Advertising Information Group's Response to the European Commission's Digital Omnibus Proposals

Executive Summary

The Advertising Information Group (AIG) welcomes the simplification objectives of the European Commission's Digital Omnibus initiative, particularly Article 3's codification of the relative nature of personal data and expanded scientific research definitions. However, new proposed GDPR Articles 88a and 88b perpetuate fundamental flaws in current privacy regulation, namely the fact that consent is required for any data processing, without delivering meaningful user benefits, while undermining the digital economy by also making it more difficult to obtain the necessary consent.

Current data protection law has failed both consumers and businesses. Consent is required for any data processing, including low-risk applications that are necessary for the functioning of websites, creating meaningless background noise, whilst legitimate business activities like advertising, email marketing measurement, and ad and audience analytics face disproportionate compliance barriers.

The proposals create new complexities rather than simplification and threaten the €7 economic multiplier effect advertising generates for every €1 spent.[1] Article 88a undermines established soft opt-in mechanisms for existing customer communications and restricts the design and frequency of consent requests, whilst Article 88b concentrates control over digital advertising in browser vendors' hands, impacting the viability of digital services, competitiveness, media diversity and democratic discourse.

Risk-based regulation offers a better path forward. Rather than treating all data interactions identically, regulation should distinguish genuinely privacy-intrusive activities from essential commercial operations like fraud prevention, audience measurement, and advertising that support free digital services.

AIG's recommendations focus on achieving the Commission's stated simplification objectives whilst preserving the advertising-funded ecosystem that provides free access to digital services, information and entertainment across Europe.

1. Introduction

The Advertising Information Group (Transparency number: 11220347045-31) welcomes the simplification objectives of the European Commission's Digital Omnibus initiative. Current data protection law imposes significant compliance

[1] https://valueofadvertising.org

burdens whilst failing to protect consumers effectively. Cookie consent has become ubiquitous, now required for any data processing activities, turning a tool designed to improve transparency, consumer choice and data protection into a nuisance for consumers and a hurdle for businesses.

This response demonstrates how risk-based regulation can deliver genuine consumer protection whilst preserving the advertising-funded digital services that provide free access to services, information, entertainment, and communication across Europe.

2. Codification of the Relative Nature of Personal Data

We strongly welcome Article 3 amending GDPR Article 4(1), which codifies that *'information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates'*. This reflects the judgement of the CJEU in Case C-413/23 P EDPS v SRB (Concept of personal data) that pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725.

This aligns with the proper scope of Article 8 of the Charter of Fundamental Rights (CFR), which protects personal data processing through requirements for lawful and fair processing, purpose limitation, access rights, rectification, and independent supervision. Importantly, Article 8 does not require that data protection obligations take a maximalist approach with the broadest categorisation of information as personal data.

More importantly, this clarification addresses longstanding uncertainty about the GDPR's scope with respect to handling pseudonymised data. The provision supports the development of privacy-enhancing technologies and a risk-based approach to the processing of personal data by reducing compliance complexity for data processors who are handling pseudonymised data and do not have the means to reidentify or attribute the data to a specific data subject.

3. Improved Scientific Research Definition

Article 3, which amends GDPR Article 4(38)'s definition of scientific research, acknowledges that innovation and commercial development are interconnected rather than artificially separate categories. This reform will bring clarity and legal certainty to the market research community that the regime already affords to academic research.

Privately funded market research is an integral part of the European research and innovation system. For decades, it has provided scientifically grounded contributions to

labour market, social, education, economic and broader societal analyses, regularly carrying out research on behalf of both public and private entities.

Importantly, it aligns with GDPR Recital 159, which states that '*for the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.*' The key point is that scientific research was intended to be interpreted in a broad manner to include academic and commercial research.

Unfortunately, the EDPB and the EDPS, in their joint opinion on the Digital Omnibus proposal,[2] have recommended that scientific research should:

'*1. be conducted following a methodological and systematic approach of the relevant scientific research field. In addition, it should be added that scientific research should be conducted in an autonomous and independent manner;*

2. lead to verifiable and transparent results. It is recommended to explain in the recitals that transparency may, among other things, involve making research results publicly available. In this regard, it is noted that the publication of the results may also contribute to the aim of contributing to the growth of society's general knowledge and wellbeing.'

Furthermore, it recommends:

'*moving the phrases 'any research which can also support innovation, such as technological development and demonstration' and '[t]his does not exclude that the research may also aim to further a commercial interest' from the definition into the relevant Recital'*

The introduction of phrases such as 'methodological and systematic approach' and 'verifiable and transparent results' directly targets and limits commercial research. Also, by moving innovation and commercial interest from the definition to the relevant Recital, it sends an implicit signal that there is a legal hierarchy with respect to what counts as scientific research.

