

## Regulation of online advertising Position paper

### Key messages

[Schibsted](#) is a family of digital consumer brands based in the Nordics with world-class Scandinavian media houses, leading classifieds marketplaces and tech start-ups in the field of personal finance and collaborative economies. Many of Schibsted's digital services are financed by online advertising. It is an important source of revenue for our newspapers, but also ensures access to digital consumer services such as price comparison sites, that make people's daily lives easier. Moreover, it supports the operation of classified marketplaces that allow people to sell used goods to each other, contributing to a circular economy.

Schibsted fully understands the concerns of decision-makers about intrusive online advertising and the use of users' data. However, a complete prohibition of targeted advertising or strict opt-in requirements would pose fundamental challenges to the continued availability of high quality journalistic content for the public and lead to fewer and poorer services for users. **Online advertising directly funds high quality journalism, the creation of new content and services, and makes services available with lower or no financial payment from users. A reduction in online advertising revenue is likely to lead to fewer services for users, decreased quality, and increase the imbalance in access to authoritative and reliable news media for those who cannot or will not pay for access to such content.**

We believe that the concerns related to the use of personal data in online advertising can be solved by the following means:

- 1. Effective enforcement of GDPR and e-privacy rules to ensure personal data is not used in a way that is harmful to consumers or the interest of society at large.**
- 2. Limit the extensive data collection across the Internet by digital gatekeepers by strengthening Article 5a in the DMA.**
- 3. Add transparency requirements for and opt-out from online advertising in the DSA that would benefit consumers, publishers and advertisers alike.**

There are already several aspects of EU law that protect users' personal data, which is broadly defined and includes pseudonymous data, the type of data mostly used in online advertising. The use of personal data for online advertising is regulated by GDPR, according to which there are two potentially relevant legal bases (*consent*, art. 6(1a) and *legitimate interest*, art. 6(1f)), and the use of device identifiers is regulated by the e-privacy Directive (forthcoming e-privacy Regulation).

**Adding new rules for the use of personal data for advertising in the DSA would risk double or even triple regulatory scrutiny over the same issue. It would also lead to multiple national authorities enforcing rules around online advertising.**

## DMA Article 5a - Collection and combination of personal data by digital gatekeepers

Digital gatekeepers, usually the “point of first contact” online, often require users to agree and consent to the use of their data across other parts of their business and the wider internet, including from sites and apps where users cannot reasonably be expected to understand that their data is being collected by the gatekeeper. This “aggregation of consent” leads to an accumulation of data in the hands of the few largest companies, raising barriers to competition, and to users feeling “followed” online and not understanding how their data is being collected and used online.

Gatekeepers collect data from third party services in different ways, for example when consumers sign into an app or website using the gatekeepers’ sign in functionality. A gatekeeper can also be a data processor as defined in GDPR. In this scenario the gatekeeper may process data from external sources, but only as a service provider processing data in accordance with instructions from their customers (the data controller) and limited to the purposes defined by their customers.

The prohibition on gatekeepers combining personal data from third party services with their own services in Article 5a of the DMA would ensure gatekeepers cannot collect personal data about users across the Internet. We are of the strong view that the feeling of being surveilled on the Internet, especially for advertising purposes, would be well addressed by the proposed prohibition. **However, for Article 5a to be efficient and really make a difference, the consent exception must be removed.**

Consent is often a precondition to allow users to access and use gatekeepers’ services and most gatekeepers already use consent to justify broad data collection and nudge users towards accepting their terms and conditions.

We therefore call for the following amendment to Article 5a to clarify and strengthen the provision.

