Response to the European Commission's Call for Evidence: Digital Omnibus – Cookie Regulation and AI Act Implementation

EXECUTIVE SUMMARY

Current cookie regulations are failing consumers and businesses alike. Users face constant interruption from meaningless consent prompts whilst businesses bear disproportionate compliance costs for low-risk activities. The AI transparency regulation creates potential compliance issues for the advertising industry. The Advertising Information Group (AIG) proposes risk-based frameworks that focus regulatory attention where it matters most: protecting consumers from genuine privacy harm whilst enabling sustainable digital innovation.

Cookie Regulation Reform:

- Replace blanket consent requirements with risk-proportionate regulation distinguishing high-risk behavioural tracking from essential commercial operations.
- Expand 'strictly necessary' interpretations to include ad fraud prevention, measurement, and privacy enhancing technologies, e.g. contextual advertising that directly enable service delivery.
- Align ePrivacy requirements with a risk-based GDPR legitimate interest assessment to eliminate regulatory duplication and complexity.
- Exempt low-risk activities from consent whilst maintaining transparency obligations and appropriate safeguards.
- Focus consent requirements exclusively on genuinely privacy-intrusive activities such as cross-site profiling and detailed personal data combination.
- We remain sceptical about any proposals for "central cookie management mechanisms" within the framework of the omnibus package given the potential impact to digital competition. Such proposals should be avoided at all costs.

AI Act Implementation:

- Adopt risk-based transparency framework assessing actual deception potential rather than requiring universal AI content labelling.
- Distinguish between high-risk applications (synthetic testimonials, misleading product demonstrations) requiring mandatory disclosure and low-risk technical enhancements requiring no labelling.
- Clarify that the AI Act's deepfake definition should not encompass legitimate advertising practices using AI for standard creative enhancement.
- Prevent labelling fatigue by avoiding universal disclosure requirements that could mirror cookie consent banner problems and undermine meaningful transparency.

- Provide clear guidance on commercial content exemptions to prevent competitive distortions favouring traditional production methods over AI innovation.
- Align AI transparency obligations with existing advertising standards frameworks rather than creating parallel regulatory requirements.
- Support proportionate compliance pathways for SMEs and mid-cap companies facing disproportionate implementation burdens.

Integrated Framework:
Both reforms should harmonise with existing advertising regulations, respect established self-regulatory frameworks and focus enforcement on activities presenting genuine consumer harm whilst eliminating barriers to legitimate commercial innovation and digital service sustainability.

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, broadcaster (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 showed that for every €1 spent on advertising it generated €7 for the wider European economy.[1] 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 a 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.

[1] https://valueofadvertising.org/value-of-advertising/value-of-advertising-report/

INTRODUCTION

The Advertising Information Group (Transparency number: 11220347045-31) welcomes the European Commission's Digital Omnibus initiative. Current cookie rules and AI transparency requirements create a regulatory paradox: they impose significant compliance burdens whilst failing to protect consumers effectively. Cookie consent has become meaningless background noise, whilst blanket AI disclosure risks similar 'labelling fatigue'.

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

PART I: Cookie Regulation Reform - Moving Beyond Consent Fatigue

The current ePrivacy Directive fails both users and businesses through three fundamental problems:

- User experience: Estimates suggest that on average, a user visits about 100 websites per month, totalling 1,200 websites per year. With approximately 85% of these websites displaying a cookie banner, a user will encounter about 1,020 cookie banners every year.[2] This can lead to 'consent fatigue' where users automatically accept all prompts rather than making informed choices.[3]
- Business burden: Companies face unnecessary compliance costs for low-risk activities like fraud prevention and basic measurement, whilst higher risk behavioural tracking receives identical regulatory treatment.
- Regulatory incoherence: The requirements for companies, regardless of their size, to formally comply with the current ePrivacy regulation go beyond what companies need to adhere to for protecting consumers from direct financial fraud, revealing the system's disconnect from actual privacy risks.

Recent jurisprudence from the Court of Justice of the European Union provides clear legal foundation for pragmatic reform, particularly the Court's clarifications in Case C-413/23 P regarding pseudonymised data transfer, which creates a pathway for risk-based regulation distinguishing between genuinely privacy-invasive activities and essential commercial operations.