We therefore believe that the Digital Omnibus codification brings greater alignment between the GDPR definition and its practical application.

4. Article 88a: Terminal Equipment Processing

The proposal's stated aim of introducing a regulatory solution to address the fatigue and proliferation of cookie banners and simplify the interplay between GDPR and Article 5(3)

[2] https://www.edps.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

of Directive (EU) 2002/58/EC (ePrivacy Directive) is one that we wholeheartedly support. However, we believe the proposal itself falls short of this aim and it would be a missed opportunity if not fully addressed.

Fundamentally, there are issues with a consent-centric framework and treating all terminal equipment interactions as equivalent privacy intrusions regardless of actual risk. It ignores critical distinctions between active data access and passive information flows inherent in internet communication protocols and restricts the design and frequency of consent requests, with harmful practical consequences.

4.1 The Access versus Flow Distinction

The EDPB's final Guidelines 2/2023 (version 2.0) emphasise that ePrivacy Directive Article 5(3) applies when entities 'proactively send specific instructions to the terminal equipment.' However, this interpretation fails to distinguish between active data retrieval and information flows that are necessary for standard internet communication protocols. This distinction is crucial for understanding legitimate commercial operations that do not constitute privacy intrusions.

Consider key internet functions where terminal equipment initiates information transmission:

- HTTP header requests containing user agent strings and encoding preferences automatically sent with website requests
- IP address allocation processes where terminal equipment requests network addresses from Dynamic Host Configuration Protocol (DHCP) servers
- URL tracking parameters appended to links that capture click events without identifying specific users
- Email tracking pixels that measure engagement without collecting sensitive information or storing data on terminal equipment

German data protection authorities[3] recognised this distinction, clarifying that processing information 'transmitted inevitably or due to browser settings of the end device when a telemedia service is accessed' does not constitute 'access to information already stored in the end device.'

4.2 Impact on Legitimate Marketing Practices

Article 88a's broad consent requirements undermine established ePrivacy Directive provisions, particularly the soft opt-in mechanism under ePrivacy Directive Article 13(2) that enables direct marketing to existing customers. Since email tracking pixels are

[3] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

embedded in marketing emails, Article 88a effectively requires separate consent even when relying on soft opt-in, rendering this legitimate marketing mechanism meaningless.

Email tracking pixels collect individual-level engagement data before any aggregation occurs.

Article 88a(3)(c) provides an exemption for *'creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use.'* However, as drafted, the exemption only covers the aggregated output, not the individual data collection that enables it.

Furthermore, 'solely for its own use' is unnecessarily limiting given that many businesses use email service providers (Mailchimp, Constant Contact, etc.) or share engagement data with:

- Marketing agencies managing campaigns
- Parent companies for consolidated reporting
- Analytics platforms for cross-channel attribution
- Customer Relationship Management (CRM) systems for lead scoring

It is also unclear whether marketing emails constitute an 'online service' within the exemption's intended meaning, which seems focused on website audience measurement.

The current proposal creates an untenable imbalance between privacy rights and Article 16 of the Charter of Fundamental Rights on the freedom to conduct a business, especially as many businesses and charities rely on email marketing effectiveness measurement to justify their communications.

4.3 Scope of Necessary Activities

Article 88a(3)'s exemptions remain too narrow for modern digital service realities.

Audience measurement is an important function for media owners to determine consumption of content and to price advertising space for advertisers. Such metrics are crucial for assessing the effectiveness of a media channel.

For sites that carry advertising, cookies are used to verify the delivery and performance of a digital ad, i.e., confirmation that an ad has been served or presented to a user, and whether it has been clicked on. This information is necessary to accurately invoice an advertiser for the number of ad impressions in a digital ad campaign.

Current legal guidance requires media owners to seek separate consents for each purpose, and consumers can decline these important cookies and render the ads to that user worthless. Put simply, if the advertiser is not provided with evidence that the user has interacted with the ad, due to the user declining cookies that measure ad performance, the advertiser cannot be invoiced for it and the publisher does not get paid.

The 'strictly necessary' interpretation should acknowledge that modern advertising-funded services require inter alia integrated technical systems for security, performance optimisation, and fraud prevention that cannot be artificially separated into purely editorial versus commercial functions.

The current regulatory approach creates uneven outcomes whereby protecting users from advertising fraud, for example, requires more compliance than protecting them from financial fraud, revealing incoherence in applying blanket consent requirements across diverse activities with vastly different privacy implications.

The sustainability of advertising-funded services depends on measurement and attribution capabilities. Publishers and content providers need to demonstrate audience engagement to justify advertiser investment, whilst advertisers require performance metrics to allocate budgets effectively.

Without these essential commercial mechanisms, the economic foundation of free digital services collapses, forcing paid access models that exclude many users.

