location APIs are used here. Approaches such as geo-fencing also enable the targeted addressing of users who enter or leave a defined geographical area (such as a 3 km radius around a football stadium).

- *Contextual targeting*

Contextual targeting involves displaying advertising that is relevant to the content of a website, app or media format without personally identifying users. Algorithms analyse text, images, videos or metadata to select thematically relevant ads (e.g. travel ads on a travel blog site). The focus is on the environment and macro context, not on individual user profiles. Technologically, natural language processing, image and video classification or semantic analyses are used to identify relevant connections between content and ads. Contextual targeting can be suitable for some purposes. However, contextual targeting only takes into account the page or app content, not individual user behaviour. As a result, the approach is often less precise, long-term user profiles cannot be built up, and the relevance of the advertising may be limited for very specific target groups.

Contextual targeting is currently being further defined within the framework of the BVDW in one of its working groups.

- *Analysis/comparison of data via data clean rooms*

Data clean rooms are secure, privacy-compliant environments where advertisers and platforms can compare and analyse data without directly exchanging personal information. They enable this comparison to define target groups, measure campaigns or gain insights without the raw data leaving the domain of the controller. Technologically, encrypted IDs, aggregations and anonymised analyses are often used so that no conclusions can be drawn about individual users. Data clean

rooms are particularly relevant for enabling data protection-compliant attribution, target group analysis and campaign optimisation even without third-party cookies.

- *Ultrasonic beacons (cross-device tracking)*

A rather exotic and rarely used method is tracking via ultra-high-frequency sound signals to assign different devices to the same person. For example, a TV commercial or an advertising banner on a laptop emits an ultrasonic pattern that is inaudible to humans. An app on the smartphone listens with the microphone and recognises this signal, allowing it to determine that both devices belong to the same user. This could be used, for example, to track whether someone searches for the product on their mobile phone after seeing a TV commercial. From an advertising industry perspective, this technology is irrelevant. It is neither used as standard nor defended, as it would massively jeopardise user trust.

6. Purposes and TCF

6.1. Purposes

The following sections provide an overview of the various purposes for which tracking and targeting technologies are used in digital advertising. They show how usage and interaction data is used to deliver targeted advertising, measure reach, personalise content or optimise the effectiveness of campaigns.

It becomes clear that the data collected is not only used for traditional advertising purposes, but also to improve the user experience, detect fraud and support data-driven product development. This chapter explains the common methods, the technical mechanisms behind them and the different objectives in the digital advertising ecosystem.

The Transparency & Consent Framework (TCF) is a standard developed by IAB Europe that ensures that users are informed transparently about tracking and advertising purposes and can give or refuse their consent in accordance with data protection regulations. It enables publishers and advertising partners to process consent systematically and thus display digital advertising in a legally compliant manner.

- *Ad targeting (targeted advertising)*

This refers to the delivery of advertising to specific target groups based on certain criteria. Behavioural targeting is the analysis of previous online behaviour, e.g. websites visited, search terms, clicks and demographic characteristics, in order to deduce the user's interests and display appropriate advertisements.

These forms of targeting use the data mentioned above. For example, cookie IDs or device IDs are used for behavioural targeting to create interest profiles based on usage behaviour, or account data such as age information is used for demographic targeting.

- *Conversion tracking/attribution*

This records which advertisement led to a conversion (a defined success, e.g. purchase, registration). Typically, when an advert is clicked on, an identifier (cookie ID or specific click ID) is provided and read on the landing page or when the purchase is completed in order to assign the conversion to the original advert. Tracking pixels or scripts are often used, which fire on the order confirmation page and report the success to the advertising system (e.g. the Meta/Facebook pixel, which reports website actions to Facebook Ads for success measurement).

This enables attribution, i.e. the assignment of success to an advertising channel or campaign. Advanced attribution models distribute the user's path across multiple touchpoints (e.g. when a

user converts across multiple ad contacts and devices), using cross-device IDs or identity resolution models to merge a person's interactions across cookies and devices.

- *Reach measurement*

The reach of a campaign or website indicates how many unique users were reached. Unique identifiers are required for measurement in order to recognise multiple contacts. For example, an ad server counts the unique cookie IDs or device IDs that have seen an ad to determine the number of individual users. Frequency capping (see below) is also used to count how often the same user has seen an ad – both together result in the reach and frequency of a campaign. , identity matching is used for cross-device reach measurement (e.g. a user surfing on their mobile phone and laptop), such as login IDs (if the user is logged in on both devices) or probabilistic models that combine usage based on common characteristics (IP address, device type, time).