Article 5a - Current text	Article 5a – Proposed text
<p>[In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:]</p> <p>(a) refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing 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 provided consent in the sense of Regulation (EU) 2016/679.</p>	<p>[In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:]</p> <p>(a) refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, <del>unless the end user has been presented with the specific choice and provided consent in the sense of</del> Regulation (EU) 2016/679.</p>

## DSA – Article 24 - Transparency and user choice on all online platforms

Transparency is generally lacking in the online advertising ecosystem, to the detriment of users, advertisers and publishers. While Article 24 in the Commission's proposal on the DSA introduces certain elements of transparency, we suggest the following additions:

1. **More transparency** around which entities are involved in the delivery of an online advertisement. The first step in controlling personal data, both for consumers, publishers and advertisers, is insight. Especially for smaller publishers, a lack of knowledge about vendors involved in their advertising business makes taking meaningful decisions around business partnerships and data usage challenging. Additional transparency is important to enable collaboration with vendors that handle personal data in compliance with GDPR, and to select trustworthy partners and vendors.
2. **Greater user choice** in how personal data is used in online advertising. Although targeted advertising is a key source of revenue for most online media services, **users should have the option of opting out should they wish.**

The GDPR already applies to targeted advertising based on personal data, and to a great extent the current weaknesses in user choice, is an enforcement issue of the GDPR. Under GDPR, there are several potential legal bases for processing personal data. *Consent* (GDPR art. 6(1a)) is one of these, but not the only one. The legislator therefore has acknowledged under GDPR that *consent* should not always be the legal basis for processing personal data, and that other legal bases may sometimes be more appropriate. Through the legal basis *legitimate interest* (GDPR art. 6(1f)), different interests that may be present are acknowledged. Additionally, the *legitimate interest* legal basis opens for a concrete assessment of how personal data is actually processed, and what measures to protect users' integrity are in place. User choices are often relevant also under the legal basis of *legitimate interest*, although normally as an opt-out and not opt-in.

To strengthen user choice, we propose the following amendment to Article 24 of the DSA:

Article 24.2 – Current text	Article 24.2 new – Proposed text
	<p><u><i>Online platforms shall offer users the possibility to easily opt-out from micro-targeted tracking and advertisements that are based on their behaviour data or other profiling techniques, within the meaning of Article 4(4) of Regulation (EU) 2016/679.</i></u></p>

Schibsted also supports further clear prohibitions to strengthen privacy and consumer protection in the online advertising ecosystem . These are:

1. **No use of sensitive data for targeting purposes.** Sensitive data is defined as *special categories of data* according to GDPR art. 9(1), meaning personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation.
2. **No targeting of vulnerable groups** such as children, or people showing interest for specific health issues (such as illnesses or medicines), or specific sensitive content such as ethnicity, religious beliefs or sexual orientation.

## **Contextual advertising**

Many decision-makers favour “contextual advertising” over “targeted advertising” and believe this would be a workable and beneficial solution to news publishers in Europe. While contextual advertising is already in use and complements other forms of online advertising, the commercial potential remains uncertain. At Schibsted, contextual advertising is in a nascent stage and only a small part of our overall online advertising revenues. Our estimates show that even in the longer term, contextual advertising will most likely not amount to more than 15% of our advertising revenue in the future.

Contextual advertising is for several reasons not as effective for advertisers and not as relevant to users. For contextual advertising to function effectively on a news publishers’ platform, the user would need to read a relevant, non-generic article in the same time period an advertiser has a relevant message to communicate. This is not always the case. Viewing a single article is also not a clear indication of a user's interests, limiting the ability of contextual advertising to present users with advertising of relevant products and services based on their interests.

Furthermore, contextual advertising in its current form is not clearly defined by legislators, and its scope and value will differ depending on the definition used. It can be an advertisement based on the content of a newspaper article, but also based on certain personal data such as geographical location of the user or keywords used. In both cases, those set to benefit most from contextual advertising would be search engines and / or large social networks that already cater to different groups based on these criteria; keywords used in search queries or geographical locations of groups active on their platforms.

Finally, it is important to note that the delivery of contextual advertising also uses personal data. Personal data is used in the technical delivery of the advertisement (e.g. the IP address of the user is processed by a server to place the advertisement on a given site), and for advertisement / campaign measurement (how many times an advertisement has been shown to a user).

**We are strongly of the view that permitting only contextual advertising would be to the detriment of the media sector in Europe. Contextual advertising can continue to be a useful form of advertising, but should not replace more targeted advertising that is both more relevant to the user and has a higher value to both advertisers and publishers alike.**