

## **IAB Europe's preliminary comments on the review of legal framework for digital services (Digital Services Act) - Executive Summary**

This document contains an overview of IAB Europe's preliminary comments on the review of legal framework for digital services, further to the European Commission stating in its 2020 work programme that it will propose a new Digital Services Act (DSA) to strengthen the single market and protect citizens and their rights. IAB Europe (Transparency Register: 43167137250-27) is the European-level association for the digital advertising and marketing ecosystem.

- We recognise the importance of discussion to strengthen the single market and protect citizens and their rights. We find it critical for the European businesses to continue deriving value from their activity in the digital space, in particular, the European media for which advertising is the major revenue stream that consequently provides users with unpaid access to content and services.
- We call on the policymakers to be cognisant of the existing regulatory framework, in particular, the EU privacy and data protection framework applicable to any business activity underpinned by data. The General Data Protection Regulation unambiguously established the principles of data protection in the digital advertising context.
- Keeping users safe online is critical from the digital advertising industry perspective.
  - In doing so, one should acknowledge the difference between illegal and harmful content. Existence of a well-established self-regulatory framework for advertising content allows consumers to lodge complaints about any type of advertising considered to be inappropriate.
  - The industry is committed to minimise the risk of advertising inadvertently funding websites hosting illegal or illicit content, as well as content considered to be disinformation with strong voluntary 'follow-the-money' measures. While eradicating such malpractice is challenging due to the boundless and pervasive nature of the internet, the industry has proven that technology standards and best practice constitute a sound approach. This allows for rapid reaction and significant improvement of the situation over time, further enabling innovation, to the advantage of the businesses and ultimately users benefiting from access to free ad-supported content that powers the open web.
  - It is vital to keep in mind that from the user perspective, the EU privacy and data protection framework explicitly recognises a host of user rights from which consumers can benefit in relation to advertising powered by data.
- The industry is committed to maintaining transparency and quality across the digital advertising and marketing ecosystem, for all forms of trading. Industry-driven approaches and technical standards to generate said transparency should be recognised. Given the ever-evolving technology, imposing prescriptive measures would stifle innovation and growth, besides the fact that any legal rules would very quickly become outdated.
- The existing liability regime reflects the reality of the market, whereby digital media is bought on behalf of the buyer. We do, however, welcome reflection on the 'Good Samaritan' provision, which could allow the digital advertising ecosystem players to continue voluntary monitoring without losing the benefit of the safe harbours.

## IAB Europe's preliminary comments on the review of legal framework for digital services (Digital Services Act)

IAB Europe (Transparency Register: 43167137250-27) represents 25 European national associations who in turn associate over 5,000 companies from across the digital advertising and marketing ecosystem, from advertisers and advertising agencies on the buy side, news publishers and other ad-funded sites and online services on the sell side, and technology providers facilitating the delivery of ads. We have over 90 companies in direct membership, including agencies, technology companies, publishers and eCommerce companies.

In its 2020 work programme, the European Commission (Commission) stated that it will propose a new Digital Services Act (DSA) to strengthen the single market and protect citizens and their rights<sup>1</sup>. IAB Europe (Transparency Register: 43167137250-27) would like to take the opportunity to provide feedback on the themes already being discussed in connection with the DSA package, conveying the views of the digital advertising and marketing ecosystem.

We recognise the importance of discussion to strengthen the single market and protect citizens and their rights. We find it critical for the European businesses to continue deriving value from their activity in the digital space, in particular, the European media for which advertising is the major revenue stream that consequently provides users with unpaid access to content and services. Advertising accounts for over 81% of European newspaper and magazine digital revenues, and any decrease in these monetisation opportunities supporting the objective, good-quality journalism would have serious consequences for the social and political landscape in Europe. We, therefore, call on the policymakers to be cognisant of the existing regulatory framework, in particular, the EU privacy and data protection framework applicable to any business activity underpinned by data. The General Data Protection Regulation (GDPR)<sup>2</sup> unambiguously established the principles of data protection in the digital advertising context.

This paper has been framed in the following way:

- **Part 1 – Introduction – Background**
  - *Digital advertising and the European economy*
  - *Digital advertising – practical considerations and binding regulatory framework*
- **Part 2 – Keeping users safe online from digital advertising perspective**
  - *Self-regulatory framework for advertising content*
  - *Follow-the-money approach to minimise ad misplacement*
  - *Relevance of the GDPR for user rights*
- **Part 3 – Transparency in digital advertising supply chain**
- **Part 4 – Liability regime of digital services**

---

<sup>1</sup> European Commission, [Commission Work Programme 2020](#), 29 January 2020.