In the UK, standardisation often involves the use of common measurement methods (e.g. IVW or AGF), which use tracking scripts or tracking pixels on many websites to collect anonymous user identifiers in order to calculate overlaps. Modern web analytics tools also offer cookie-free reach measurement, which, for example, only counts aggregated page views without individual-specific IDs.

- *Personalisation of content*

In addition to advertising, the data is also used to tailor content to the user. Recommendation systems (recommenders) on streaming platforms or news sites, for example, analyse usage behaviour in order to make personalised suggestions. Netflix, for example, takes into account "*your interactions with our service (such as your viewing history and ratings of other titles)*" as *well* as *"other signals such as time of day, device used, language settings and how long you watched something*" for its recommendations. Similarly, YouTube evaluates video history and interactions (likes, watch time) to personalise the feed. Spotify analyses listening history, skipped songs and preferred genres to compile curated playlists (Daily Mix, Discover Weekly). Profiles are created for each user or device (via login, cookie or device ID) to store preferences. The algorithms often compare the behaviour of many users (collaborative filtering) and use content metadata to play relevant content individually.

- *Frequency capping*

This refers to limiting how often the same user sees a particular advertisement. To implement this, the ad server must be able to recognise a returning user. On the web, this is usually done via cookies: when the user first encounters an ad, they are assigned a unique user key in a cookie, which is used to count how many ad impressions this user has received. In mobile apps, device-side advertising IDs (IDFA/GAID) serve as identifiers that are read by the ad SDK and reported to the ad system. For example, it is possible to set a specific ad to appear once per user in 24 hours – the system stops delivering ads to the same ID after a certain number of impressions. Frequency capping prevents ad fatigue and improves the user experience by avoiding excessive repetition.

- *Fraud Prevention / Bot Detection*

In digital advertising, fraud detection is important for filtering out invalid impressions or clicks (e.g. from bots, scripts or fraudulent websites). Technical characteristics and usage data are used to identify conspicuous patterns. For example, device fingerprints can be created to recognise a device and detect fraudulent behaviour (e.g. a device that loads hundreds of ads per minute). IP addresses are monitored (many clicks from the same IP in a short period of time), behavioural metrics are analysed (inhumanly uniform mouse movements or scrolling behaviour) and blacklists of suspicious device IDs or user agents are maintained.

In addition, there are industry-standard fraud and bot lists, e.g. from the IAB Tech Lab or the TAG initiative, whose known sources are centrally recorded and automatically excluded from delivery. Modern fraud detection systems use machine learning to distinguish fraudulent behaviour from genuine behaviour. If a pattern is recognised as a bot, further requests from this user can be

blocked or excluded from billing. Overall, these measures help to protect advertising budgets from ineffective deliveries and increase brand safety.

- *A/B testing and product development*

Web services and apps also use user data to test new features or designs. In an A/B test, the user base is randomly divided into groups (e.g. by cookie ID or user ID) and each group sees a different version of a website or app. By tracking usage metrics (click-through rate, conversion rate, dwell time, etc.) for each variant, it is possible to analyse which version performs better. The same tracking data is used for this purpose: unique user IDs ensure that a user consistently sees only one variant, and events from usage behaviour show differences in engagement. The results are incorporated into product development – for example, the layout that achieved better results in the test is chosen. A/B testing therefore requires the collection of interaction data and often the linking of this data with customer data (e.g. to check results for specific segments). Overall, such experiments enable data-driven optimisation of products and advertising materials.

- *CRM onboarding / target group matching*

This involves linking offline customer data (from an advertiser's CRM) with online identifiers in order to address existing customers or defined target group segments online. One example is uploading an encrypted customer list (e.g. hashed email addresses) to an advertising platform such as Facebook or Google. The platform then performs a comparison and creates a custom audience from the users it was able to match in its database. This allows a company to use ads to re-target customers whose contact details were collected in-store, for example (retargeting existing customers), or to find similar target groups (lookalike audiences). Device IDs can also be used for onboarding, e.g. to find app users in an advertising network. Technically, first-party data (email, telephone number, customer number) is anonymised using hashing and passed on to the ad provider, who compares it with their login databases.