4.4 Restrictions to the design and frequency of consent requests

Article 88a(4)(a) would introduce a mandatory single-click 'Reject all' button on the first layer of the consent request. This proposal represents a significant tightening of the current legal framework, would substantially reduce consent rates, impair the financing of digital services, and is incompatible with Consent or Pay models.

Furthermore, Article 88a(4)(b) prohibits renewed consent requests until consent remains valid, while Article 88a(4)(c) imposes a six-month prohibition on renewed consent requests following a refusal. However, purposes, partners, and services typically change more frequently than the duration of consent (i.e. more frequently than every six months), and such updates legally require renewing consent, which is prevented by these provisions. These provisions would not only discourage innovation, but without data processing, it would also not be possible to determine whether or when a user previously refused consent.

5. Article 88b: Machine-Readable Privacy Signals

5.1 Competitive Market Distortions

Article 88b's automated consent mechanisms risk creating distortions in digital services markets by concentrating control over key commercial data flows with browser vendors. This approach delegates regulatory compliance to a concentrated market of gatekeepers, potentially determining which services can access data necessary for commercial sustainability.

The requirement for web browser providers to facilitate these mechanisms effectively creates new intermediation layers in the direct publisher-user relationship. This concentration of control over advertising-funded services' commercial viability risks exacerbating competitive asymmetries between large platforms and smaller services and undermines the viability of advertising-funded businesses, as generalised consent requests are more likely to be declined.

Moreover, whilst Article 88b(3) exempts media service providers from machine-readable consent mechanisms, this provides no meaningful relief as they remain subject to Article 88a's consent requirements for all advertising and measurement activities, including the unworkable design and frequency restrictions per Article 88a(4) described above. The exemption therefore falls short of its objective of supporting media financing and pluralism, whilst leaving the underlying consent barriers intact for advertising-funded media operations. This selective approach undermines the Commission's stated simplification objectives by creating a cosmetic carve-out rather than addressing the core regulatory problems that affect media sustainability.

5.2 Lessons from Failed ePrivacy Proposals

Article 10 of the Commission's previous draft ePrivacy Regulation proposal included similar centralised consent mechanisms but was abandoned following extensive stakeholder consultation that identified core concerns about competitive distortions, implementation complexity, and unintended market concentration. These considerations led to the deletion of Article 10 by the Council and to insurmountable disagreements between the co-legislators that triggered the withdrawal of the proposal. Nothing has fundamentally changed with respect to these concerns, which remain equally valid for Article 88b's approach, so it is unclear why the Commission decided once again to propose the same recently rejected idea without conducting an impact assessment.

5.3 Technical Implementation Challenges

The regulatory design questions present significant challenges: voluntary versus mandatory participation, abstract versus context-specific preferences, interoperability across diverse implementations, and critically, preventing new gatekeeping functions. Apart from stipulating standards, the proposals do not appear to recognise the need for a comprehensive impact assessment and extensive stakeholder consultation.

Beyond Articles 88a and 88b, the Digital Omnibus creates additional complexity through Article 5's parallel regulatory structure.

6. Article 5: Parallel Data Protection Regimes

6.1 Structural Complexity and Legal Uncertainty

Article 5's amendment to ePrivacy Directive Article 5(3) creates a parallel regulatory structure by adding: *'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.'* This establishes separate data protection regimes for personal and non-personal data within the same regulatory framework.

This proposal creates significant implementation challenges and legal uncertainty as data controllers must determine in real time whether information 'constitutes or leads to' personal data processing. The same technical operation may require different legal bases depending on downstream use. A single data flow containing personal data could simultaneously fall under ePrivacy (if pseudonymised for the data processor) and GDPR (for the data controller), creating inconsistent obligations.

Businesses will face compliance complexity when data flows span both personal and non-personal categories given the significant legal uncertainty about the boundary between ePrivacy and GDPR obligations.

Recital 44 suggests that controllers may rely on legitimate interests under GDPR Article 6(1)(f) for subsequent personal data processing. However, this conflicts with established regulatory guidance. WP29 Opinion 2/2010 on online behavioural advertising effectively restricts advertising activities to consent-based processing, creating uncertainty about whether the Digital Omnibus proposals actually enable the alternative legal bases they appear to consider.

Recital 44's statement that 'the controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf' further compounds this uncertainty. It remains unclear whether this refers to terminal equipment access, subsequent personal data processing, or both, and how such arrangements interact with the Article 88a(3)(c) exemption's 'solely for its own use' limitation.

This parallel regime approach contradicts the policy goal of simplification and harmonisation. Rather than creating clearer rules, it establishes a complex dual-track system where identical technical operations may fall under different regulatory frameworks depending on contextual factors that may not be apparent at the time of data collection.