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

## Part 1 – Introduction – Background

### ***Digital advertising and the European economy***

Digital advertising is an umbrella term for a large range of activities. It stretches from paid-for search, over online banners, social media, video advertising, to digital audio and other emerging formats like out of home and connected TV, increasingly blending with traditional media.

In Europe, digital ad spend amounts to €55 bn<sup>3</sup>. But digital advertising’s estimated contribution to the wider EU economy exceeds €118 bn, while the industry powers over 1 mln jobs directly and over 6 mln indirectly. Critically, Europe’s content economy depends on digital advertising, with advertising accounting for over 80% of European newspaper and magazine digital revenues<sup>4</sup>. Digital advertising ensures consumers can choose what they pay for, thus democratising access to information and other online services. In fact, European online users are happy for their data to be used for targeted advertising in order to get access to free content supported by advertising, and 83% would prefer free sites with ads to paying for ad-free content<sup>5</sup>.

### ***Digital advertising – practical considerations and binding regulatory framework***

In practice, the mechanics of the digital advertising ecosystem<sup>6</sup> are underpinned by the ability to process data for advertising-related purposes, including but not limited to delivery and measurement of digital advertising. The data processed for the purpose of this type of activities may include IP addresses, online advertising identifiers, URLs of sites that users spend time on, information about user behaviour on those sites, and indications about the users’ physical whereabouts (“geolocation” data). Most or all of these data points are considered to be personal data under the GDPR. From this perspective, the EU privacy and data protection legal framework is the prime legal regime that the ecosystem players consider to be relevant. Currently, that regime is the conjunction of the GDPR and the ePrivacy Directive (2002/58/EC), with the former regulating the processing of personal data and the latter storage and access of information on a user’s device.

Digital advertising has pioneered the better addressability of right audiences. Instead of relying just on broad demographics segments, digital advertising can use information about users’ online behaviour to assign them to large segments – or “audiences” – that all share common interests, and because of those common interests, may be interested in a specific good or service. The identity of a specific individual consumer is not of interest to an advertiser. Rather, the aim is to create narrower

---

<sup>3</sup> [AdEx Benchmark 2018 study](#), IAB Europe, 2019.

<sup>4</sup> [The Economic Contribution of Digital Advertising in Europe](#), IHS Markit, 2017.

<sup>5</sup> [Europe Online: An Experience Driven by Advertising](#), GfK, 2017.

<sup>6</sup> There are many different digital advertising models, including but not limited to: ad servers, ad exchanges, SSPs, DSPs, DMPs, ad networks, attribution vendors, market research companies, data companies, affiliate marketing companies and cross device vendors. Each digital advertising company has its own unique characteristics. That said, in all instances the ecosystem as such relies on the interplay of a variety of market participants, from the buy and sell side, from technology and creativity.

segments. For instance, brand advertisers do not want or need to know who individuals are to reach customers that might enjoy their products or services.

When done correctly, profiling and targeting also serves the interest of consumers. It ensures the provision of quality advertising that is likely to be relevant to them and reduces the chance of consumers being exposed to ads too frequently.

## **Part 2 – Keeping users safe online from digital advertising perspective**

In trying to ensure that users are kept safe online, from the digital advertising perspective it is imperative to understand and address the issues at hand, which also envisages clearly differentiating between illegal and potentially harmful content.

### ***Self-regulatory framework for advertising content***

To start with, one should not confuse any malpractice with some of legal advertising practices, including native advertising<sup>7</sup>, advertorials<sup>8</sup> or sponsored content more broadly. Moreover, one should acknowledge existence of a robust advertising self-regulatory system<sup>9</sup>, which covers 97% of all advertisements seen by the EU population, builds on the Unfair Commercial Practices Directive legal framework and plays an essential role in preventing the spread of misleading or otherwise harmful advertising on all media, including online. Striving to achieve that all advertising practices must be legal, decent, honest and truthful, the self-regulatory framework plays an important role in ensuring a high level of consumer protection and trust. The self-regulatory system features not only codes of conduct, independently enforced by the self-regulatory bodies, but provides monitoring, training and compliance advice to the industry. The European bodies deal with on average 60,000 complaints per year and deliver additional 90,000 pieces of tailored advice to the industry<sup>10</sup>.