6.2. Transparency and Consent Framework (TCF)

The IAB Europe Transparency and Consent Framework (TCF) defines standardised purposes for data processing, which make it possible to inform users transparently about processing activities, obtain the specific legal basis in a legally valid manner, and ensure that users can make competent and independent decisions. For points 1 to 11, for example, consent or objections are obtained from users.

These purposes are explained in English below:

1. **Storing and/or retrieving information on a device.** Storage of or access to information such as cookies, device identifiers or other data on the user's device (e.g. for recognition on subsequent visits).
2. **Use limited data to select advertisements.** Select advertisements based on general information (e.g. page context or rough location data) without using individual profiles.
3. **Creating profiles for personalised advertising**. Building detailed user profiles based on browsing behaviour to derive preferences, interests and demographic characteristics for targeted advertising.
4. **Selecting personalised advertising based on a profile**. Selecting advertisements based on previously created user profiles in order to display the most relevant advertising possible.
5. **Creating profiles for content personalisation.** Creating profiles to customise editorial or editorial-like content, such as recommendations on news portals or streaming services.
6. **Selecting personalised content based on a profile.** Selecting and displaying individualised content based on known user preferences (e.g. recommended articles, videos, products).

7. **Measuring the performance of advertisements.** Analysing the effectiveness of individual advertisements, for example, how many users saw them, clicked on them or subsequently purchased a product.
8. **Measuring content performance.** Evaluating how well content (e.g. articles, videos, products) is received by users, e.g. through dwell time, scrolling behaviour or interactions.
9. **Understanding target groups based on statistics or data combinations.** Aggregated data analyses to gain insights into user segments, e.g. typical interests, age structure or usage patterns.
10. **Develop and improve services**. Use the collected data to optimise digital products, apps and websites – e.g. through A/B testing or user feedback.
11. **Use limited data to select content.** Non-personalised selection of content based on contextual information, such as the type of page accessed or the device used.
12. **Ensure security, prevent fraud and troubleshoot errors.** Detection and prevention of fraudulent or erroneous use, e.g. through bot detection, protection against misuse or debugging.
13. **Delivering and presenting advertising and content.** Technical provision of content and advertisements – including loading time, formatting, and display on the end device.
14. **Store and transmit data protection preferences.** Collect and manage users' consent decisions (e.g. via the consent banner) and pass them on to the providers involved.
15. **Matching and combining data with other data sources.** Merging different data sources to obtain a more complete picture of user interactions – e.g. CRM data with online data.
16. **Link devices across different contexts.** Identification and assignment of users across multiple devices – e.g. when someone clicks on a smartphone and later makes a purchase on a laptop.
17. **Identify devices based on automatically transmitted characteristics**. Recognise devices via technical characteristics such as screen resolution, browser version or installed fonts (device fingerprinting).
18. **Use precise geolocation data.** Use accurate location data (e.g. via GPS) to localise the user – e.g. for location-based advertising or services.
19. **Actively scan device characteristics to identify them**. Actively collect technical data from the device (e.g. via a script) to uniquely identify individual devices – usually for fraud detection or recognition.

7. What data is currently being used?

In online advertising and personalised services, the following types of data are primarily used, depending on function and necessity. Often, several types of data are used simultaneously, while some data are used less frequently or in very specific cases:

Type of data	Description
Cookie ID	Unique identifier in a browser cookie, used to recognise a user or browser across different page views and websites. Often set by advertising networks to track user activity across pages.