[2] Legiscope Blog. https://www.legiscope.com/blog/hidden-productivity-drain-cookie-banners.html
[3] The Behavioural Insights Team. Evaluating browser-based cookie setting options to help the UK public optimise online privacy behaviours https://assets.publishing.service.gov.uk/media/660d15f338f66c001184a95d/BIT_Evaluating_browser-based_cookie_settings_report.pdf

The advertising industry has evolved significantly since the ePrivacy Directive's conception, yet cookie regulation remains frozen in an earlier era of privacy thinking. 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 also creates uneven outcomes whereby protecting users from advertising fraud, for example, requires more compliance than protecting them from financial fraud, revealing fundamental incoherence in applying blanket consent requirements across diverse activities with vastly different privacy implications.

The commercial reality of digital service provision demonstrates why reform has become essential rather than merely desirable. The European digital economy rests on advertising-funded services providing free access to information, entertainment, and communication platforms. This model has democratised digital participation regardless of economic circumstances, supporting the diversity of voices essential to democratic societies. Current cookie rules impose costs extending far beyond direct consent management expenses, requiring complex technical infrastructure for activities posing minimal privacy risk whilst small and medium enterprises face disproportionate burdens competing with larger platforms that can absorb compliance costs and have highly competitive consent-centred data usage regimes for vertically and horizontally fully integrated services.

The user experience under current rules demonstrates regulatory failure through constant interruption and choice. Users encounter dozens of consent banners daily seeking permission for technical activities they cannot reasonably evaluate. Research consistently shows users cannot meaningfully engage with technical consent decisions about cookie categories, data processing purposes, or vendor relationships. The system requires every internet user to become a privacy and technology expert capable of assessing hundreds of different data processing activities, creating widespread consent fatigue where users automatically accept all prompts rather than engaging with underlying privacy choices. These fundamental failures require moving beyond blanket consent towards risk-based regulation.

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 fundamental commercial mechanisms, the economic foundation of free digital services collapses, forcing paid access models that exclude many users.

Our proposal centres on transforming the current consent model into a sophisticated, risk-proportionate framework. For lower risk activities such as ad fraud prevention, brand safety, measurement, and privacy enhancing technologies e.g. contextual advertising, we advocate exempting certain low-risk processing from consent requirements.

Legal Framework Integration

However, exempting cookies from e-Privacy consent requirements whilst providing no guidance on the legal basis (such as legitimate interests or contractual performance) for processing the associated personal data renders the exemption practically meaningless. Cookies typically involve processing pseudonymous personal data such as IP addresses, device identifiers, and other information that requires a lawful basis under GDPR.

If service providers still need to seek consent for personal data processing, then it will negate the intended relief. We therefore believe that it is necessary to permit legitimate interest assessments with appropriate safeguards and transparency obligations. The Court's guidance in Case C-413/23 P regarding information obligations provides additional clarity – controllers must inform data subjects about all potential recipients of their data at the point of collection, but this transparency requirement does not automatically necessitate consent for all subsequent processing activities. Where legitimate interests provide an appropriate lawful basis under GDPR, cookie rules should recognise this determination rather than imposing additional consent requirements that serve no additional privacy purpose.

Implementing this risk-based approach requires addressing the relationship between ePrivacy and GDPR frameworks. The current disconnect between cookie consent requirements and GDPR lawful bases creates legal uncertainty and compliance complexity serving neither privacy protection nor regulatory clarity. GDPR should provide and acknowledge a roadmap for already provides sophisticated mechanisms for balancing commercial interests against privacy rights through legitimate interest assessments, necessity determinations, and purpose limitation requirements. Cookie regulation should leverage these frameworks.

Privacy advocates may argue that any relaxation of consent requirements weakens consumer protection. However, our approach enhances meaningful control by eliminating meaningless barriers and focusing user attention on decisions that genuinely affect privacy.

Assessing the privacy impact of cookies

Effective cookie regulation must distinguish between activities based on actual privacy impact rather than commercial context.