EU Transparency Number: Transparency number: 11220347045-31
www.aig-europe.eu

The 'constitutes or leads to' formulation is particularly problematic as it requires predictive assessment of future data use scenarios. This creates perverse incentives for over-compliance and may discourage legitimate innovation in privacy-enhancing technologies that could benefit both businesses and consumers.

These implementation challenges demonstrate why the Digital Omnibus requires a more sophisticated approach than blanket consent requirements.

7. Towards Risk-Based Regulation

7.1 Fundamental Principles

Effective privacy regulation must balance confidentiality of private communications with industry sustainability and fundamental rights. Rather than treating terminal equipment as uniformly part of a user's private sphere, regulation should examine in granular detail what information is revealed under what circumstances and what user controls exist.

The notion that all information must receive the same protection as personal data is untenable, particularly when non-personal data falls outside GDPR scope. Regulation should distinguish between communication technology protocol implementation, which necessitates information exchange, and information that is intercepted or surreptitiously accessed.

7.2 Charter Rights Balance

Whilst respecting Articles 7 and 8 of the Charter (private life and data protection), regulation must maintain an equitable balance with Article 11 (media freedom and pluralism) and Article 16 (freedom to conduct business). Article 1 of the ePrivacy Directive explicitly aims not only to protect privacy but also to 'ensure the free movement of data and electronic communication services' in the Union. This principle is further reinforced by GDPR Recital 13, which states that 'the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'.

8. Recommendations

a. Revise Article 88a(3):
   - Recognise internet communication protocol implementations that necessitate information exchange
   - Include fraud prevention, cybersecurity measures, and brand safety technologies under an extended cookie consent exemption
   - Permit aggregate audience measurement that is important for media sustainability

EU Transparency Number: Transparency number: 11220347045-31
www.aig-europe.eu

- Preserve soft opt-in mechanisms for legitimate direct marketing measurement

b. Delete restrictions to consent requests:
   - Delete the requirement for a one-click reject-all button in the first layer of consent requests per Article 88a(4)(a)
   - Delete the restrictions to the frequency / repetition of consent requests per Article 88a(4)(b) and (c)

c. Clarify GDPR Integration:
   - Explicitly permit legitimate interest assessments for exempted activities
   - Provide guidance distinguishing active access from passive information flows
   - Ensure transparency requirements focus on meaningful rather than technical information

d. Reconsider Article 88b:
   - Conduct a comprehensive impact assessment on digital market competition and extensive stakeholder consultation
   - Delete the proposed Article, or strengthen the media exemption to include advertising and measurement partners
   - Evaluate alternatives that enhance user control without intermediation layers

9. Conclusion

Successful digital regulation requires moving beyond binary technology-based requirements towards sophisticated risk assessment that considers actual privacy impact, user understanding and control, commercial necessity, and proportionality. This approach would leverage existing self-regulatory frameworks whilst maintaining competitive neutrality.

The Digital Omnibus presents a critical opportunity to address core regulatory failures whilst preserving the advertising-funded digital ecosystem essential to European media diversity and democratic discourse. Article 3's clarifications provide a strong foundation, but Articles 88a and 88b should be deleted or substantially revised, as they fail to address the root cause of consent fatigue while disrupting the digital economy and distorting competition. Consent fatigue should be addressed by allowing other legal bases for data processing for low-risk uses, rather than by restricting consent requests.

Our analysis shows that sophisticated risk-based approaches can deliver better consumer protection whilst maintaining commercial viability. Remaining true to the Simplification agenda could position Europe as the global standard for balanced digital governance, which remains compatible with growth and innovation.

EU Transparency Number: Transparency number: 11220347045-31
www.aig-europe.eu

We emphasise the need for European regulation to serve both privacy protection and economic sustainability, supporting the diverse digital services that underpin democratic participation and cultural expression across the EU.

About AIG

AIG is an informal pan-European network of European advertising and media associations that brings together various parts of the advertising industry: from advertising agencies, broadcasters (TV and radio) and publisher bodies to direct marketing and online advertising.

Advertising is a key driver of growth in the creative industries. It employs the services of other creative industries: from music, fashion, film production and special effects, to animation, games and photography. A study conducted by Deloitte[4] showed that for every €1 spent on advertising, it generated €7 for the wider European economy. Advertising forms approximately 4.6% of the EU's GDP whilst helping SMEs to find new markets and charities to find new donors. Advertising also plays a key role in fostering brand competition, supporting product innovation while enabling diverse and pluralistic media.

Current regulatory approaches that undermine advertising effectiveness threaten the economic multiplier effect of advertising. Risk-based frameworks would preserve these economic benefits whilst strengthening consumer protection.

Advertising Information Group
10 March 2026

[4] https://valueofadvertising.org