### ***Follow-the-money approach to minimise ad misplacement***

Regrettably, legitimate advertising may appear on websites which host illegal or illicit content and revenues derived from advertising can partially or wholly fund such websites.

It is important to appreciate that in such cases the whole industry – advertisers and advertising agencies on the buy side, news publishers and other ad-funded sites and online services on the sell side, and technology providers serving both sides – must be considered as collateral damage of intentional misbehaviour and not as contributors to malpractice.

---

<sup>7</sup> Contextually targeted branded content, designed to fit in with the particular online environment to give consumers a visually consistent browsing experience and be less disruptive, while having prominent labelling to make clear that it's a marketing communication.

<sup>8</sup> Advertising, which provide advertising information in the style of an editorial or an objective journalistic article.

<sup>9</sup> [European Advertising Standards Alliance \(EASA\)](http://European Advertising Standards Alliance (EASA)) represents and coordinates the advertising self-regulatory systems across Europe.

<sup>10</sup> Estimates are based on average number of complaints and copy advice requests respectively, provided in the five-year period between 2014 and 2018. For more information please refer to [EASA's European annual statistics reports](http://EASA's European annual statistics reports).

Minimising the risk of advertising inadvertently appearing on such sites can be facilitated with the use of brand safety tools and sound business practices. Brand safety describes an entire area of practice where advertisers, agencies and technology companies try to prevent advertising from being misplaced. The digital advertising industry is deeply invested in brand safety, as our strong support for the European Commission’s “follow-the-money approach” on misplacement of ads on websites that infringe intellectual property rights attests<sup>11</sup>. The European approach builds on experiences from national markets where a number of successful industry initiatives emerged<sup>12</sup>.

Similarly, the digital advertising industry is committed to tackling the issue of disinformation. IAB Europe endorsed the EU Code of Practice on Disinformation<sup>13</sup>, recognising that legitimate online infrastructure can be misused by bad actors to deceive and confuse citizens, making it more difficult for them to make fact-based judgments, and ultimately undermining our democracies. Conversely, it is in our communal interest to ensure that the digital ecosystem primarily remains a powerful platform for the democratic dissemination of information and views. Though all manifestations of online disinformation do not leverage, or relate to, advertising, digital advertising may facilitate the creation and propagation of disinformation, for example, by inadvertently enabling the placing of legitimate advertising on websites enabling disinformation. Reducing such ad misplacement can be indeed improved by investment in brand safety tools.

### ***Relevance of the GDPR for user rights***

The GDPR unambiguously establishes the principles of data protection in the digital advertising context. What is important from the user perspective is the fact that the legal framework explicitly recognises a host of user rights from which consumers can benefit in relation to advertising powered by data, which is essentially all advertising online. Any new regulatory framework should acknowledge the existence of such user rights in the GDPR and not duplicate them, or create legal uncertainty by introducing ambiguous related provisions.

---

<sup>11</sup> [The Memorandum of Understanding \(MoU\) on Online Advertising and IPR](#) is a voluntary agreement facilitated by the European Commission to limit advertising on websites and mobile applications that infringe copyright or disseminate counterfeit goods. In addition to the MoU efforts, IAB Europe has been supportive of the initiative embracing a similar approach spearheaded by the World Intellectual Property Organisation (WIPO), [WIPO ALERT](#). WIPO ALERT is a secure, online platform to which authorized bodies in WIPO member states can upload details of websites or apps which have been determined to infringe copyright according to national rules. Access to the platform is given to any genuine digital advertising industry player which is willing to undertake to use the information solely for preventing the appearance of advertising on pirate websites.

<sup>12</sup> [IAB Europe Navigator: Quality Initiatives](#) (January 2020) demonstrates the vast amount of work being undertaken in Europe and beyond to build and ensure a sustainable future for digital advertising and marketing, in particular the national-level quality initiatives. There already exist several market-wide programmes, driven by European National IABs, that are designed to increase transparency & trust in how digital advertising is bought and sold, built on more specific pillars such as brand safety, fraud prevention, viewability, user experience. These initiatives include fully-fledged schemes with existing or to-be-developed monitoring and certification mechanisms. IAB Europe is working with members to share these best practices and help in harmonising relevant business standards across the continent.

<sup>13</sup> [The Code of Practice on Disinformation](#), unveiled in September 2018, addresses the spread of online disinformation. This is the first time worldwide that industry has committed, on a voluntary basis, to self-regulatory standards to fight disinformation. It aims at achieving the objectives set out by the [Commission's Communication presented in April 2018](#) by setting a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation. The Code includes an annex identifying best practices that signatories will apply to implement the Code's commitments.