High-risk activities requiring explicit consent include:

- Cross-site behavioural profiling that builds detailed personal profiles.
- Combining data from multiple sources to infer sensitive characteristics.
- Long-term tracking across unrelated websites and services.

Lower-risk activities manageable through legitimate interests include:

- Contextual advertising
- Fraud prevention protecting user accounts and payments.
- Aggregate audience measurement that cannot identify individuals.
- Essential service functionality like remembering user preferences.

This risk-based approach should recognise that many processing activities serve dual purposes: protecting users whilst enabling commercial sustainability. The 'strictly necessary' exception under Article 5(3) of the ePrivacy Directive already recognises this principle, but European data protection authorities interpret it too narrowly to accommodate modern digital service realities. This approach would also have a higher chance of success if it focused on the principle of purpose limitation rather than focussing on eliminating or minimising data collection via cookies entirely. Reformed GDPR principles (Art. 5) should acknowledge that certain foundational activities enabling service delivery can be 'strictly necessary' from users' perspectives when they directly enable access to requested services.

Maintaining User Control Under Risk-Based Regulation

Risk-based regulation enhances rather than diminishes user control by focusing attention where it matters most. Instead of overwhelming users with technical decisions about cookie categories, this approach would provide:

- **Enhanced transparency**: Clear explanations of actual data uses rather than technical jargon. Users would understand "we measure article readership to improve content" rather than navigating complex vendor lists.
- **Ongoing visibility**: Privacy dashboards showing real-time data use, with regular plain-language reports on any changes to data practices.

This approach respects user agency whilst eliminating the current system's fundamental problem: requiring every internet user to become a privacy expert to make informed decisions.

Beyond risk assessment, successful reform must also address emerging technical proposals that could undermine the direct publisher-user relationship.

Centralised Cookie Consent Mechanisms

We remain deeply sceptical about proposals for 'centralised cookie consent mechanisms'[4] within the Digital Omnibus framework. Whilst superficially appealing as a solution to consent fatigue, such mechanisms risk creating fundamental distortions in the digital services market whilst failing to address the underlying regulatory problems.

The processing of device-related information sits at the core of the relationship between digital services and their users, forming the basis for sustainable commercial models. Centralised consent mechanisms would aggregate control over metrics essential for data-driven advertising and marketing, targeted advertising delivery, and commercial content distribution. This concentration of control would have profound implications regardless of whether future regulation maintains opt-in consent requirements or transitions toward opt-out frameworks with legitimate interest processing.

The competitive implications of centralised consent mechanisms warrant particular scrutiny. Centralised consent mechanisms risk exacerbating competitive asymmetries rather than addressing them. If such mechanisms enable users to set abstract, general preferences – either consenting to or rejecting data processing without offer-specific context – they would undermine the value of informed, specific consent that currently provides smaller services some ability to compete for user consent. This approach would further concentrate competitive advantages with gatekeepers whilst marginalising the competitive position of SMEs and mid-sized digital services.

More fundamentally, centralised consent mechanisms could create new forms of intermediation in the direct publisher-user relationship. The ability to influence or filter consent flows would represent significant market power, potentially determining which services can access necessary data for commercial sustainability. Any legislative measures, especially mandatory regulations, will likely have a significant impact on the diversity and quality of the open internet, in particular media diversity.

Beyond competitive concerns, centralised consent mechanisms present substantial technical and regulatory complexity. The Commission's suggestion that such systems would 'strengthen autonomy and rights of users by giving them more control' oversimplifies the implementation challenges and potential unintended consequences. Effective mechanisms must balance user convenience with service sustainability and

[4] CALL FOR EVIDENCE, Digital Omnibus (Digital Package on Simplification) p3

maintain strict competition neutrality – objectives difficult to reconcile in centralised architectures.

The regulatory design questions alone present significant challenges: whether participation should be voluntary or mandatory; whether preferences should be abstract and general or offer-specific and informed; how to ensure interoperability across diverse technical implementations; and critically, how to prevent the emergence of new gatekeeping functions. These complexities require comprehensive impact assessment and extensive stakeholder consultation – processes incompatible with the urgent timeline needed for fundamental ePrivacy and GDPR reforms.