Background paper

Device ID	Device-related identifier, especially on mobile devices (e.g. Apple's IDFA or Google's Advertising ID). This allows users to be identified across devices, provided that apps or advertising SDKs read this ID. Often used for in-app tracking and mobile advertising.
IP address	Numerical network address of the user. It enables rough location determination (geolocation) and can be used for fraud detection or visitor recognition. However, multiple users sometimes share an IP address (e.g. in company networks).
Geolocation data	Location data of the user, either precise (GPS data, Wi-Fi) or approximate (derived from the IP address). This is used to display location-based content or advertising (e.g. local offers near the user).
Usage behaviour	Data about the user's behaviour and interactions, e.g. websites visited, content viewed, clicks, search queries, purchase history or length of stay. Such behavioural data is used to create interest profiles (for personalised recommendations or targeted ads).
Account data	Profile data provided by the user in an account, e.g. name, email address, age, gender, customer history or interests. This data is mainly used in login-based platforms to display advertising based on demographics or to personalise content (e.g. personalised recommendations, greeting by name).
Browser/ Device characteristics	Technical characteristics of the device and browser used: e.g. device type (smartphone/desktop), operating system, browser version, screen resolution, language settings, installed plugins or fonts. Such information is used in part for device or browser recognition (fingerprinting) or to optimise content technically (e.g. mobile vs. desktop version).
Segments	Grouped user groups with similar characteristics or behaviour patterns defined by advertisers or data platforms. Segments can reflect interests (e.g. "travel enthusiasts"), demographics (e.g. "men aged 30–45") or purchase intentions (e.g. "car purchase in the next 30 days"). They are created by clustering user data from various sources (, onsite tracking, CRM, DMPs) and are used for targeted advertising. Segments are often standardised and marketed by data providers or adtech platforms. A person can be part of several segments at the same time.
Clickstream / referrer data	The sequence of pages visited by a user within a session (including previously visited websites, known as referrers). This data provides information about user intent and navigation patterns and is used for attribution, targeting and UX optimisation.
Session data	Information that is only stored for the duration of a browser session, e.g. session ID, login status or interim results from forms. Often used for conversion tracking, shopping baskets or login-based applications.
Payment and transacti data	Data relating to orders, purchases, bookings or payments (e.g. product type, shopping basket value, payment method). This data is used to evaluate campaign success (ROI) and to create buyer segments for targeting and retargeting purposes.

Feedback and interacti data	Reviews, comments, support requests or feedback forms. This qualitative data supplements quantitative user behaviour and can be used to improve the customer experience and form affinity groups.
Campaign IDs / Creativ IDs	Technical markers for identifying individual advertising materials or campaigns. Used to attribute clicks and conversions to specific creatives or campaign variants (e.g. A/B testing, performance optimisation).
Consent data	Information about the consents or objections given by the user, stored e.g. in TC strings or via consent management platforms (CMPs). These are essential for the lawful processing of personal data in the context of advertising and analysis.

8. What measures and techniques are essential?

Tracking and data processing are indispensable in many areas of the digital economy. They form the basis of many innovations, from recommendation algorithms and user experience optimisation to fraud prevention. Personalised digital advertising is a key application of these data flows and makes a central contribution to the refinancing of freely accessible content and digital services. It enables companies, especially small and medium-sized providers, to finance their offerings efficiently, target them effectively and provide users with relevant content instead of irrelevant mass advertising. At the same time, many innovations, from recommendation logic and user-friendliness to fraud prevention, would be inconceivable without the underlying data flows and technical processes.

The measures and techniques listed below are examples of practices that, from the perspective of the digital economy, are indispensable for the operation, financing and continuous optimisation of digital offerings. Detailed descriptions of the respective measures and techniques can be found in chapters 5 and 6.

8.1. Measures

1. **Reach and campaign measurement.** Tracking unique users, impressions and conversions is essential for measuring the success of campaigns and allocating advertising budgets efficiently, especially in the highly competitive digital market.
2. **Frequency capping (limiting ad repetition).** This protects users from excessive ad repetition and prevents ad fatigue. Not only does this improve the user experience, it is also a key control tool for advertising quality and user experience.
3. **Fraud prevention and security (e.g. fraud prevention, bot detection, invalid traffic).** The use of technical features (e.g. device fingerprints, behaviour patterns) to detect fraudulent access is essential for the integrity of advertising systems and the protection of budgets and users. General fraud lists, e.g. from the IAB, are also used to exclude suspicious devices or IPs.
4. **Personalised advertising.** Targeted advertising based on interests, behaviour or demographic characteristics increases relevance for users, boosts the efficiency of marketing budgets and contributes to the refinancing of digital offerings.
5. **Content personalisation.** The adaptation of editorial content, product recommendations or user interfaces based on user behaviour is part of the contractual service provision for many platforms or is carried out on the basis of a legitimate interest, such as increasing relevance.
6. **Conversion tracking/attribution.** The assignment of advertising contacts to specific conversions (purchase, registration, etc.) is crucial for measuring the success of campaigns.