For background on relevance of the law for the industry, the scope of the law is comprehensive and guarantees the protection of personal data both in the context of electronic communication services and information society services. Pseudonymous identifiers (Rec. 26), online identifiers, such as cookies, and device identifiers, are examples of personal data under the GDPR (Art. 4(1), Rec. 30). In addition, the GDPR contains rules on profiling and provides enhanced rights to users where profiling takes place (Art. 4(4), Art. 22, Rec. 72), including where user behaviour is tracked online (Rec. 24). The GDPR also explicitly calls out online advertising (Rec. 58).

The principle of fairness enshrined in the GDPR requires that users be informed of the fact that the supplier of an online service (or its partners) intends to process their personal data or is already doing so (Rec. 39). It also requires that they understand the purposes of the processing (Rec. 60), as well as whether they are obliged to provide the data in order to avail themselves of the service, and what would happen if they elected not to. Users should also not be subject to any decision based on automated processing without human intervention that produces legal or similarly grave effects on them (Rec. 71). The whole gamut of user rights is expressly recognized in the GDPR, and consequently applicable to instances where personal data is processed in relation to digital advertising. These include: right to know whether one's personal data are being processed, right to know why one's personal data are being processed, right to know the categories of personal data that are being processed, right to access the personal data that are being processed, right to information about whom the personal data have been, or will be, shared with (Art. 15), right to know how long personal data will be kept (Art. 15), right to rectification (Art. 16), right to erasure (Art. 17), right not to be the object of automated decision-making with legal or similar effects (Art. 22), right to data portability (Art. 20), right to object to having personal data processed (Art. 21), right to information as to where personal data in the possession of the data controller were originally obtained (Art. 15), right to be able to lodge a complaint with an appropriate authority (Art. 15), right to an effective judicial remedy against a controller or processor in case of a breach of the law (Art. 79), right to compensation for damage suffered as a consequence of an infringement of the Regulation (Art. 82).

Given the fact that the GDPR requires that individual users have full transparency about, and control over, any processing of their personal data, which consequently obliges data controllers to leverage a relevant legal ground for processing personal data and providing users with certain specific pieces of information in order for the processing to be legal, the industry has invested considerable resources in developing legal compliance solutions.

IAB Europe and its members created an open-source, cross-industry standard, the IAB Europe's Transparency & Consent Framework<sup>14</sup> (TCF). It is to ensure that where personal data is processed in connection with the delivery and measurement of advertisements or the personalisation of editorial content, consumers as well as industry stakeholders benefit from transparency and control. The TCF standardises how websites make the information disclosures required by the GDPR, how the sites collect and log users' choices, how they communicate those choices to their third-party technology partners, and what those partners may and may not do as a consequence. It delivers this

---

<sup>14</sup> <https://iab europe.eu/tcf>.

functionality using a combination of software and a digital signal that is transmitted from each website to a defined set of technology partners with whom the website works. The signal captures which data processing purposes and data controllers the user has authorised, if any, and requires those receiving the signal to honour it in accordance with clearly defined rules.

### Part 3 – Transparency in digital advertising supply chain

Digital advertising trading can happen in a variety of ways. The industry is committed to maintaining transparency and quality across the digital advertising and marketing ecosystem, for all forms of trading.

As the ecosystem is ever-evolving, and new and more players join the open market, it is important to hone the approaches to generate transparency developed by the industry. Resources and technical tools, such as IAB Europe Supply Chain Transparency Guide<sup>15</sup>, IAB Tech Lab’s ads.txt<sup>16</sup>, sellers.json and OpenRTB Supply Chain object<sup>17</sup> allow for analysis of the broad supply chain<sup>18</sup>, and may even be applicably nationally, like some of the market-wide Programmatic Codes of Conduct<sup>19</sup>.

These instruments help buyers and sellers of digital media to navigate through pertinent questions concerning data, cost and inventory source, or verify entities to ensure that only authorized players participate in ad transacting. Despite the fact that the open market may on the surface come across as complex, due to the abundance of participants and offerings, it remains critically important to reach audiences at scale and to monetise inventory. In particular, given the fact that smaller players and publishers specifically rely on support from their technical providers.