The decisive factor for enhancing EU digital services competitiveness in a practical manner lies in enabling alternatives to consent within the meaning of the GDPR for the processing of terminal-related information and personal data. This could be achieved if Community law legitimises low-risk processing through evidence-based legitimate interest assessments, which fits with a more risk-based GDPR, and at the same time scales back the consent-centric provisions under ePrivacy. This would also address consent fatigue for users whilst reducing compliance burdens for businesses, particularly SMEs lacking resources to navigate complex consent management requirements.

Attempting to resolve regulatory complexity through centralised consent mechanisms would fail to address fundamental legal framework problems. The urgent need for Digital Omnibus reforms centres on revising Article 5 of the ePrivacy Directive and Articles 5 and 6 of GDPR to enable risk-proportionate regulation. These reforms are both more urgently needed and should be the focus of legislative attention.

It bears noting that Article 10 of the Commission's previous ePrivacy Regulation proposal, which addressed similar centralised consent mechanisms, was recognised as unsustainable through extensive stakeholder consultation. The fundamental concerns that led to that provision's revision – including competitive distortions, implementation complexity, and unintended market concentration – remain equally valid today.

The Digital Omnibus presents an opportunity to deliver meaningful regulatory improvement through risk-based frameworks and legitimate interest recognition. Centralised consent mechanisms should not divert attention or resources from these essential reforms that can deliver immediate benefits for consumers, businesses, and digital services sustainability.

PART II: AI Act Implementation - Transparency Obligations

The EU AI Act's transparency requirements for advertising content present implementation challenges that risk undermining both consumer protection and industry innovation. As AI becomes integral to creative processes – from initial concepts to final production – determining what requires labelling becomes increasingly complex and potentially misleading.

The advertising industry has rapidly embraced generative AI across creative supply chains, from initial concept development and storyboarding to final content production, with major ad agency networks investing significantly in AI capabilities as they are viewed as critical to future competitiveness.

AI applications in advertising now span the full spectrum of creative activities: generating copy and taglines for campaigns, creating synthetic imagery and video content, developing personalised advertisements tailored to specific audiences, producing virtual brand ambassadors and influencers, enhancing or editing existing visual content, and automating ideation processes for creative concepts. These diverse applications create significant complexity when applying AI Act transparency requirements under Article 50, as advertising workflows increasingly integrate AI tools throughout creative processes, making it difficult to determine where human creativity ends and AI generation begins.

The current transparency obligations risk creating definitional ambiguity undermining their intended purpose. Many advertising campaigns now use AI tools existing on a spectrum of minor copywriting assistance to fully generated creative content. Determining whether such content requires transparency labelling becomes problematic and potentially misleading to consumers who may assume either complete AI generation or complete human creation. For instance, an advertisement might use AI for background removal and colour correction, human creativity for concept development, AI-generated imagery for product placement, and human-written copy enhanced by AI suggestions.

These requirements impose disproportionate compliance costs on advertising agencies and brands, particularly where consumer deception risk is minimal. The advertising industry already operates under robust consumer protection frameworks prohibiting misleading or deceptive practices. Existing advertising standards bodies across Europe enforce principles of legality, honesty, and truthfulness that have successfully adapted to previous technological changes. Blanket AI labelling requirements risk creating unnecessary administrative burdens without providing meaningful consumer benefit,

particularly for creative content where AI use enhances rather than replaces human judgement.

More concerning from an advertising perspective is potential consumer confusion and unintended market effects. Research indicates indiscriminate labelling may trigger the 'implied truth effect',[5] whereby unlabelled advertising content is perceived as more trustworthy simply by virtue of not carrying AI disclosure. This could inadvertently advantage advertisers avoiding AI tools, potentially stifling innovation and creating competitive distortions favouring traditional production methods over more efficient AI-assisted approaches.