7. **A/B testing and product optimisation.** The use of tracking data for data-based further development of services, e.g. by testing alternative UX designs or features, is indispensable for the innovation and competitiveness of digital products.
8. **Geotargeting / contextual targeting.** The delivery of content or advertising based on location data or page context increases relevance for users and is a proven marketing control tool.
9. **On-platform recommendations / on-platform personalisation.** Within platforms, user activities are analysed in order to customise feeds, recommendations or content. These improve the user experience and loyalty to the platform.

8.2. Techniques

10. **Cross-device tracking and identity resolution.** The consolidation of interactions across multiple devices enables consistent user profiles, which are crucial for both advertising efficiency and personalised services.
11. **Consent management and transfer (TCF/CMP systems).** Without functioning consent management systems, legally compliant data processing is not possible. The storage and transmission of consent decisions (e.g. TCF string) provides a technical basis for many other processes.
12. **Data clean rooms.** These enable the data protection-compliant comparison and analysis of first-party and, where applicable, third-party data in order to gain insights for campaign optimisation without directly passing on personal data.
13. **ID partnerships.** Technical solutions such as login-based IDs or shared identification systems (e.g. EU ID, ID5, Ramp ID) enable consistent targeting across platforms and are important for reach measurement, conversion tracking and personalised advertising.

9. Facts about tracking and personalisation in the context of the Digital Fairness Act

As part of the planned Digital Fairness Act, the EU is discussing policy measures against unethical techniques in digital marketing. User trust is essential for the survival of the digital economy. Without trust in products, offers and information about how data is used, digital business models cannot survive, let alone flourish.

Today's political debate often focuses on the exploitation of consumers' vulnerabilities or emotional states for commercial gain. With this technical paper, we aim to contribute to raising awareness about the use of data for tracking. It serves as a basis for discussion and aims to highlight the necessary distinction between responsible data processing and genuinely problematic practices.

The fundamental question: "What is actually collected during tracking?"

This paper clarifies what types of data are currently used for tracking and personalised advertising – from technical identifiers (such as cookie ID, device ID), rough usage profiles, account information, location, surfing behaviour and segmentation based on obvious interests and past interactions.

This paper clearly states that the direct collection and evaluation of particularly sensitive data, which explicitly includes emotional states, is deliberately excluded, both for technical reasons (no reliable measurement without an explicit signal, e.g. health data) and for regulatory reasons (Art. 9 GDPR, prohibition of profiling based on specially protected characteristics). There is no technical infrastructure or practice that allows the tracking of individual emotional states, in the sense of continuous emotion measurement or evaluation, in everyday advertising or personalisation. Neither are psychological profiles created at this level, nor do standard processes for individual "emotion or

vulnerability recognition" exist. Methods that are considered particularly invasive (such as ultrasound tracking for context coupling or psychometric fingerprinting at the individual level) are explicitly not used and rejected by the industry itself.

Personalised, behaviour- and interest-based advertising, as is common practice in the digital world, is based on segmented group profiles ("target groups", "segments"), not on individual weaknesses or situational emotions.

The ban on systemic emotion control or the targeted exploitation of momentary weaknesses through personalisation and advertising systems, which is repeatedly called for in political debate, is not based on any real technical foundation. In current practice, these risks are abstract and are ruled out by technical limitations. The targeted exploitation of emotional states or individual vulnerabilities does not take place in digital advertising practice. Personalisation is based on group profiles and obvious usage interests, not on psychological manipulation. In addition, the numerous existing data protection and consumer protection regulations (in particular the GDPR and DSA) as well as industry self-restrictions ensure that certain practices are excluded.

However, what needs to be improved is the implementation and enforcement of the existing legal framework. Consistent and fair enforcement practices towards all market participants would not only better protect consumers, but also strengthen fraud prevention and ensure a genuine level playing field for the digital economy. In addition, we strive for legal certainty and clear, practicable guidelines that are comprehensible to both authorities and businesses. The aim is to create a common understanding of legitimate, innovation-driven business practices in the digital economy while minimising grey areas that could lead to uncertainty or unequal competitive conditions. Responsible data processing in conjunction with legal clarity in today's regulatory framework is the basis for digital business models to operate in a sustainable, efficient and trustworthy manner for all parties involved.