Overall, the issue is not with inaccessibility of information, but rather with managing complexity and having the right analytical and data science skills. On that note, one should not confuse alleged *opacity* in the ecosystem with the *complexity* of the industry, which has evolved considerably over the period of the last decade, notably as of 2010 with the inception of the Real-

<sup>15</sup> <https://iab europe.eu/research-thought-leadership/iab-europe-transparency-guide/>.

<sup>16</sup> <https://iabtechlab.com/ads-txt/>.

<sup>17</sup> <https://iabtechlab.com/sellers-json/>.

<sup>18</sup> The initiatives and standards continue to evolve, to keep apace with technology and industry developments. For instance, more recently, the industry has been working together to standardise log level data fields and definitions. In February 2020, IAB Europe created a working group within the Programmatic Trading Committee tasked to look at Supply-Side Platforms (SSP) Data best practices. The group includes SSPs, publishers and agencies, to understand the differences across these data fields and to harmonise the reporting fields.

<sup>19</sup> The [DACH](#) (German speaking markets: Germany (D), Austria (A), and Switzerland (CH)), and [Polish](#) markets put in place Programmatic Codes of Conduct, which include commitments with precise rules for all market participants. The objective is to ensure quality in programmatic advertising as well as to achieve the highest possible transparency and sustainable professionalism in view of modes of operation and methods of the market participants. The signing parties obligate themselves at the very least to comply with the defined criteria and conditions and to make sure that their contractual partners are also in compliance. Complaints are handled in a standardised process that is binding for all parties, and the board of complaint will process all matters as well as review processes and violations against the commitment. As IAB Europe, we are working with members exploring the scalability of the instrument.

Time Bidding. IAB Europe is actively promoting education and relevant skills to get more people with those skills into digital advertising and help companies connect with such talent.

## Part 4 – Liability regime of digital services

The existing eCommerce Directive<sup>20</sup> governs ‘information society services’ (ISS) (Art. 1(b)(ii), Art. 1(b)(iii) of the Information Society Services Directive<sup>21</sup>, and Art. 2(d), Rec. 18, Rec. 20 of the eCommerce Directive). It can be reasonably assumed that most of the players in the digital advertising ecosystem provide a service that may be deemed an ‘information society service’.

The regime also governs ‘commercial communications’ which are part of, or constitute, an information society service (Art. 2(f), Art. 6). Commercial communications must be clearly identifiable as such, along with the natural or legal person on whose behalf the commercial communication is made and various other details such as the conditions for any promotional offers like discounts (Art. 6). They therefore impose a burden on those on behalf of whom they are made.

This is relevant in a highly interconnected digital advertising ecosystem where parties collaborate to place advertisements and can be ultimately considered as subcontractors of one another. Most advertisements will constitute commercial communications if sent as part of an information society service and they will almost always be sent on behalf of a buyer. Most of the partners in the supply chain will not usually be involved in transmitting commercial communications, as it is the buyer’s ad server that normally transmits advertisements to the publisher. The advertiser is therefore generally the party on whose behalf an advertisement is made. The paradigm reflects the reality of the market, whereby it is the advertiser that is knowledgeable about the product or service advertised for, thus being in a position to take decisions about contents of advertising and its purpose, as well as other determinations regarding the media buying, for instance, the method of trading and desired target audience.

The Directive also sets out various provisions governing the liability of ‘intermediary service providers’ (ISP). Where certain conditions are met, the providers are not liable for information transmitted or stored, as appropriate. Member States are also obliged not to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity. A provider of an ISS is not automatically entitled to the safe harbours offered to ISPs under the Directive (Rec. 42).

As a general rule, it is worthwhile recalling that while technical capacity and functions of specific players in the supply chain will differ, these players remain entities working on behalf of other parties, notably advertisers and publishers. Generally, the various players have no knowledge or control over the content, or data stored or transmitted. That said, it should be noted that many

---

<sup>20</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), OJ L 178, 17.7.2000.

<sup>21</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society Services.



players may undertake various monitoring activities, in order to comply with the law but not limited to, for instance, to improve the quality and transparency of digital trading, minimize associated risk, or ensure measurement of the advertising itself or services provided – all further to wishes of their clients.

One of the challenges of the current regime for ISS providers is that, if they undertake moderation or monitoring and obtain too high degree of knowledge or control of content or data, then they can lose the benefit of the safe harbours under the Directive. It would be unfortunate if by virtue of complying with the law or performing due diligence digital advertising players were losing the protection from liability that they enjoy due to additional knowledge or control that they may exercise over the content or data that they monitor. We, therefore, generally welcome reflection on the ‘Good Samaritan’ provision.