The advertising industry faces 'AI aversion'[6] risk, where consumers may automatically distrust any AI-labelled content, regardless of its accuracy or quality. Studies suggest when consumers are informed about AI use in advertising, they tend to find advertisements less credible and view them less favourably, even when AI assistance is minimal or purely technical. This effect could undermine legitimate advertising practices and reduce communication effectiveness, ultimately harming both businesses and consumers relying on advertising for product information.

The potential for 'credibility transfer'[7] effects present another significant concern. If consumers discover that one advertisement aspect contains AI-generated content, they may dismiss accurate information about product specifications or benefits contained elsewhere in the same advertisement. Similarly, the 'tainted truth effect'[8] could undermine truthful commercial communications and create perverse incentives for advertisers to avoid transparency about legitimate AI use. These compliance challenges are compounded by definitional ambiguity in the AI Act itself.

A critical concern lies in the AI Act's definition of deepfakes in Article 3(60) as "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful". This definition is sufficiently ambiguous that it could encompass legitimate advertising practices that have been industry standard for decades.

---

[5] Pennycook et al (2020). The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings. https://pubsonline.informs.org/doi/10.1287/mnsc.2019.3478

[6] Qin et al (2025). AI aversion or appreciation? A capability–personalization framework and a meta-analytic review. https://psycnet.apa.org/doiLanding?doi=10.1037%2Fbul0000477

[7] Effect of disclosing AI-generated content on prosocial advertising evaluation. Baek et al (2024). https://www.tandfonline.com/doi/epdf/10.1080/02650487.2024.2401319?needAccess=true

[8] Szpitalak, M., & Polczyk, R. (2010). Warning against warnings: Alerted subjects may perform worse. Misinformation, involvement and warning as determinants of witness testimony. https://psycnet.apa.org/record/2011-07399-003

Advertising content routinely features synthetic elements, stylised representations, and creative interpretations of products and services that are understood by consumers to be promotional rather than documentary in nature. The term 'deepfake', which carries negative connotations and is typically associated with malicious deception, should not be conflated with standard advertising practices that use AI tools for legitimate creative enhancement.

Consider these common advertising scenarios under current definitions:

- A car advertisement using AI to enhance product imagery could be classified as a 'deepfake' despite transparent commercial intent.
- Fashion brands using AI-generated models might face identical labelling requirements as malicious deepfakes impersonating real people.
- Food photography with lighting enhanced by AI algorithms could require the same disclosures as fabricated customer testimonials.

This definitional confusion undermines consumer understanding and creates perverse incentives against legitimate technological innovation.

The current definitional framework risks creating confusion between advertising content that uses synthetic elements for creative effect and malicious deepfakes intended to deceive consumers about factual matters. Advertising content that uses AI to create stylised product demonstrations, enhanced visual presentations, or creative brand storytelling should be distinguished from content specifically designed to mislead consumers about product characteristics, false endorsements, or fabricated testimonials. The regulatory framework must recognise that advertising operates within established consumer protection principles where the commercial intent is transparent, and the creative nature of promotional content is well understood by audiences.

The widespread application of AI transparency requirements across advertising content also risks creating 'labelling fatigue'[9] that mirrors the problems experienced with cookie consent banners. Industry projections suggest 90% of advertisers will use AI tools to create video ads by 2026.[10] Universal labelling requirements would mean consumers encounter AI disclosure notices as frequently as cookie banners, potentially leading to similar patterns of automatic acceptance or dismissal without meaningful engagement.

[9] Gamage et al (2025). Labeling Synthetic Content: User Perceptions of Warning Label Designs for AI-generated Content on Social Media. https://arxiv.org/html/2503.05711v1
[10] IAB – 2025 Digital Video Ad Spend & Strategy Report. https://www.iab.com/wp-content/uploads/2025/07/2025_IAB_Digital_Video_Ad_Spend_Full_Report_July_2025.pdf

This proliferation of AI labels could paradoxically undermine the transparency objectives the requirements seek to achieve, as consumers learn to ignore ubiquitous disclosures that provide little meaningful information about content that genuinely warrants their attention.

The risk of labelling fatigue is particularly acute given that many AI applications in advertising involve technical enhancements or creative assistance that pose no meaningful risk of consumer deception. When consumers encounter identical disclosure language for AI-assisted colour correction and synthetic spokesperson presentations, they lose the ability to distinguish between activities that merit their consideration and those that are essentially technical necessities. This regulatory approach risks diluting the impact of transparency measures for genuinely problematic AI applications whilst creating compliance burdens that serve no consumer protection purpose. Like cookie regulation, successful AI transparency requirements need risk-based approaches that focus on actual consumer harm potential

Integrated Reform Framework

Both cookie regulation and AI Act implementation require moving beyond binary technology-based requirements towards nuanced, risk-based approaches focusing on actual consumer harm potential. For cookies, this means distinguishing between high-risk behavioural tracking requiring consent and low-risk activities manageable through legitimate interests with appropriate safeguards. For AI transparency, this means assessing whether AI use affects material product claims, whether synthetic endorsements could mislead consumers, and whether AI content influences core purchasing decisions.

The advertising industry requires practical guidance acknowledging the creative nature of advertising communications whilst maintaining consumer protection. Both regulatory areas should focus on harmonised standards across member states accounting for advertising-specific contexts, including developing implementation formats appropriate for different advertising media, establishing technical standards working with advertising technology platforms, and creating guidance for different advertising formats and contexts.

Enforcement coordination becomes particularly crucial for advertising given its cross-border nature within the EU single market. National advertising standards bodies and supervisory authorities need harmonised interpretation guidelines respecting existing self-regulatory frameworks whilst ensuring consistent application of both cookie and AI transparency requirements. This coordination should build upon advertising self-regulation's successful track record rather than displacing established industry practices.

Both regulatory frameworks should complement rather than conflict with existing advertising regulations. Integration with the Unfair Commercial Practices Directive should ensure requirements work alongside existing misleading advertising prohibitions, avoiding duplicate or contradictory obligations. Coordination should prevent consumer fatigue from multiple disclosure requirements whilst creating coherent regulatory frameworks.

The risk of creating uneven playing fields requires careful attention in both areas. If AI-generated content requires labelling whilst advertisements incorporating photoshop editing, CGI, and other digital manipulation techniques do not, or if certain cookie activities face different requirements based on commercial context rather than privacy risk, this could create competitive distortions penalising innovation without corresponding consumer protection benefits.

Implementation Recommendations

For cookie regulation, the Commission should adopt a comprehensive framework recognising commercial legitimate interests for essential advertising operations whilst maintaining consent for high-risk privacy activities. This includes potentially expanding 'strictly necessary' interpretations to acknowledge foundational activities enabling service delivery, permitting legitimate interest assessments for low-risk activities with appropriate transparency and opt-out mechanisms, and providing regulatory incentives for privacy-enhancing technologies through reduced compliance requirements.

For AI Act implementation, a risk-based transparency framework should assess actual deception potential considering degree of AI influence on core messages, clarity of AI use to reasonable consumers, verifiability of content claims, likelihood of influencing consumer decisions, and context setting appropriate authenticity expectations. High-risk applications requiring mandatory transparency labelling should focus on realistic AI-generated testimonials, synthetic product demonstrations potentially misleading about performance, and virtual influencers presented as real people without clear disclosure.

Implementation should occur through phased approaches with clear milestones for both regulatory areas. The Commission should begin with detailed guidance on legitimate interest assessments and expanded 'strictly necessary' interpretations for cookies within six months, alongside sector-specific AI transparency guidance for advertising applications. Industry consultation on technical safeguard standards and certification programmes should follow within twelve months, creating standardised frameworks for both privacy-preserving cookie implementations and proportionate AI disclosure mechanisms.

Conclusion

Europe has the opportunity to lead global regulation by focusing on outcomes rather than process. Risk-based frameworks that protect consumers from genuine harm whilst enabling sustainable digital services will deliver better results than blanket requirements that serve neither purpose effectively.

The Commission's leadership on pragmatic regulation could position Europe as the global standard for balanced digital governance. The advertising industry stands ready to collaborate on implementation that strengthens consumer protection whilst maintaining the diverse, accessible digital ecosystem essential to European democracy and economic growth.

Advertising Information Group
14 October 2025